OcNOS®

Open Compute
Network Operating System for Data Centers
Version 5.0

OcNOS Configuration Guide

October 2021

IP Infusion Inc. Proprietary

Contents

Preface lxix
Audience lxix
Conventions lxix
Chapter Organization lxix
Related Documentation lxix
Migration Guide lxix
Feature Availability lxx
Support lxx
Comments lxx

Command Line Interface 63
Overview 63
Command Line Interface Help 63
Command Completion 64
Command Abbreviations 64
Command Line Errors 64
Command Negation 65
Syntax Conventions 65
Variable Placeholders 66
Command Description Format 67
Keyboard Operations 67
Show Command Modifiers 68
String Parameters 71
Command Modes 71
Transaction-based Command-line Interface 73

Architecture Guide 77
Contents 77

CHAPTER 1 Architecture Overview 79
High-Level Architecture 80
Management Interface 81
Layer 2 Protocols 82
Layer 3 Protocols 85
Multicast Protocols 89
System Management 90
Virtual Extensible Local Area Network 93

System Management Configuration Guide 97
Contents 97

CHAPTER 1 Access Control Lists Configurations 99
Overview 99
Topology 99
IPv4 ACL Configuration 99

© 2021 IP Infusion Inc. Proprietary

ICMP ACL Configuration 100
Access List Entry Sequence Numbering 101
IPv6 ACL Configuration 102
MAC ACL Configuration 102
Management ACL Overview 103
ARP ACL Overview 108
ACL OVER LOOPBACK 109
ACL OVER VTY 111
Timed ACL 112
Topology 112

CHAPTER 2 Debounce Timer 115
Overview 115
Topology 115
Configuration 115
Validation 116
Log Messages 116

CHAPTER 3 DHCP Client Configuration 119
Overview 119
DHCP Client Configuration for IPv4 119

CHAPTER 4 DHCP Relay Agent Configuration 121
Overview 121
DHCP Relay for IPv4 121
DHCP Relay for IPv6 Configuration 122
DHCP Relay option 82 123
Physical Interface Configuration with non-default vrf 125
Validation 126

CHAPTER 5 DHCP Relay Agent Over L3VPN Configuration 133
DHCP Relay Over L3 VPN for IPv4 133
DHCP Relay Over L3 VPN for IPv6 138

CHAPTER 6 DHCP Snooping 145
Overview 145
Topology 146
Configuration Guidelines 146
Procedures 146
DHCP Snooping Operation 147
DHCP Snooping with Option-82 149

CHAPTER 7 DHCP Snooping IP Source Guard 155
Overview 155
Topology 155
Configuration 155
Configuring Trusted and Un-trusted Ports 157
Configuring IP Source Guard on LAG Port 158

CHAPTER 8 DHCP Snooping over MLAG 161
Overview 161

© 2021 IP Infusion Inc. Proprietary

Topology 162
Configuration 163
Validation 171

CHAPTER 9 DHCPv6 Prefix Delegation 177
Overview 177
Topology 177
Configuration 178
Validation 180

CHAPTER 10 DHCPv6 Relay Prefix Delegation Route Injection Configuration . . 183
Overview 183
Topology 183

CHAPTER 11 DNS Configuration 189
Overview 189

CHAPTER 12 ErrDisable for Link-Flapping Configuration 191
Topology 191
Automatic Recovery 191
Log Message 192
Manual Recovery 192
Errdisable at the Interface Level 194

CHAPTER 13 Ethernet Interface Loopback Support Configurations 195
Overview 195
Topology 195

CHAPTER 14 LAG with RTAG7 Hashing 205
Overview 205
Topology 205
Dynamic LAG with RTAG7 205
Static LAG with RTAG7 208

CHAPTER 15 Link Detection Debounce Timer 211
Log Messages 212

CHAPTER 16 Max Session and Session Limit Configuration 213
Overview 213
Configuration of SSH Server Session Limit Lesser than Max-Session 214
Configuration of Telnet Session Limit Greater than Max-Session 215
Configuration of SSH Session Limit Greater than Max-Session 216

CHAPTER 17 NTP Client Configuration 217
Overview 217
NTP Modes 217
NTP Configuration 218
Maxpoll and Minpoll Configuration 219
NTP Authentication 219

CHAPTER 18 Port Breakout Configuration 221
Overview 221

© 2021 IP Infusion Inc. Proprietary

Terminology . . . 221
Configuring Port Breakout 40G to 4x10G . . . 222
Removing Port Breakout . . . 222
Configuring Port Breakout (100G to 4x10G) . . . 230
Configuring Port Breakout (100G to 4x25G) . . . 231
Configuring Port Breakout (100G to 2x50G) . . . 232
Configuring Port Breakout at Global Configuration Level . . . 233

CHAPTER 19 Proxy ARP and Local Proxy ARP . . . 235
Overview . . . 235
Local Proxy ARP Overview . . . 236

CHAPTER 20 RADIUS Client Configuration . . . 241
Overview . . . 241
RADIUS Server Authentication . . . 241
RADIUS Server Accounting . . . 251
Sample Radius Clients.conf File . . . 252
Sample Radius Users Configuration File . . . 253

CHAPTER 21 sFlow Configuration . . . 255
Overview . . . 255
Configuration . . . 256
Validation . . . 256

CHAPTER 22 Show Tech Support Configurations . . . 257
Overview . . . 257
Tech Support Samples . . . 257
Validation Commands . . . 258

CHAPTER 23 Simple Network Management Protocol . . . 259
Overview . . . 259
Standard SNMP Configurations . . . 260
Validation . . . 260

CHAPTER 24 Software Monitoring and Reporting . . . 263
Overview . . . 263
Configuration . . . 263
Validation . . . 263

CHAPTER 25 SSH Client Server Configuration . . . 265
Overview . . . 265
Topology . . . 265
Basic Configuration . . . 265
SSH Keys . . . 266
SSH Encryption Cipher . . . 267
SSH Key Based Authentication . . . 268
Topology . . . 268
Public Key Authentication Method . . . 268
Restrictions . . . 270

© 2021 IP Infusion Inc. Proprietary

CHAPTER 26 Syslog Configuration 273
Logging to a File 273
Logging to the Console 275
Logging to Remote Server 276
Configuration 277
Remote machine Syslog Configuration: 278
Monitoring Logging Server: 278

CHAPTER 27 Telnet Configuration 281
Overview 281
Topology 281
Enable and Disable the Telnet Server 281
Configure the Telnet Server Port 281
Telnet Client Session 282

CHAPTER 28 TACACS Client Configuration 283
Overview 283
TACACS Server Authentication 283
TACACS Server Accounting 293
TACACS Server Authorization 295

CHAPTER 29 Traffic Mirroring Configuration 297
SPAN Overview 297
Port Mirroring Configuration 298
Port Mirroring Configuration 304

CHAPTER 30 Trigger Failover Configuration 309
Overview 309
Basic Configuration 309
Validation 310
Port-Channel Configuration 310
Validation 311

CHAPTER 31 User Configuration 313
Overview 313

CHAPTER 32 Using the Management Interface 315
Overview 315
Management Port 315
In-Band Ports 316

System Management Command Reference 319
Contents 319

CHAPTER 1 Access Control List Commands (Standard) 321
ip access-list standard 322
ip access-list standard filter 323
Ipv6 access-list standard 324
ipv6 access-list standard filter 325

CHAPTER 2 Access Control List Commands (XGS) 327
access-list logging cache-size 329
access-list logging rate-limit 330
arp access-group 331
arp access-list 332
arp access-list filter 333
arp access-list remark 335
arp access-list resequence 336
arp access-list response 337
clear access-list 339
clear access-list log-cache 340
clear arp access-list 341
clear ip access-list 342
clear ipv6 access-list 343
clear mac access-list 344
ip access-group 345
ip access-list 348
ip access-list default 349
ip access-list filter 350
ip access-list fragments 353
ip access-list icmp 354
ip access-list remark 359
ip access-list resequence 360
ip access-list tcp|udp 361
ipv6 access-group 366
ipv6 access-list 368
ipv6 access-list default 370
ipv6 access-list filter 371
ipv6 access-list fragments 374
ipv6 access-list icmpv6 375
ipv6 access-list remark 379
ipv6 access-list resequence 380
ipv6 access-list sctp 381
ipv6 access-list tcp|udp 384
line vty 390
mac access-group 391
mac access-list 393
mac access-list default 394
mac access-list filter 395
mac access-list remark 397
mac access-list resequence 398
show access-lists 399
show access-list log-cache 400
show arp access-lists 401
show ip access-lists 402
show ipv6 access-lists 403
show mac access-lists 404

© 2021 IP Infusion Inc. Proprietary

show running-config aclmgr 405
show running-config access-list 406
show running-config ipv6 access-list 407

CHAPTER 3 Authentication, Authorization and Accounting 409
aaa authentication login 410
aaa accounting default 411
aaa authentication login console 412
aaa authentication login default 413
aaa authentication login console fallback error 414
aaa authentication login default fallback error 415
aaa group server 416
aaa local authentication attempts max-fail 417
aaa local authentication unlock-timeout 418
debug aaa 419
server 420
show aaa authentication 421
show aaa authentication login 422
show aaa groups 423
show aaa accounting 424
show running-config aaa 425

CHAPTER 4 Basic Commands 427
banner motd 429
clock timezone 430
clock set 431
configure terminal 432
configure terminal force 433
copy running-config startup-config 434
crypto pki generate rsa common-name ipv4 435
debug nsm 436
disable 438
do 439
enable 440
enable password 441
end 442
exec-timeout 443
exit 444
help 445
history 446
hostname 447
line console 448
line vty (all line mode) 449
line vty (line mode) 450
logging cli 451
logout 452
max-session 453
ping 454

© 2021 IP Infusion Inc. Proprietary

ping (interactive) . . . 456
privilege level . . . 458
quit . . . 459
reload . . . 460
service advanced-vty . . . 461
service password-encryption . . . 462
service terminal-length . . . 463
show clock . . . 464
show cli . . . 465
show cli history . . . 466
show crypto csr . . . 467
show debugging nsm . . . 468
show list . . . 469
show logging cli . . . 470
show nsm client . . . 471
show nsm forwarding-timer . . . 472
show privilege . . . 473
show process . . . 474
show running-config . . . 475
show startup-config . . . 476
show timezone . . . 477
show users . . . 480
show version . . . 481
sys-reload . . . 483
sys-shutdown . . . 484
terminal length . . . 485
terminal monitor . . . 486
traceroute . . . 487
write . . . 488
write terminal . . . 489

CHAPTER 5 Chassis Management Module Commands . . . 491
cpu-core-usage . . . 492
debug cmm . . . 494
locator led . . . 495
show hardware-information . . . 496
show system-information . . . 510
system-load-average . . . 514

CHAPTER 6 Configuration Management . . . 517
copy empty-config startup-config . . . 518
copy running-config . . . 519
copy running-config (interactive) . . . 520
copy startup-config . . . 521
copy startup-config (interactive) . . . 522
copy system file . . . 523
copy system file (interactive) . . . 524
copy ftp startup-config . . . 525

© 2021 IP Infusion Inc. Proprietary

copy scp startup-config 526
copy sftp startup-config 527
copy tftp startup-config 528
copy http startup-config 529
copy ftp startup-config (interactive) 530
copy scp filepath 531
copy scp startup-config (interactive) 532
copy sftp startup-config (interactive) 533
copy tftp startup-config (interactive) 534
copy http startup-config (interactive) 535
copy file startup-config 536

CHAPTER 7 Common Management Layer Commands 537
abort transaction 538
cml logging 539
cml netconf translation 540
cmlsh transaction 541
cmlsh transaction limit 542
commit 543
debug cml 545
show max-transaction limit 546
show transaction current 547
show transaction last-aborted 548
show (xml|json) running-config 549

CHAPTER 8 DHCP Snooping Commands 551
debug ip dhcp snooping 552
ip dhcp snooping database 553
renew ip dhcp snooping binding database 554
show debugging ip dhcp snooping 555
show ip dhcp snooping arp-inspection statistics bridge 556
show ip dhcp snooping bridge 557
show ip dhcp snooping binding bridge 559

CHAPTER 9 DHCPv6 Prefix delegation Commands 561
ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER 562
ipv6 address PREFIX_FROM_SERVER X:X::X:X/M 563
ipv6 address autoconfig 564
show ipv6 dhcp interface 565

CHAPTER 10 Digital Diagnostic Monitoring Commands 567
clear ddm transceiver alarm 568
clear ddm transceiver alarm all 569
ddm monitor 570
ddm monitor all 571
ddm monitor interval 572
debug ddm 573
service unsupported-transceiver 574
show controller details 575

show supported-transceiver . . . 576
show interface transceiver details . . . 577

CHAPTER 11 Dynamic Host Configuration Protocol Client . . . 579
feature dhcp . . . 580
ip address dhcp . . . 581
ip dhcp client request . . . 582
ipv6 address dhcp . . . 583
ipv6 dhcp address-prefix-length . . . 584
ipv6 dhcp client request . . . 585
ipv6 dhcp client . . . 587
show ipv6 dhcp vendor-opts . . . 589

CHAPTER 12 Dynamic Host Configuration Protocol Relay . . . 591
clear ip dhcp relay option statistics . . . 592
clear ip dhcp relay statistics . . . 593
ip dhcp relay (configure mode) . . . 594
ip dhcp relay (interface mode) . . . 595
ip dhcp relay address . . . 596
ip dhcp relay information option . . . 597
ip dhcp relay information source-ip . . . 598
ip dhcp relay (L3VPN) . . . 599
ipv6 dhcp relay (configure mode) . . . 600
ipv6 dhcp relay (interface mode) . . . 601
ipv6 dhcp relay address . . . 602
ipv6 dhcp relay subscriber-id . . . 603
ipv6 dhcp relay (L3VPN) . . . 604
show ip dhcp relay . . . 605
show ip dhcp relay address . . . 607
show ip dhcp relay option statistics . . . 608
show ip dhcp relay statistics . . . 609
show ipv6 dhcp relay . . . 610
show ipv6 dhcp relay address . . . 611
show running-config dhcp . . . 612

CHAPTER 13 Domain Name System . . . 613
debug dns client . . . 614
ip domain-list . . . 615
ip domain-lookup . . . 616
ip domain-name . . . 617
ip host . . . 618
ip name-server . . . 619
show hosts . . . 620
show running-config dns . . . 622

CHAPTER 14 Interface Commands . . . 623
admin-group . . . 626
bandwidth . . . 627
bandwidth-measurement uni-available-bandwidth static . . . 628

© 2021 IP Infusion Inc. Proprietary

bandwidth-measurement uni-residual-bandwidth static 629
bandwidth-measurement uni-utilized-bandwidth static 630
clear hardware-discard-counters 631
clear interface counters 632
clear interface cpu counters 633
clear interface fec 634
clear ip prefix-list 635
clear ipv6 neighbors 636
clear ipv6 prefix-list 637
debounce-time 638
delay-measurement min-max-uni-link-delay 639
delay-measurement uni-delay-variation 640
delay-measurement uni-link-delay 641
description 642
duplex 643
fec 644
flowcontrol 645
hardware-profile portmode 647
if-arbiter 648
interface 649
ip address A.B.C.D/M 650
ip address dhcp 651
ip forwarding 652
ip prefix-list 653
ip proxy-arp 655
ip remote-address 656
ip unnumbered 657
ip vrf forwarding 658
ipv6 address 659
ipv6 forwarding 660
ipv6 prefix-list 661
ipv6 unnumbered 663
link-debounce-time 664
load interval 665
loopback 666
loss-measurement uni-link-loss 667
monitor speed 668
monitor queue-drops 669
monitor speed threshold 670
mtu 671
multicast 672
show flowcontrol 673
show hardware-discard-counters 674
show interface 676
show interface capabilities 678
show interface counters 680
show interface counters drop-stats 683

© 2021 IP Infusion Inc. Proprietary

show interface counters error-stats 686
show interface counters (indiscard-stats|outdiscard-stats) 687
show interface counters protocol 690
show interface counters queue-drop-stats 691
show interface counters queue-stats 692
show interface counters rate 694
show interface counters speed 696
show interface counters summary 697
show interface fec 699
show ip forwarding 701
show ip interface 702
show ip prefix-list 704
show ip route 705
show ip route A.B.C.D/M longer-prefixes 707
show ip vrf 716
show ipv6 forwarding 717
show ipv6 interface brief 718
show ipv6 route 720
show ipv6 prefix-list 722
show hosts 723
show running-config interface 725
show running-config interface ip 727
show running-config interface ipv6 728
show running-config ip 729
show running-config ipv6 730
show running-config prefix-list 731
shutdown 732
speed 733
switchport 735
switchport allowed ethertype 736
switchport protected 737
transceiver 738

CHAPTER 15 IP Service Level Agreements Commands 741
clear ip sla statistics 742
frequency 743
icmp-echo 744
ip sla 745
ip sla schedule 746
show ip sla statistics 747
show ip sla summary 749
show running-config ip sla 750
threshold 751
timeout 752

© 2021 IP Infusion Inc. Proprietary

CHAPTER 16 Linux Shell Commands 753

CHAPTER 17 Network Time Protocol 755
clear ntp statistics 756
debug ntp 757
feature ntp 758
ntp acl 759
ntp authenticate 760
ntp authentication-key 761
ntp discard 762
ntp enable 763
ntp logging 764
ntp master 765
ntp master stratum 766
ntp peer 767
ntp server 769
ntp source-interface 771
ntp sync-retry 772
ntp trusted-key 773
show ntp authentication-keys 774
show ntp authentication-status 775
show ntp logging-status 776
show ntp peer-status 777
show ntp peers 779
show ntp statistics 780
show ntp trusted-keys 782
show running-config ntp 783

CHAPTER 18 RADIUS 785
clear radius-server 786
debug radius 787
radius-server login host 788
radius-server login host acct-port 789
radius-server login host auth-port 790
radius-server login host key 791
radius-server login key 793
radius-server login timeout 794
show debug radius 795
show radius-server 796
show running-config radius 798

CHAPTER 19 Secure Shell 799
clear ssh host-key 800
clear ssh hosts 801
debug ssh server 802
feature ssh 803
show debug ssh-server 804
show running-config ssh server 805
show ssh host-key 806

© 2021 IP Infusion Inc. Proprietary

show ssh server . . . 808
show username . . . 809
ssh . . . 810
ssh6 . . . 811
ssh server algorithm encryption . . . 813
ssh keygen host . . . 815
ssh login-attempts . . . 816
ssh server port . . . 817
ssh server session-limit . . . 818
username sshkey . . . 819
username keypair . . . 820

CHAPTER 20 sFlow Commands . . . 821
clear sflow statistics . . . 822
debug sflow . . . 823
feature sflow . . . 824
sflow agent-ip . . . 825
sflow collector . . . 826
sflow poll-interval . . . 827
sflow sampling enable . . . 828
sflow sampling-rate . . . 829
show sflow . . . 830
show sflow interface . . . 832
show sflow statistics . . . 833

CHAPTER 21 Simple Network Management Protocol . . . 835
clear snmp hostconfig . . . 837
debug snmp . . . 838
debug snmp-server . . . 839
show running-config snmp . . . 840
show snmp . . . 841
show snmp community . . . 842
show snmp engine-id . . . 843
show snmp group . . . 844
show snmp host . . . 845
show snmp user . . . 846
show snmp view . . . 847
snmp-server community . . . 848
snmp-server contact . . . 849
snmp-server enable snmp . . . 850
snmp-server enable traps . . . 851
snmp-server host . . . 852
snmp-server location . . . 854
snmp-server tcp-session . . . 855
snmp-server user . . . 856
snmp-server view . . . 857

© 2021 IP Infusion Inc. Proprietary

CHAPTER 22 Software Monitoring and Reporting 859
copy techsupport 860
feature software-watchdog 861
show bootup-parameters 862
show cores 863
show software-watchdog status 864
show system log 867
show system login 869
show system reboot-history 870
show system resources 871
show system uptime 873
show techsupport 874
show techsupport status 876
software-watchdog 877
software-watchdog keep-alive-time 879

CHAPTER 23 Syslog 881
Syslog Severities 882
Log File Rotation 883
clear logging logfile 885
feature rsyslog 886
debug logging 887
log syslog 888
logging console 889
logging level 890
logging logfile 892
logging monitor 893
logging remote facility 894
logging remote server 895
logging timestamp 897
show logging 898
show logging last 900
show logging logfile 901
show logging logfile last-index 902
show logging logfile start-seqn end-seqn 903
show logging logfile start-time end-time 904
show running-config logging 905

CHAPTER 24 System Configure Mode Commands 907
forwarding custom-profile 908
forwarding profile 910
hardware-profile filter (XGS) 911
hardware-profile filter (Qumran) 912
hardware-profile flowcontrol (Qumran) 913
hardware-profile statistics (Qumran) 914
load-balance rtag7 915
load-balance rtag7 hash 918
load-balance rtag7 macro-flow 919

© 2021 IP Infusion Inc. Proprietary

show forwarding profile limit . . . 920
show hardware-profile filters . . . 922
snmp restart . . . 924

CHAPTER 25 TACACS+ . . . 925
add policy . . . 926
clear tacacs-server counters . . . 927
debug tacacs+ . . . 928
default . . . 929
deny . . . 930
feature dynamic-rbac enable . . . 931
feature tacacs+ . . . 932
permit . . . 933
policy . . . 934
role . . . 935
show debug tacacs+ . . . 936
show rbac-policy . . . 937
show rbac-role . . . 938
show running-config tacacs+ . . . 939
show tacacs-server . . . 940
tacacs-server login host . . . 942
tacacs-server login key . . . 944
tacacs-server login timeout . . . 945

CHAPTER 26 Telnet . . . 947
debug telnet server . . . 948
feature telnet . . . 949
show debug telnet-server . . . 950
show running-config telnet server . . . 951
show telnet-server . . . 952
telnet . . . 953
telnet6 . . . 954
telnet server port . . . 955
telnet server session-limit . . . 956

CHAPTER 27 Time Range Commands . . . 957
end-time (absolute) . . . 958
end-time after (relative) . . . 959
frequency . . . 960
frequency days (specific days) . . . 961
start-time (absolute) . . . 962
start-time after (relative) . . . 963
start-time now (current) . . . 964
time-range . . . 965

CHAPTER 28 Traffic Mirroring Commands . . . 967
monitor session . . . 968
monitor session shut . . . 969
source port . . . 970

© 2021 IP Infusion Inc. Proprietary

source vlan 971
destination port 972
no shut 973
shut 974
filter 975
description 977
remote destination 978
show monitor 979
show monitor session 981
show filter 984
show monitor running configuration 985

CHAPTER 29 Trigger Failover Commands 987
clear tfo counter 988
fog 989
fog tfc 990
fog type 991
link-type 992
show tfo 993
tfo 995

CHAPTER 30 User Management 997
clear aaa local user lockout username 998
clear line 999
clear user 1000
debug user-mgmt 1001
show user-account 1002
username 1003

CHAPTER 31 VLOG Commands 1005
show vlog all 1006
show vlog clients 1007
show vlog terminals 1008
show vlog virtual-routers 1009

Install, License, and Upgrade Configuration Guide 1013
Contents 1013

CHAPTER 1 Install, License, and Upgrade Configuration 1015

Install, License, and Upgrade Command Reference 1017
Contents 1017

CHAPTER 1 Licensing and Upgrade Commands 1019
license get 1020
license refresh 1021
license release 1022
show installers 1023
show license 1024
show sys-update details 1025

© 2021 IP Infusion Inc. Proprietary

sys-update commit 1026
sys-update delete 1027
sys-update get 1028
sys-update install 1029
sys-update list-version 1031
sys-update rollback 1032
sys-update un-install 1033

Layer 1 Configuration Guide 1037
Contents 1037

CHAPTER 1 Cross-Connect (XC) 1039
Overview 1039

CHAPTER 2 Cross-Connect (XC) Resiliency 1055
Overview 1055

Layer 1 Command Reference 1065
Contents 1065

CHAPTER 1 Port Based xConnect Commands 1067
backup 1068
cross-connect 1069
cross-connect switchover type revertive 1070
disable 1071
ep1 <interface_name> ep2 <interface_name> 1072
link-fault-pass-through enable 1073
show cross-connect 1074

Layer 2 Configuration Guide 1079
Contents 1079

CHAPTER 1 802.1X Configuration 1081
Switch Configuration 1081

CHAPTER 2 Disabling Native VLAN Configuration 1083
Topology 1083
Configuration 1083
Configuring acceptable-frame-type vlan-tagged on ingress interface 1085

CHAPTER 3 Disable Spanning Tree Configuration 1087
Disabling MSTP Configuration 1087
STP Configuration 1092
RSTP Configuration 1095

CHAPTER 4 Layer 2 Control Protocols Tunneling 1099
Overview 1099
L2CP Tunneling for Provider Bridging 1099
L2CP Tunneling for VPLS/VPWS/Hybrid (Bridge+VPWS) 1100
L2CP Behavior 1100
Default L2CP configuration 1101

© 2021 IP Infusion Inc. Proprietary

Operational Concepts and Scenarios 1102

CHAPTER 5 Link Aggregation Configuration 1107
Topology 1107
Dynamic LAG Configuration 1107
Static LAG Configuration 1109
Static LAG Minimum Link Configuration 1112
Static-LAG Minimum Bandwidth Configuration 1114
Dynamic-LAG Minimum Link Configuration 1117
Dynamic LAG Minimum Bandwidth Configuration 1121
LACP Minimum-Link, Minimum-Bandwidth Configurations on dynamic, static Channel-Groups with MC-LAG 1124
LACP Force-Up 1135
Validation 1137
LACP force-up with McLAG 1139
Validation 1142

CHAPTER 6 Link Layer Discovery Protocol Configuration 1149
Topology 1149
LLDPv2 (Interface Mode TLV) 1149
LLDPV2 (Global Mode TLV) 1156
LLDP-MED 1158

CHAPTER 7 MC-LAG Configuration 1165
Dynamic Configuration 1165
Static Configuration 1173
ARP ACL Configuration 1182
Disabling STP for MC-LAG 1188

CHAPTER 8 MSTP Configuration 1193
Configuration 1193

CHAPTER 9 Port Security Configuration 1207
Secured MACs Learned Dynamically 1207
Secured MAC Addresses Learned Statically 1209
Static Mode 1210
Port Security using MC-LAG 1212

CHAPTER 10 RPVST+ Configuration 1219
Topology 1219
Configuration 1219

CHAPTER 11 RSTP Configuration 1225
Configuration 1225

CHAPTER 12 Spanning Tree Protocol Configuration 1235
Configurations 1235

CHAPTER 13 VLAN Configuration 1243
Configuring VLAN Tags 1243

CHAPTER 14 VLAN Cross-Connect (XC) 1251
Overview 1251
Topology 1252
Configuration - Single-tagged VLAN 1252
Double-tagged VLAN 1256

CHAPTER 15 Unidirectional Link Detection Configuration 1261
Topology 1261
S1 1261
S2 1262
Validation 1262

Layer 2 Command Reference. 1265
Contents 1265

CHAPTER 1 Fundamental Layer 2 Commands 1267
errdisable cause 1268
errdisable link-flap-setting 1269
errdisable timeout 1270
show errdisable details 1271
show interface errdisable status 1272
show running-config switch 1273
show tcp 1275
watch static-mac-movement 1277

CHAPTER 2 Bridge Commands 1279
bridge acquire 1280
bridge address 1281
bridge ageing 1282
bridge forward-time 1283
bridge hello-time 1284
bridge mac-priority-override 1285
bridge max-age 1286
bridge max-hops 1287
bridge priority 1288
bridge shutdown 1289
bridge transmit-holdcount 1290
bridge-group 1291
bridge-group path-cost 1292
bridge-group priority 1293
clear allowed-ethertype 1294
clear mac address-table 1295
mac ageing display 1297
show allowed-ethertype 1298
show bridge 1299
show interface switchport 1300
show mac address-table count bridge 1302
show mac address-table bridge 1303
show mac-address-table bridge 1 learning 1305

© 2021 IP Infusion Inc. Proprietary

switchport 1306
switchport allowed ethertype 1307

CHAPTER 3 Spanning Tree Protocol Commands 1309
bridge cisco-interoperability 1311
bridge instance 1312
bridge instance priority 1313
bridge instance vlan 1314
bridge multiple-spanning-tree 1316
bridge protocol ieee 1317
bridge protocol mstp 1318
bridge protocol rstp 1319
bridge provider-rstp 1320
bridge rapid-spanning-tree 1321
bridge region 1322
bridge revision 1323
bridge spanning-tree 1324
bridge spanning-tree errdisable-timeout 1325
bridge spanning-tree force-version 1326
bridge spanning-tree pathcost 1327
bridge spanning-tree portfast 1328
bridge te-msti 1329
bridge te-msti vlan 1330
bridge-group instance 1331
bridge-group instance path-cost 1332
bridge-group instance priority 1333
bridge-group path-cost 1334
bridge-group priority 1335
bridge-group spanning-tree 1336
clear spanning-tree detected protocols 1337
clear spanning-tree statistics 1338
customer-spanning-tree customer-edge path-cost 1339
customer-spanning-tree customer-edge priority 1340
customer-spanning-tree forward-time 1341
customer-spanning-tree hello-time 1342
customer-spanning-tree max-age 1343
customer-spanning-tree priority 1344
customer-spanning-tree provider-edge path-cost 1345
customer-spanning-tree provider-edge priority 1346
customer-spanning-tree transmit-holdcount 1347
debug mstp 1348
show debugging mstp 1350
show spanning-tree 1351
show spanning-tree mst 1355
show spanning-tree statistics 1357
snmp restart mstp 1360
spanning-tree autoedge 1361

© 2021 IP Infusion Inc. Proprietary

spanning-tree edgeport 1362
spanning-tree guard 1363
spanning-tree instance restricted-role 1364
spanning-tree instance restricted-tcn 1365
spanning-tree link-type 1366
spanning-tree mst configuration 1367
spanning-tree bpdu-filter 1368
spanning-tree bpdu-guard 1369
spanning-tree restricted-domain-role 1370
spanning-tree restricted-role 1371
spanning-tree restricted-tcn 1372
spanning-tree te-msti configuration 1373
storm-control 1374
show strom-control 1377

CHAPTER 4 RPVST+ Commands 1379
bridge vlan 1380
bridge vlan priority 1381
bridge-group vlan 1382
bridge protocol rpvst+ 1383
bridge rapid-pervlan-spanning-tree 1384
show spanning-tree rpvst+ 1385
spanning-tree rpvst+ configuration 1389
spanning-tree vlan restricted-role 1390
spanning-tree vlan restricted-tcn 1391

CHAPTER 5 Link Aggregation Commands 1393
channel-group mode 1394
clear lacp 1396
debug lacp 1397
interface po 1398
interface sa 1399
lacp destination-mac 1400
lacp force-up 1401
lacp port-priority 1402
lacp system-priority 1403
lacp timeout 1404
port-channel load-balance 1405
port-channel min-bandwidth - dynamic LAG min-bandwidth 1406
port-channel min-links - dynamic LAG min-links 1407
port-channel min-bandwidth - static LAG min-bandwidth 1408
port-channel min-links - static LAG min-links 1409
show debugging lacp 1410
show etherchannel 1411
show lacp sys-id 1414
show lacp-counter 1415
show port etherchannel 1416
show static-channel-group 1419

© 2021 IP Infusion Inc. Proprietary

show static-channel load-balance 1420
snmp restart lacp 1421
static-channel-group 1422

CHAPTER 6 Multi-Chassis Link Aggregation Commands 1425
clear mcec statistics 1426
debug mcec 1427
domain-address 1428
domain hello timeout 1429
domain priority 1430
domain-system-number 1431
intra-domain-link 1432
intra-domain-peer 1433
mcec domain configuration 1434
mlag 1435
mode 1436
show mcec statistics 1437
show mlag detail 1439
show mlag domain 1441
show mlag phy-digest 1444
show spanning-tree mlag operational-config 1445
show spanning-tree mlag sync-detail 1446
switchover type 1447

CHAPTER 7 VLAN and Private VLAN Commands 1449
private-vlan association 1450
private-vlan community 1451
private-vlan isolated 1452
private-vlan primary 1453
show dtag vlan 1454
show vlan access-map 1455
show vlan 1456
show vlan brief 1458
show vlan classifier 1459
switchport access 1461
switchport hybrid 1462
switchport mode 1464
switchport mode access ingress-filter 1465
switchport mode hybrid acceptable-frame-type 1466
switchport mode hybrid ingress-filter 1467
switchport mode trunk ingress-filter 1468
switchport trunk allowed 1469
switchport trunk allowed vlan dtag 1471
switchport trunk native 1472
switchport mode private-vlan 1473
switchport private-vlan host-association 1474
switchport private-vlan mapping 1475
feature vlan classifier 1476

© 2021 IP Infusion Inc. Proprietary

vlan classifier activate 1477
vlan classifier group 1478
vlan classifier rule ipv4 1479
vlan classifier rule mac 1480
vlan classifier rule proto 1481
vlan database 1483
vlan dtag 1484
vlan state 1485
vlan VLAN_RANGE bridge 1486
vlan VLAN_RANGE type customer 1487
vlan VLAN_RANGE type service 1488
. 1489

CHAPTER 8 802.1x Commands 1491
auth-mac auth-fail-action 1492
auth-mac disable 1493
auth-mac dynamic-vlan-creation 1494
auth-mac enable 1495
auth-mac mac-aging 1496
auth-mac system-auth-ctrl 1497
debug dot1x 1498
dot1x initialize 1499
dot1x keytxenabled 1500
dot1x port-control 1501
dot1x protocol-version 1502
dot1x quiet-period 1503
dot1x reauthMax 1504
dot1x reauthentication 1505
dot1x system-auth-ctrl 1506
dot1x timeout re-authperiod 1507
dot1x timeout server-timeout 1508
dot1x timeout supp-timeout 1509
dot1x timeout tx-period 1510
ip radius source-interface 1511
radius-server dot1x deadtime 1512
radius-server dot1x host 1513
radius-server dot1x key 1515
radius-server dot1x retransmit 1516
radius-server dot1x timeout 1517
show debugging dot1x 1518
show dot1x 1519
snmp restart auth 1522

CHAPTER 9 Link Layer Discovery Protocol Commands 1523
lldp debug 1524
lldp ip 1525
lldp run 1526
lldp tlv 1527

© 2021 IP Infusion Inc. Proprietary

lldp tlv-select 1528
set lldp chassis-id-tlv 1530
set lldp disable 1531
set lldp enable 1532
set lldp locally-assigned 1533
set lldp management-address-tlv 1534
set lldp msg-tx-hold 1535
set lldp system-description 1536
set lldp system-name 1537
set lldp timer 1538
set lldp too-many-neighbors 1539
show lldp 1540
snmp restart lldp 1541

CHAPTER 10 Port Security Commands 1543
port-security 1544
show port-security 1545
switchport port-security 1546
switchport port-security logging 1547
switchport port-security mac-address 1548
switchport port-security maximum 1550

CHAPTER 11 VLAN Cross-Connect Commands 1551
cross-connect 1552
disable 1553
outer-vlan VLAN_RANGE2 (inner-vlan VLAN_RANGE2 |) 1555
show cross-connect 1556

CHAPTER 12 Unidirectional Link Detection Commands 1557
udld 1558
udld message-time 1559
udld mode 1560
udld state 1561
show udld 1562
show udld interface 1563

Layer 3 Unicast Configuration Guide 1567
Contents 1567

CHAPTER 1 Static Routes 1569
Configuration 1569

CHAPTER 2 RIP 1575
Enable RIP 1575
Specify RIP Version 1580
Authentication with a Single Key 1583
Text Authentication with Multiple Keys 1588
MD5 Authentication with Multiple Keys 1595

CHAPTER 3 RIPng 1603
Configuration 1603

CHAPTER 4 OSPFv2 1605
Enable OSPF on an Interface 1605
Set Priority 1609
Area Border Router 1614
Redistribute Routes into OSPF 1618
Cost 1620
Virtual Links 1625
OSPF Authentication 1630
Multiple OSPF Instances 1634
Multiple OSPF Instances on Same Subnet 1644
Multi-Area Adjacency Configuration 1647
LSA Throttling 1650

CHAPTER 5 OSPFv3 1673
Enable OSPFv3 on an Interface 1673
Set Priority 1676
Area Border Router 1680
Redistribute Routes into OSPFv3 1684
Cost 1689
Virtual Links 1699
Multiple Instances 1705
Graceful Restart 1719
Not-So-Stubby Area 1725
NSSA with the Summary Address Option 1728
NSSA with the Translator Role Option 1732
Link LSA Suppression 1736
Originate Type-7 LSAs and Translate to Type-5 1738
Summarize Intra-Area and External Routes 1742
Distribute List 1747

CHAPTER 6 IS-IS IPv4 1751
Enable IS-IS on an Interface 1751
Set Priority 1754
Dynamic hostname 1756
Redistribute Routes into IS-IS 1758
Metric 1764
L1-L2 Area Routing with a Single Instance 1771
L1-L2 Area Routing with Multiple Instances 1777
Route Leaking 1783
Route Summarization 1788
IS-IS Distance 1793
Passive Interface 1799
IS-IS IPv4 Loop-Free Alternate Fast Reroute 1804
Overview 1804
Basic Configuration 1805
Backup Path based on Route-Map Prefixes 1812

© 2021 IP Infusion Inc. Proprietary

LFA Tie-Breaker 1813
LFA Termination 1815
LFA For ECMP Paths 1818

CHAPTER 7 IS-IS IPv6 Configuration 1829
Enable IS-ISv6 on an Interface 1829
Set Priority 1831
Dynamic hostname 1833
Redistribute Routes into IS-IS 1836
Interface Metric 1838
Route Summarization 1842
Passive Interface 1847
Enable BFD over IS-ISv6 1852
Originate Default Route to ISISv6 Neighbors 1855

CHAPTER 8 IS-IS Graceful Restart Configuration 1859

CHAPTER 9 BGP 1861
Enable BGP Routers in the Same Autonomous System 1861
Enable BGP Between Different Autonomous Systems 1862
Route-Map 1864
Route Reflector 1866
Multiple Route Reflectors 1870
BGP Confederations 1881
Dynamic BGP Peering 1894
Enable eBGP Multihop 1924
Enable Peer Groups 1928
Route Redistribution in BGP 1939
Add Multiple Instances of the Same Autonomous System 1940
Remove the Multi-Exit Disc Attribute from Update Messages 1942
Removing Sent and Received MED values 1943
BGP Four-Byte Autonomous System 1945
4-Octet ASN Capability Enabled on R1 and R2 1945
4-Octet ASN Capability Enabled on R1 and Disabled on R2 1946
BGP Extended Community Attribute 1948
Nexthop Tracking 1968
Nexthop Tracking Delay Timer 1971
BGP Distance 1977
BGP Weight per Peer 1981
OSPF as PE-CE Protocol for VPNs 1984
BGP Multipath for IPv4 1987
Multipath eBGP 1990
Multipath eiBGP 1993
6BGP AS-PATH Multipath-relax 1998
BGP FIB Install (Selective Route Download) 2001
Route Target Constraint 2007
BGP Best Path Selection Process 2016
BGP Dampening 2018

© 2021 IP Infusion Inc. Proprietary

BGP Authentication 2023
BGP Unnumbered 2026
BGP Blackhole Community Attribute 2035

CHAPTER 10 BGP Labeled Unicast 2041
BGP Labeled Unicast as Transport 2041
BGP Labeled Unicast with Seamless MPLS 2052
BGP Labeled Unicast with Inter-AS 2071
BGP Peer Groups for Address-Family IPv4 Labeled Unicast 2083

CHAPTER 11 BGP Graceful Restart Configuration 2095

CHAPTER 12 Static Route Discard Configuration 2103
Overview 2103
IPv4 Route Discard 2103
IPv6 Route Discard 2106

CHAPTER 13 Route-map Continue Configuration 2111
Overview 2111
Topology 2111
Validation 2114

VRF Lite Configuration Guide 2119
Contents 2119

CHAPTER 1 VRF Configuration 2121
Overview 2121
Default VRF 2121
User-Defined VRF 2121

CHAPTER 2 OSPF Configuration 2123
Overview 2123
Configuration IPv4 VRF 2123

CHAPTER 3 RIP Configuration 2125
Configuration IPv4 VRF 2125
Configuration IPv6 VRF 2127

CHAPTER 4 ISIS Configuration 2131
Overview 2131
Topology 2131
Configuration IPv4 VRF 2131

CHAPTER 5 BGP Configuration 2135
Overview 2135
Configuration 2135

CHAPTER 6 Inter-VRF Route Leaking Configuration 2139
Overview 2139
Static Leaking 2139
Dynamic Leaking 2141

© 2021 IP Infusion Inc. Proprietary

Fundamental Layer 3 Command Reference 2147
Contents 2147

CHAPTER 1 Fundamental Layer 3 Commands 2149
automatic-router-id-selection enable 2150
clear ip route kernel 2151
clear ip route 2152
clear ip route vrf NAME 2153
clear router-id 2154
debug rib 2155
description 2157
fib retain 2158
ip route 2159
ip urpf enable 2161
ip urpf allow-default 2162
ip vrf 2163
maximum-paths 2164
max-static-routes 2165
router-id 2166
show debugging rib 2167
show ip rpf 2168
show ipv6 rpf 2170
show router-id 2172
show running-config router 2173
show running-config router-id 2174
show running-config urpf 2175
show running-config vrf 2176
snmp restart rib 2177
subscriber urpf enable 2178

CHAPTER 2 Route-Map Commands 2179
continue 2181
match as-path 2183
match community 2184
match extcommunity 2185
match interface 2186
match ip address 2187
match ip address prefix-list 2188
match ip next-hop 2189
match ip next-hop prefix-list 2190
match ip peer 2191
match ipv6 address 2192
match ipv6 address prefix-list 2193
match ipv6 next-hop 2194
match ipv6 next-hop prefix-list 2195
match ipv6 peer 2196
match metric 2197
match origin 2198

© 2021 IP Infusion Inc. Proprietary

match route-type 2199
match tag 2200
route-map 2201
set aggregator 2202
set as-path 2203
set atomic-aggregate 2204
set comm-list 2205
set community 2206
set dampening 2208
set extcommunity 2209
set interface null0 2211
set ip next-hop 2212
set ipv6 next-hop 2213
set level 2214
set local-preference 2215
set metric 2216
set metric-type 2217
set origin 2218
set originator-id 2219
set tag 2220
set vpnv4 next-hop 2221
set weight 2222
show route-map 2223
show running-config route-map 2224

Open Shortest Path First Command Reference 2225
Contents 2225

CHAPTER 1 OSPFv2 Commands 2227
area authentication 2230
area default-cost 2231
area interface 2232
area interface authentication 2233
area interface network-type 2234
area interface passive 2235
area filter-list 2236
area nssa 2237
area range 2239
area shortcut 2240
area stub 2241
area virtual-link 2242
auto-cost reference bandwidth 2245
bfd all-interfaces 2246
capability cspf 2247
capability lls 2248
capability opaque 2249
capability restart 2250

© 2021 IP Infusion Inc. Proprietary

capability traffic-engineering 2251
capability vrf-lite 2252
clear ip ospf 2253
compatible rfc1583 2254
debug ospf 2255
debug ospf database-timer rate-limit 2257
debug ospf events 2258
debug ospf ifsm 2259
debug ip ospf graceful-restart 2260
debug ip ospf lfa 2261
debug ip ospf redist 2262
debug ip ospf retransmission 2263
debug ospf lsa 2264
debug ospf nfsm 2265
debug ospf nsm 2266
debug ospf packet 2267
debug ospf rib 2268
debug ospf route 2269
default-information originate 2270
default-metric 2272
distance 2273
distribute-list 2274
enable db-summary-opt 2276
fast-reroute keep-all-paths 2277
fast-reroute tie-break 2278
host area 2280
ip ospf authentication 2281
ip ospf authentication-key 2282
ip ospf bfd 2284
ip ospf cost 2285
ip ospf database-filter 2286
ip ospf dead-interval 2287
ip ospf disable 2288
ip ospf fast-reroute per-prefix candidate disable 2289
ip ospf flood-reduction 2290
ip ospf hello-interval 2291
ip ospf multi-area 2292
ip ospf message-digest-key 2293
ip ospf mtu 2295
ip ospf mtu-ignore 2296
ip ospf network 2297
ip ospf priority 2298
ip ospf retransmit-interval 2299
ip ospf transmit-delay 2300
log-adjacency-changes 2301
max-concurrent-dd 2302
maximum-area 2303

© 2021 IP Infusion Inc. Proprietary

neighbor . . . 2304
network . . . 2305
ospf abr-type . . . 2307
ospf area-interface-config-mode . . . 2308
ospf flood-reduction . . . 2309
ospf restart grace-period . . . 2310
ospf restart helper . . . 2311
ospf router-id . . . 2312
overflow database . . . 2313
overflow database external . . . 2314
passive-interface . . . 2315
redistribute . . . 2316
restart ospf graceful . . . 2318
router ospf . . . 2319
show cspf rsvp forwarding-timer . . . 2320
show debugging ospf . . . 2321
show ip ospf . . . 2322
show ip ospf border-routers . . . 2326
show ip ospf database brief . . . 2327
show ip ospf database detail . . . 2329
show ip ospf igp-shortcut-lsp . . . 2336
show ip ospf igp-shortcut-route . . . 2337
show ip ospf interface . . . 2338
show ip ospf multi-area-adjacencies . . . 2341
show ip ospf neighbor . . . 2343
show ip ospf route . . . 2347
show ip ospf valid . . . 2349
show ip ospf virtual-links . . . 2350
show ip protocols . . . 2352
show ip route fast-reroute . . . 2354
shutdown . . . 2355
snmp restart ospf . . . 2356
summary-address . . . 2357
timers lsa arrival . . . 2358
timers spf exp . . . 2359
timers throttle lsa . . . 2360

CHAPTER 2 OSPFv3 Commands . . . 2361
abr-type . . . 2363
area default-cost . . . 2364
area nssa . . . 2365
area range . . . 2367
area stub . . . 2368
area virtual-link . . . 2369
auto-cost reference bandwidth . . . 2371
bfd all-interfaces . . . 2372
capability restart . . . 2373

© 2021 IP Infusion Inc. Proprietary

clear ipv6 ospf process 2374
debug ipv6 ospf 2375
debug ipv6 ospf bfd 2376
debug ipv6 ospf events 2377
debug ipv6 ospf ifsm 2378
debug ipv6 ospf lfa 2379
debug ipv6 ospf lsa 2380
debug ipv6 ospf nfsm 2381
debug ipv6 ospf nsm 2382
debug ipv6 ospf packet 2383
debug ipv6 ospf retransmission 2384
debug ipv6 ospf rib 2385
debug ipv6 ospf route 2386
default-information originate 2387
default-metric 2389
distance 2390
distribute-list 2391
enable db-summary-opt 2393
fast-reroute keep-all-paths 2394
fast-reroute tie-break 2395
ipv6 ospf bfd 2397
ipv6 ospf cost 2398
ipv6 ospf dead-interval 2399
ipv6 ospf display route single-line 2400
ipv6 ospf hello-interval 2401
ipv6 ospf link-lsa-suppression 2402
ipv6 ospf mtu-ignore 2403
ipv6 ospf neighbor 2404
ipv6 ospf network 2406
ipv6 ospf priority 2407
ipv6 ospf restart grace-period 2408
ipv6 ospf restart helper 2409
ipv6 ospf restart planned-only 2410
ipv6 ospf retransmit-interval 2411
ipv6 ospf transmit-delay 2412
ipv6 router ospf 2413
ipv6 te-metric 2415
log-adjacency-changes 2416
max-concurrent-dd 2417
passive-interface 2418
redistribute 2419
restart ipv6 ospf graceful 2421
router-id 2422
router ipv6 ospf 2423
show debugging ipv6 ospf 2424
show ipv6 ospf 2425
show ipv6 ospf database 2426

© 2021 IP Infusion Inc. Proprietary

show ipv6 ospf interface 2430
show ipv6 ospf neighbor 2432
show ipv6 ospf route 2435
show ipv6 route fast-reroute 2437
show ipv6 ospfv3 topology 2438
show ipv6 ospf virtual-links 2440
show ipv6 vrf 2442
shutdown 2443
snmp restart ospf6 2444
summary-address 2445
timers spf exp 2447

CHAPTER 3 OSPF VPN Commands 2449
capability vrf-lite 2450
router ospf vrf 2451
domain-id 2452

Border Gateway Protocol Command Reference 2455
Contents 2455

CHAPTER 1 BGP Commands 2457
address-family 2461
aggregate-address 2463
auto-summary 2464
bgp aggregate-nexthop-check 2465
bgp always-compare-med 2466
bgp as-local-count 2467
bgp bestpath as-path ignore 2468
bgp bestpath as-path multipath-relax 2469
bgp bestpath compare-confed-aspath 2470
bgp bestpath compare-routerid 2471
bgp bestpath dont-compare-originator-id 2472
bgp bestpath med 2473
bgp bestpath tie-break-on-age 2475
bgp client-to-client reflection 2476
bgp cluster-id 2477
bgp confederation identifier 2478
bgp confederation peers 2479
bgp config-type 2480
bgp dampening 2481
bgp default local-preference 2483
bgp deterministic-med 2484
bgp enforce-first-as 2485
bgp extended-asn-cap 2486
bgp fast-external-failover 2487
bgp graceful-restart 2488
bgp g-shut 2490
bgp g-shut-capable 2491

© 2021 IP Infusion Inc. Proprietary

bgp g-shut-local-preference 2492
bgp log-neighbor-changes 2493
bgp nexthop-trigger delay 2495
bgp nexthop-trigger enable 2496
bgp rfc1771-path-select 2497
bgp rfc1771-strict 2498
bgp router-id 2499
bgp scan-time 2500
bgp update-delay 2503
clear bgp (A.B.C.D|X:X::X:X) 2504
clear bgp * 2505
clear bgp <1-4294967295> 2507
clear bgp dampening 2509
clear bgp external 2510
clear bgp flap-statistics 2512
clear bgp peer-group 2513
clear bgp statistics 2515
clear ip bgp A.B.C.D 2516
clear ip bgp A.B.C.D vrf 2518
clear ip bgp table-map 2519
debug bgp 2520
distance bgp 2522
exit-address-family 2523
ip as-path access-list 2524
ip community-list <1-99> 2525
ip community-list <100-500> 2526
ip community-list expanded 2527
ip community-list standard 2528
ip community-list WORD 2529
ip extcommunity-list <1-99> 2530
ip extcommunity-list <100-500> 2531
ip extcommunity-list expanded 2532
ip extcommunity-list standard 2533
l2vpn-unnumbered-mode 2534
match ip peer 2535
max-paths 2536
neighbor activate 2537
neighbor advertisement-interval 2538
neighbor allowas-in 2539
neighbor as-origination-interval 2541
neighbor attribute-unchanged 2542
neighbor authentication-key 2543
neighbor capability dynamic 2544
neighbor capability graceful-restart 2545
neighbor capability orf prefix-list 2546
neighbor capability route-refresh 2548
neighbor collide-established 2549

© 2021 IP Infusion Inc. Proprietary

neighbor default-originate 2550
neighbor description 2551
neighbor disallow-infinite-holdtime 2552
neighbor distribute-list 2553
neighbor dont-capability-negotiate 2554
neighbor ebgp-multihop 2555
neighbor enforce-multihop 2556
neighbor fall-over bfd 2557
neighbor filter-list 2558
neighbor g-shut 2559
neighbor g-shut-timer 2560
neighbor limit 2561
neighbor local-as 2562
neighbor maximum-prefix 2563
neighbor next-hop-self 2564
neighbor optional-as 2565
neighbor override-capability 2566
neighbor passive 2567
neighbor peer-group 2568
neighbor WORD peer-group range 2571
neighbor port 2572
neighbor prefix-list 2573
neighbor remote-as 2575
neighbor remove-private-AS 2577
neighbor restart-time 2578
neighbor route-map 2579
neighbor route-reflector-client 2581
neighbor route-server-client 2582
neighbor send-community 2583
neighbor shutdown 2584
neighbor soft-reconfiguration inbound 2585
neighbor strict-capability-match 2586
neighbor timers 2587
neighbor unsuppress-map 2589
neighbor update-source 2590
neighbor version 2591
neighbor weight 2592
neighbor WORD peer-group 2594
network 2595
network synchronization 2597
redistribute 2598
restart bgp graceful 2600
router bgp 2601
snmp restart bgp 2602
synchronization 2603
timers bgp 2604
v4-unnumbered-mode 2605

© 2021 IP Infusion Inc. Proprietary

undebug bgp 2606
bgp unnumbered-mode 2607

CHAPTER 2 BGP Labeled Unicast Commands 2609
address-family labeled-unicast 2610
allocate-label 2611
clear ip bgp A.B.C.D ipv4 labeled-unicast 2612
clear ip bgp peer-group WORD ipv4 labeled-unicast 2613
clear ip bgp * ipv4 labeled-unicast 2614

CHAPTER 3 BGP Virtual Private Network Commands 2615
bgp inbound-route-filter 2616
clear bgp * l2vpn vpls 2617
clear ip bgp * vpnv4 2618
clear bgp <1-4294967295> l2vpn vpls 2619
clear ip bgp <1-4294967295> vpnv4 2620
clear bgp A.B.C.D l2vpn vpls 2621
clear ip bgp A.B.C.D vpnv4 2622
debug bgp mpls 2623
export map 2624
import map 2625
ip vrf 2626
neighbor allow-ebgp-vpn 2627
neighbor as-override 2628
neighbor send-community 2629
neighbor soo 2630
rd (route distinguisher) 2631
route-target 2632

CHAPTER 4 BGP Show Commands 2633
show bgp 2635
show bgp A.B.C.D 2636
show bgp A.B.C.D/M 2638
show bgp client 2639
show bgp community 2640
show bgp community-list 2642
show bgp dampening dampened-paths 2643
show bgp dampening flap-statistics 2644
show bgp dampening parameters 2647
show bgp filter-list 2649
show bgp inconsistent-as 2651
show bgp ipv6 2652
show bgp ipv6 peer-group 2655
show bgp l2vpn vpls 2656
show bgp neighbors 2659
show bgp neighbors advertised-routes 2663
show bgp neighbors received prefix-filter 2664
show bgp neighbors received-routes 2665

© 2021 IP Infusion Inc. Proprietary

show bgp neighbors routes . . . 2666
show bgp nexthop-tracking . . . 2668
show bgp nexthop-tree-details . . . 2670
show bgp paths . . . 2671
show bgp prefix-list . . . 2672
show bgp quote-regexp . . . 2673
show bgp regexp . . . 2674
show bgp route-map . . . 2675
show bgp statistics . . . 2676
show bgp summary . . . 2678
show bgp X:X::X:X . . . 2681
show bgp X:X::X:X/M longer prefixes . . . 2682
show debugging bgp . . . 2683
show ip bgp . . . 2684
show ip bgp cidr-only . . . 2687
show ip bgp community-info . . . 2689
show ip bgp peer-group . . . 2690
show ip bgp peer-group vrf all . . . 2691
show ip bgp rtfilter all . . . 2692
show ip bgp scan . . . 2693
show ip bgp vpnv4 . . . 2694
show ip extcommunity-list . . . 2698
show ip protocols . . . 2699
show ip vrf . . . 2701
show running-config as-path access-list . . . 2702
show running-config community-list . . . 2703

Appendix 5 Regular Expressions . . . 2705

Intermediate System to Intermediate System Command Reference 2707

Contents . . . 2707

CHAPTER 1 IS-IS Commands . . . 2709
accept-lifetime . . . 2712
address-family ipv6 . . . 2714
adjacency-check . . . 2715
area-password . . . 2716
authentication key-chain . . . 2717
authentication mode . . . 2718
authentication send-only . . . 2719
bfd all-interfaces . . . 2720
capability cspf . . . 2721
clear clns neighbors . . . 2722
clear clns is-neighbors . . . 2723
clear ip isis route . . . 2724
clear isis adjacency . . . 2725
clear isis counter . . . 2726
clear isis interface counter . . . 2727

© 2021 IP Infusion Inc. Proprietary

clear isis process 2728
debug isis 2729
default-information originate 2731
distance (IPv4) 2732
distance (IPv6) 2733
domain-password 2734
dynamic-hostname 2735
fast-reroute per-prefix 2736
fast-reroute terminate-hold-on interval 2737
fast-reroute tie-break 2738
ignore-lsp-errors 2740
ip router isis 2741
ipv6 router isis 2742
isis authentication key-chain 2743
isis authentication mode md5 2744
isis authentication send-only 2745
isis bfd 2746
isis circuit-type 2747
isis csnp-interval 2748
isis fast-reroute per-prefix candidate disable 2749
isis hello-interval 2750
isis hello-multiplier 2751
isis hello padding 2752
isis lsp-interval 2753
isis mesh-group 2754
isis metric 2755
isis network 2756
isis password 2757
isis priority 2758
isis retransmit-interval 2759
ispf 2760
isis wait-timer 2761
isis wide-metric 2762
isis tag 2763
isis te-metric 2764
is-type 2765
key chain 2766
key 2767
key-string 2768
key-string encrypted 2769
lsp-gen-interval 2770
lsp-mtu 2771
lsp-refresh-interval 2772
max-area-address 2773
max-lsp-lifetime 2774
metric-style 2775
mpls traffic-eng 2777

© 2021 IP Infusion Inc. Proprietary

mpls traffic-eng router-id . . . 2778
net . . . 2779
passive-interface . . . 2780
prc-interval-exp . . . 2781
redistribute . . . 2782
redistribute isis . . . 2784
redistribute isis WORD . . . 2785
router isis . . . 2786
send-lifetime . . . 2787
snmp restart isis . . . 2789
spf-interval-exp . . . 2790
summary-address . . . 2791
summary-prefix . . . 2792

CHAPTER 2 IS-IS Graceful Restart Commands . . . 2793
capability restart graceful . . . 2794
isis restart grace-period . . . 2795
isis restart-hello-interval . . . 2796
isis restart helper . . . 2797
isis restart suppress-adjacency . . . 2798
restart isis graceful . . . 2799
restart-timer . . . 2800

CHAPTER 3 IS-IS Show Commands . . . 2801
show clns is-neighbors . . . 2802
show clns neighbors . . . 2804
show cspf rsvp forwarding-timer . . . 2806
show debugging isis . . . 2807
show ip isis igp-shortcut-lsp . . . 2808
show ip isis route . . . 2809
show ip isis route igp-shortcut . . . 2811
show ip protocols . . . 2813
show ip route fast-reroute . . . 2814
show ip isis route fast-reroute . . . 2815
show ip isis lfa-config . . . 2816
show isis counter . . . 2817
show isis database . . . 2818
show isis interface . . . 2821
show isis spf-logs . . . 2824
show isis topology . . . 2825
show running-config interface isis . . . 2827
show running-config router isis . . . 2828

Neighbor Discovery Command Reference . . . 2829
Contents . . . 2829

CHAPTER 1 Neighbor Discovery Commands . . . 2831
arp-ageing-timeout . . . 2832

© 2021 IP Infusion Inc. Proprietary

arp-reachable-time 2833
clear arp 2834
clear ipv6 neighbors 2835
debug ip arp 2836
debug ipv6 nd 2837
ip arp 2838
ip arp vrf 2839
ipv6 nd current-hoplimit 2840
ipv6 nd link-mtu 2841
ipv6 nd managed-config-flag 2842
ipv6 nd other-config-flag 2843
ipv6 nd prefix 2844
ipv6 nd ra-interval 2846
ipv6 nd ra-lifetime 2847
ipv6 nd reachable-time 2848
ipv6 nd retransmission-time 2849
ipv6 nd suppress-ra 2850
ip proxy-arp 2851
ipv6 neighbor 2852
nd-ageing-timeout 2853
nd-reachable-time 2854
no debug all 2855
show arp 2856
show debugging ip arp 2858
show debugging ipv6 nd 2859
show ipv6 neighbors 2860

Multicast Configuration Guide 2865
Contents 2865

CHAPTER 1 IGMP Configuration 2867
IGMP Versions 2867
IGMP Operation 2867
Topology 2868
IGMP Configuration 2869

CHAPTER 2 IGMP Proxy Configuration 2877
Terminology 2877
Enabling IP Multicast Routing 2879
Enabling Proxy upstream interface 2879
Enabling Proxy downstream interface 2879
Enabling Unsolicited report interval 2881

CHAPTER 3 PIM Sparse Mode Configuration 2885
Terminology 2885
Data Flow from Source to Receivers in PIM-SM Network Domain 2886
PIM-SM Configuration 2888
Enabling IP Multicast Routing 2888

Configuring Rendezvous Point Statically 2889
Configure Rendezvous Point Dynamically Using Bootstrap Router Method 2892
Anycast-RP Configuration 2897

CHAPTER 4 PIM Dense Mode Configuration 2901
Terminology 2901
Configuration 2901
Enabling IP Multicast Routing 2902
Enabling PIM-DM 2903

CHAPTER 5 IGMP Snooping Configuration 2905
Configuration 2905

CHAPTER 6 MSDP Configuration 2909
Overview 2909
Caching SA state 2909
MSDP Mesh Group 2909
MSDP Default Peer 2910
Configure PIM-SM 2910
Configure MSDP 2910

Multicast Routing Information Base Command Reference. 2919
Contents 2919

CHAPTER 1 Multicast Commands 2921
clear ip mroute 2922
debug ip mrib 2923
ip mroute 2924
ip multicast route-limit 2925
ip multicast ttl-threshold 2926
ip multicast-routing 2927
ipv6 mroute 2928
show debugging ip mrib 2929
show ip mroute 2930
show ip mvif 2933
show running-config interface multicast 2935
snmp restart mribd 2936

CHAPTER 2 L3 IGMP Multicast Commands 2937
clear ip igmp 2938
debug ip igmp 2939
ip igmp 2941
ip igmp access-group 2942
ip igmp immediate-leave 2943
ip igmp join-group 2944
ip igmp last-member-query-count 2945
ip igmp last-member-query-interval 2946
ip igmp limit 2947
ip igmp mroute-proxy 2948
ip igmp offlink 2949

© 2021 IP Infusion Inc. Proprietary

ip igmp proxy-service 2950
ip igmp proxy unsolicited-report-interval 2951
ip igmp querier-timeout 2952
ip igmp query-interval 2953
ip igmp query-max-response-time 2954
ip igmp ra-option 2955
ip igmp robustness-variable 2956
ip igmp ssm-map enable 2957
ip igmp ssm-map static 2958
ip igmp static-group 2959
ip igmp startup-query-count 2960
ip igmp startup-query-interval 2961
ip igmp version 2962
show debugging ip igmp 2963
show ip igmp groups 2964
show ip igmp interface 2966
show ip igmp proxy 2968
show ip igmp ssm-map 2970
show running-config interface igmp 2971

CHAPTER 3 L2 IGMP Snooping Multicast Commands 2973
igmp snooping 2974
igmp snooping fast-leave 2975
igmp snooping mrouter 2976
igmp snooping querier 2977
igmp snooping report-suppression 2978
igmp snooping static-group 2979
show igmp snooping interface 2980
show igmp snooping groups 2982
show igmp snooping mrouter 2985
show igmp snooping statistics 2986

CHAPTER 4 PIMv4 Commands 2987
clear ip mroute 2989
clear ip pim sparse-mode 2991
debug ip pim 2992
debug ip pim packet 2993
debug pim all 2994
debug ip pim timer assert 2995
debug ip pim timer bsr 2996
debug ip pim timer hello 2997
debug ip pim timer joinprune 2999
debug ip pim timer register 3001
ip pim 3002
ip pim accept-register 3003
ip pim anycast-rp 3004
ip pim bsr-border 3005
ip pim bsr-candidate 3006

© 2021 IP Infusion Inc. Proprietary

ip pim cisco-register-checksum . . . 3007
ip pim dr-priority . . . 3008
ip pim exclude-genid . . . 3009
ip pim hello-holdtime . . . 3010
ip pim hello-interval . . . 3011
ip pim ignore-rp-set-priority . . . 3012
ip pim jp-timer . . . 3013
ip pim neighbor-filter . . . 3014
ip pim passive . . . 3015
ip pim propagation-delay . . . 3016
ip pim register-rate-limit . . . 3017
ip pim register-rp-reachability . . . 3018
ip pim register-source . . . 3019
ip pim register-suppression . . . 3020
ip pim router-id . . . 3021
ip pim rp-address . . . 3022
ip pim rp-candidate . . . 3024
ip pim rp-register-kat . . . 3025
ip pim spt-threshold . . . 3026
ip pim ssm . . . 3027
ip pim state-refresh origination-interval . . . 3028
ip pim unicast-bsm . . . 3029
show debugging ip pim . . . 3030
show debugging pim . . . 3031
show ip pim bsr-router . . . 3032
show ip pim interface . . . 3034
show ip pim local-members . . . 3036
show ip pim mroute . . . 3037
show ip pim neighbor . . . 3039
show ip pim nexthop . . . 3042
show ip pim rp-hash . . . 3043
show ip pim rp mapping . . . 3044
snmp restart pim . . . 3045
undebug all ip pim . . . 3046

Carrier Ethernet Configuration Guide . . . 3049
Contents . . . 3049

CHAPTER 1 Link Layer Discovery Protocol Configuration . . . 3051
Topology . . . 3051
Interface Mode TLV . . . 3051
Global Mode TLV . . . 3060
LLDP-MED . . . 3063

CHAPTER 2 G.8032 ERPS Version 2 . . . 3069
Topology . . . 3069
Validation . . . 3077
Sub-ring with Virtual Channel . . . 3081

© 2021 IP Infusion Inc. Proprietary

Sub-ring without Virtual Channel on a LAG interface 3101

CHAPTER 3 Ethernet CFM Configurations 3121
Continuity Check Message(CCM) 3121

CHAPTER 4 Provider Bridging Configuration 3127
Provider Bridging with Customer Hosts 3127
Provider Bridging with Customer Equipment 3131
Provider Bridging with VLAN Translation 3139
Layer 2 Protocol Tunneling (L2PT/L2CP Tunneling) 3147

Carrier Ethernet Command Reference 3151
Contents 3151

CHAPTER 1 CFM Commands 3153
cc interval 3154
cc multicast 3155
clear ethernet cfm maintenance-point remote 3156
clear ethernet cfm traceroute-cache 3157
ethernet cfm domain-type 3158
ethernet cfm mep 3159
exit-ether-ma-mep-mode 3160
exit-ether-ma-mode 3161
mep crosscheck 3162
mep lowest-priority-defect 3163
ping ethernet mac 3164
service ma-type 3165
show ethernet cfm errors 3166
show ethernet cfm ma status 3167
show ethernet cfm maintenance-points local mep 3168
show ethernet cfm maintenance-points local mip 3170
show ethernet cfm maintenance-points remote 3171
show running-config cfm 3173
traceroute ethernet 3174

CHAPTER 2 G.8032 ERPS Version 2 Commands 3175
g8032 physical-ring 3176
force-switch|manual-switch 3177
g8032 erp-instance 3178
g8032 profile 3179
level 3180
non-virtual-channel 3181
physical-ring 3182
profile name 3183
ring-id 3184
ring-type 3185
raps-channel-vlan 3186
data-traffic-vlan 3187
rpl role 3188

show g8032 erp-instance . . . 3189
show g8032 physical-ring . . . 3190
show g8032 profile . . . 3191
switching-mode . . . 3192
tcn-propogation . . . 3193
tcn-propagation-instance . . . 3194
timer . . . 3195
virtual-channel . . . 3196

CHAPTER 3 Provider Bridging Commands . . . 3197
bridge protocol provider-mstp . . . 3198
bridge protocol provider-rstp . . . 3199
cvlan registration table . . . 3200
cvlan svlan . . . 3201
show cvlan registration table . . . 3203
switchport customer-edge . . . 3204
switchport customer-edge default-svlan . . . 3205
switchport customer-edge hybrid . . . 3206
switchport customer-edge trunk . . . 3207
switchport customer-edge vlan registration . . . 3208
switchport customer-network vlan . . . 3209
switchport customer-network vlan translation . . . 3210
switchport ethertype . . . 3212
switchport mode . . . 3213
switchport mode ingress-filter . . . 3214
switchport mode customer-edge . . . 3215
switchport mode customer-edge hybrid acceptable-frame-type . . . 3216
switchport provider-edge . . . 3217
switchport provider-network vlan translation . . . 3218
vlan type customer . . . 3220
vlan type service . . . 3221
vlan type . . . 3222

CHAPTER 1 Link Layer Discovery Protocol v2 Commands . . . 3225
clear lldp counters . . . 3226
lldp-agent . . . 3227
debug lldp . . . 3228
lldp run . . . 3229
lldp tlv basic-mgmt . . . 3230
lldp tlv med . . . 3231
lldp tlv ieee-8021-org-specific . . . 3232
lldp tlv ieee-8023-org-specific . . . 3233
lldp tlv-select basic-mgmt . . . 3234
lldp tlv-select ieee-8021-org-specific . . . 3235
lldp tlv-select ieee-8023-org-specific . . . 3236
set lldp agt-circuit-id . . . 3237
set lldp chassis-id-tlv . . . 3238
set lldp chassis locally-assigned . . . 3239

© 2021 IP Infusion Inc. Proprietary

set lldp disable 3240
set lldp enable 3241
set lldp locally-assigned 3242
set lldp management-address-tlv 3243
set lldp med-devtype 3244
set lldp msg-tx-hold 3245
set lldp port-id-tlv 3246
set lldp timer 3247
set lldp too-many-neighbors 3249
set lldp tx-fast-init 3250
set lldp tx-max-credit 3251
show debugging lldp 3252
show lldp neighbors 3253
show lldp interface 3256
snmp restart lldp 3258

CHAPTER 2 Link Layer Discovery Protocol Commands 3259
lldp debug 3260
lldp disable default-agent 3261
lldp ip 3262
lldp tlv 3263
set lldp chassis-id-tlv 3264
set lldp disable 3265
set lldp enable 3266
set lldp locally-assigned 3267
set lldp management-address-tlv 3268
set lldp msg-tx-hold 3269
set lldp system-description 3270
set lldp system-name 3271
set lldp timer 3272
set lldp too-many-neighbors 3273
show lldp 3274
snmp restart lldp 3275

Data Center Bridging Configuration Guide 3279
Contents 3279

CHAPTER 1 Enhanced Transmission Selection Configuration 3281
Configuring a Bridge and Interface for ETS 3281
Configuring Priorities and Bandwidth for ETS 3281

CHAPTER 2 Priority-based Flow Control Configuration 3283
Configuring a Bridge and Interface for PFC 3283
Configuring Priorities and Link Delay Allowance for PFC 3283
Configuring Application Priority for PFC 3285

CHAPTER 3 Quantized Congestion Notification Configuration 3287
Configuring a Bridge and Interface for QCN 3287
Enable a CNPV and Create a CP 3288

CHAPTER 4 DCBx Configuration 3291
Configuring ETS Parameter Exchange 3291
Configuring PFC Parameter Exchange 3293

Data Center Bridging Command Reference 3297
Contents 3297

CHAPTER 1 Enhanced Transmission Selection Commands 3299
application-priority advertise-local-config 3300
application-priority enable (interface) 3301
application-priority enable (switch) 3302
bandwidth-percentage 3303
data-center-bridging 3304
dcbx enable 3305
enhanced-transmission-selection accept-peer-config 3306
enhanced-transmission-selection advertise-local-config 3307
enhanced-transmission-selection (switch) 3308
enhanced-transmission-selection (interface) 3309
ethertype 3310
max-traffic-class-group 3312
show application-priority bridge 3313
show application-priority interface 3314
show data-center-bridging 3315
show enhanced-transmission-selection bridge 3317
show enhanced-transmission-selection interface 3319
tcp 3321
traffic-class-group 3322
udp 3323

CHAPTER 2 Quantized Congestion Notification Commands 3325
cnpv 3326
cp enable 3327
defense-mode cnpv 3328
qcn enable 3330
show qcn configuration 3331
show qcn cnpv 3333
show qcn cp 3335

CHAPTER 3 Priority-based Flow Control Commands 3337
priority-flow-control accept-peer-config 3338
priority-flow-control advertise-local-config 3339
priority-flow-control enable 3340
priority-flow-control cap 3341
priority-flow-control enable priority 3342
priority-flow-control link-delay-allowance 3343
priority-flow-control mode 3344
show priority-flow-control details 3345
show priority-flow-control statistics 3347

© 2021 IP Infusion Inc. Proprietary

Virtual Router Redundancy Protocol Configuration Guide 3351
Contents 3351

CHAPTER 1 VRRP Configuration 3353
Terminology 3353
VRRP Process 3353
One Virtual Router 3355
Two Virtual Routers 3358
Two Backup Routers 3363
Interface Tracking 3368
VRRP-Backward Compatibility 3375
Redundancy Using VRRP and OSPF: Two Virtual Routers 3378

Virtual Router Redundancy Protocol Command Reference 3381
Contents 3381

CHAPTER 1 VRRP Commands 3383
accept-mode 3384
advertisement-interval 3385
authentication text 3386
circuit-failover 3387
debug vrrp 3388
disable 3389
enable 3390
l2-move allow-first-frame 3391
operational-ip 3392
preempt-mode 3393
priority 3394
router vrrp 3395
show debugging vrrp 3396
show running-config router vrrp 3397
show vrrp 3398
show vrrp summary 3400
show vrrp <1-255> 3401
show vrrp (global | ipv4) statistics 3403
snmp restart vrrp 3404
switch-back-delay 3405
undebug vrrp 3406
virtual-ip 3407
vrrp compatible-v2 3408
vrrp vmac 3409

Bidirectional Forwarding Detection Configuration Guide 3413
Contents 3413

CHAPTER 1 Base BFD Configuration 3415
Validation 3419
Validation: 3421

CHAPTER 2 BFD Protocol Configurations 3425
OSPF—BFD Single-Hop Session 3425
OSPF—BFD Multi-Hop Session 3434
BFD Configuration in IS-IS 3437
BFD Configuration in BGP 3440
BFD Configuration in RIP 3447

CHAPTER 3 BFD Static Route Configuration 3451

CHAPTER 4 BFD Authentication 3455
Overview 3455

CHAPTER 5 BFD with VRF Configuration 3463
Topology 3463
Validation 3465
BFD Over Static Routing IPv4 and IPv6 3471
Validation 3472

Bidirectional Forwarding Detection Command Reference 3477
Contents 3477

CHAPTER 1 Bidirectional Forwarding Commands 3479
accept-lifetime 3480
bfd auth type 3482
bfd 3483
bfd echo 3484
bfd echo interval 3485
bfd echo ipv4 source 3486
bfd-firmware 3487
bfd interval 3488
bfd multihop-peer 3489
bfd multihop-peer A.B.C.D interval 3491
bfd multihop-peer X:X::X:X interval 3492
bfd notification 3493
bfd session 3494
bfd slow-timer 3495
debug bfd 3496
hardware-profile micro-bfd 3497
key 3498
key chain 3499
key-string 3500
key-string encrypted 3501
send-lifetime 3502
show bfd 3503
show bfd interface 3504
show bfd session 3506
show bfd session A.B.C.D 3510
show bfd session ipv6 3513
show debugging bfd 3516

© 2021 IP Infusion Inc. Proprietary

snmp restart bfd 3517

CHAPTER 2 Protocol Commands for BFD 3519
area virtual-link 3520
bfd all-interfaces 3521
debug bgp bfd 3522
debug isis bfd 3523
debug ospf bfd 3524
ip ospf bfd 3525
isis bfd 3526

CHAPTER 3 BFD Static Route Commands 3527
ip bfd static all-interfaces 3528
ip static fall-over-bfd 3529
ip static bfd 3530
ipv6 bfd static all-interfaces 3531
ipv6 static fall-over-bfd 3532
ipv6 static bfd 3533

Quality of Service Configuration Guide. 3537
Contents 3537

CHAPTER 1 QoS Introduction 3539
QoS Functionality 3539
Terminology 3539
Enable/Disable Configuration 3542
Validation 3543
QoS Statistics Configuration 3543

CHAPTER 2 Dscp-to-queue Map Profile Configuration 3545
Configuration of dcsp-to-queue Map Profile on configuration mode 3545
Configuration of dscp-to-queue Map Profile on Interface mode 3546

CHAPTER 3 Cos-to-queue Map Configuration 3549
Configuration of Cos-to-queue Map on configuration mode 3549
Configuration of Cos-to-queue Map Profile on Interface mode 3549

CHAPTER 4 Queue-color-to-cos Map Profile Configuration 3553
Topology 3553
Configuration of Queue-color-to-cos Map Profile on Interface mode 3554

CHAPTER 5 Queue-color-to-dscp Map Profile Configuration 3555
Topology 3555
Configuration of Queue-color-to-dscp Map Profile on Interface mode 3556

CHAPTER 6 Trust DSCP on Layer 2 Interface Configuration 3557
Configuration Trust DSCP on Interface mode 3557

CHAPTER 7 Service based Queue Distribution Configuration 3559
Service based Queue configuration 3559

© 2021 IP Infusion Inc. Proprietary

CHAPTER 8 Weights for Queues Configuration 3563
Configuring WRR Weights for Queues 3563

CHAPTER 9 Marking/Remarking Configuration. 3573
L2 Interface 3573
L3 Interface 3579

CHAPTER 10 Policing Configuration 3587
L2 Interface 3587

CHAPTER 11 Bandwidth Configuration 3595
Topology 3595
L2/L3 Interface 3595
Validation 3596

CHAPTER 12 Shaping Configuration. 3603
Topology 3603
L2/L3 Interface 3603
Validation 3604

CHAPTER 13 Scheduling Configuration 3611
Topology 3611
Configuring Weight on L2 /L3 Interface 3611
Validation 3611

CHAPTER 14 WRED Configuration. 3619
L2/L3 Interface 3619
Validation 3620

CHAPTER 15 Tail-Drop Configuration 3625
Topology 3625
Configuring Tail-Drop 3625
Validation 3626

CHAPTER 16 Hierarchical Queuing Configuration 3635
Configuring Hierarchical Queuing 3635
Validation 3641

CHAPTER 17 VXLAN Quality of Service 3679

CHAPTER 18 FP Rules Queuing Configuration 3681
Configuring CPU Queuing Lossless 3682
Validation 3682
Configuring CPU Queuing Lossy 3684
Validation 3685

CHAPTER 19 Explicit Congestion Notification (ECN) Configuration 3689
Configuring ECN on L3 Interface 3690
Validation 3691
Configuring ECN on L2 Interface 3692
Validation 3693

© 2021 IP Infusion Inc. Proprietary

CHAPTER 20 Rate Limiting BUM Traffic 3697

Quality of Service Command Reference 3699

Contents 3699

CHAPTER 1 Quality of Service Commands 3701

bandwidth 3703
class-map type qos 3704
class-map type queuing 3705
class type qos 3706
class type queuing 3707
clear qos statistics 3708
cpu-queue 3709
egress cos map 3710
egress dscp map 3711
ingress cos map 3712
ingress dscp map 3713
ingress exp map 3714
match access-group 3715
match cos 3716
match cos inner 3717
match dscp 3718
match ip rtp 3720
match mac 3721
match precedence 3722
match protocol 3723
match qos-group 3724
match traffic-type 3725
match vlan 3726
match vlan inner 3727
police 3728
policy-map 3731
priority 3732
priority (queuing) 3733
qos (enable | disable) 3734
qos map-profile 3735
qos profile 3736
qos profile precedence-to-queue 3738
qos profile queue-to-precedence 3739
qos remark 3740
qos statistics 3741
queue-limit 3742
random-detect 3743
service-policy 3745
service-policy type qos 3746
service-policy type queuing 3747
set bridge cos 3748

© 2021 IP Infusion Inc. Proprietary

set bridge dscp . . . 3749
set cos . . . 3751
set dscp . . . 3752
set mpls class . . . 3754
set precedence . . . 3755
set qos-group . . . 3756
set qos queue scheduler . . . 3757
set queue . . . 3758
shape . . . 3759
shape rate . . . 3760
show class-map . . . 3761
show cpu-queue details . . . 3762
show policy-map . . . 3764
show policy-map interface . . . 3765
show qos-profile . . . 3768
show qos-profile interface . . . 3770
show queuing interface . . . 3771
show running-config qos . . . 3772
show running-config cpu-queue . . . 3777
storm-control . . . 3778
trust dscp . . . 3780
wrr-queue weight . . . 3781

Virtual eXtensible Local Area Network Configuration Guide . . . 3785
Contents . . . 3785

CHAPTER 1 Overview . . . 3787
Terminology . . . 3787
VXLAN Architecture . . . 3787

CHAPTER 2 VXLAN Unicast Configuration . . . 3789
Port Mapping . . . 3789
Intermediate Non-VXLAN Router . . . 3794

CHAPTER 3 VXLAN-EVPN Configuration . . . 3801
Topology . . . 3801
LAG as Access Port with ECMP on the Network Side . . . 3808

CHAPTER 4 VXLAN EVPN EVC Configuration . . . 3823
Overview . . . 3823
Topology . . . 3823
Validation . . . 3826

CHAPTER 5 VXLAN Hybrid Access Port Configuration . . . 3835
Overview . . . 3835
Topology . . . 3835
Validation . . . 3839

CHAPTER 6 VXLAN Multi-homing Configuration . . . 3847
Overview . . . 3847

© 2021 IP Infusion Inc. Proprietary

Configurations 3848
Validation 3862

CHAPTER 7 VXLAN Quality of Service Configuration 3881
Overview 3881
Topology 3881
COS-DSCP 3882

CHAPTER 8 VXLAN Trunk Access Port 3893
Topology 3893

CHAPTER 9 VXLAN Tunnel Over SVI 3915
Overview 3915
Topology 3915
Validation 3932

Virtual eXtensible Local Area Network Command Reference 3939
Contents 3939

CHAPTER 1 VXLAN Commands 3941
arp-cache disable 3943
arp-nd flood-suppress 3944
arp-nd refresh timer 3945
clear mac address table dynamic vxlan 3946
clear nvo vxlan counters 3947
clear nvo vxlan tunnels 3948
clear nvo vxlan mac-stale-entries 3949
description 3950
dynamic-learning disable 3951
encapsulation 3952
evpn esi holdtime 3953
evpn vxlan multi-homing enable 3954
evpn multi-homed 3955
evpn-vlan-service 3956
garp-gna enable 3957
load-balance rtag7 vxlan inner-l2 3958
load-balance rtag7 vxlan inner-l3 3959
mac 3960
mac vrf 3961
mac-holdtime 3962
map vnid 3963
nd-cache disable 3964
no nvo vxlan 3965
nvo vxlan 3966
. . . . . nvo vxlan access-if 3967
nvo vxlan mac-ageing-time 3969
nvo vxlan max-cache-disable 3970
nvo vxlan vtep-ip-global 3971
show bgp l2vpn evpn 3972

show bgp l2vpn evpn summary . . . 3976
show nvo vxlan . . . 3978
show nvo vxlan access-if-config . . . 3980
show nvo vxlan arp-cache . . . 3981
show nvo vxlan counters access-port . . . 3983
show nvo vxlan counters network-port . . . 3986
show nvo vxlan mac-table . . . 3988
show nvo vxlan nd-cache . . . 3991
show nvo vxlan static host state . . . 3993
show nvo vxlan tunnel . . . 3995
show running-config nvo vxlan . . . 3996
show evpn multi-homing all . . . 3998
show evpn multihoming-status . . . 3999
show nvo vxlan route-count . . . 4000
show nvo vxlan vni-name . . . 4002
shutdown . . . 4003
vxlan host-reachability-protocol evpn-bgp . . . 4004

CHAPTER 2 VXLAN Quality of Service Commands . . . 4005
clear nvo vxlan tunnels . . . 4006
cos queue . . . 4007
dscp queue . . . 4008
map qos-profile cos-to-queue . . . 4009
map qos-profile queue-color-to-cos . . . 4010
nvo vxlan tunnel qos-map-mode cos-dscp . . . 4011
qos profile cos-to-queue . . . 4012
qos profile dscp-to-queue . . . 4013
qos profile queue-color-to-cos . . . 4014
qos profile queue-color-to-dscp . . . 4015
queue cos . . . 4016
queue dscp . . . 4017

Guest Virtual Machine Command Reference . . . 4021
Contents . . . 4021

CHAPTER 1 Guest Virtual Machine Command Reference . . . 4023
debug vm-events . . . 4024
dhcp-lease-max . . . 4025
dhcp-lease-time . . . 4026
dhcp-range . . . 4027
disk-image . . . 4028
feature guest-vm . . . 4029
gateway-ip . . . 4030
host-core-affinity . . . 4031
iptables . . . 4032
iptables restore . . . 4033
iptables-template . . . 4034
memory . . . 4035

© 2021 IP Infusion Inc. Proprietary

nat dnat 4036
nat snat 4037
os-type 4038
os-variant 4039
reload vm-name 4040
secondary-disk-image 4041
service dns-masq 4042
show vm 4043
show vm-bridge 4044
show vm-iptables 4045
show vm-iptables kernel 4046
show vm-nat details 4047
show vm-template 4048
start vm-name 4049
static-bind 4050
stop vm-name 4051
vcpu count 4052
virt-type 4053
virtual-nic 4054
vm-bridge-create 4055
vm-image delete 4056
vm-template 4057

Multi-Protocol Label Switching Configuration Guide 4061
Contents 4061

CHAPTER 1 Understanding Label Space 4063
Overview 4063
Configuration 4063
Validation 4065

CHAPTER 2 Understanding MPLS TTL Processing 4071
Overview 4071

CHAPTER 4 LDP Configuration 4075
Label Distribution Protocol Overview 4075
Configure LDP 4076
LDP MD5 Authentication 4080
Configure LDP MD5 for Targeted LDP Session 4081
Removing MD5 Authentication for LDP Session 4082
MPLS LDP PING and TRACEROUTE 4084

CHAPTER 5 LDP Inter-Area Configuration 4087
Overview 4087
Configure LDP Inter-Area 4087

CHAPTER 6 MPLS LDP-IGP Synchronization 4093
Overview 4093
Prerequisites 4093
Topology 4093

© 2021 IP Infusion Inc. Proprietary

LDP-IGP Synchronization with OSPF 4094
LDP-IGP Synchronization with IS-IS 4099

CHAPTER 7 MPLS Statistics Configuration. 4107
Configure LDP-LSP 4107
Configure Static-LSP 4112

Multi-Protocol Label Switching Command Reference. 4117
Contents. 4117

CHAPTER 1 MPLS Commands 4119
bandwidth. 4121
clear mpls counters ldp 4122
clear mpls counters rsvp 4123
clear mpls counters static 4124
clear mpls l2-circuit statistics. 4125
group-id 4126
group-name 4127
control-word. 4128
label-switching. 4129
match vlan 4130
mpls ac-group 4132
mpls admin-groups. 4133
mpls bandwidth-class. 4134
mpls disable-all-interfaces. 4135
mpls enable-all-interfaces 4136
mpls ftn-entry tunnel-id 4137
mpls ftn-entry. 4139
mpls ilm-entry pop 4140
mpls ilm-entry swap 4141
mpls ilm-entry vpnpop 4143
mpls ingress-ttl 4144
mpls l2-circuit. 4145
mpls-l2-circuit NAME 4146
mpls l2-circuit-fib-entry. 4148
mpls label mode 4149
mpls local-packet-handling 4151
mpls lsp-model 4152
mpls lsp-stitching 4153
mpls map-route. 4154
mpls min-label-value 4155
mpls propagate-ttl. 4156
mpls traffic-eng 4157
mpls traffic-eng srlg 4158
ping mpls 4159
rewrite ingress. 4162
secondary srlg-disjoint. 4163
secondary-priority srlg-disjoint 4164

© 2021 IP Infusion Inc. Proprietary

service-template 4165
service-tpid 4166
show mpls 4167
show mpls admin-groups 4169
show mpls bandwidth-class 4170
show mpls counters ldp 4171
show mpls counters rsvp 4173
show mpls counters static 4175
show mpls cross-connect-table 4177
show mpls forwarding-table 4179
show mpls ftn-table 4182
show mpls ilm-table 4184
show mpls in-segment-table 4186
show mpls l2-circuit 4188
show mpls l2-circuit statistics 4190
show mpls mapped-routes 4192
show mpls out-segment-table 4193
show mpls qos-resource 4195
show mpls vc-table 4197
show mpls vrf 4198
show mpls vrf-forwarding-table vrf 4199
show running-config interface mpls 4200
show running-config mpls 4201
show running-config service-template 4202
show running-config vc 4203
show running-config vpls 4204
show service-template 4205
show vccv statistics 4206
srlg-disjoint 4207
trace mpls 4208
tunnel-id 4210
tunnel-name 4211
tunnel-select-policy 4212
vccv cc-type 4213
vccv cv-type 4214

CHAPTER 2 Differentiated Services Commands 4215
map-route A.B.C.D 4216
override-diffserv 4217
primary class-to-exp-bit 4218
primary elsp-signaled 4219
primary llsp 4220
secondary map class 4221
secondary elsp-signaled 4222
secondary llsp 4223
show rsvp diffserv-info 4224

© 2021 IP Infusion Inc. Proprietary

Label Distribution Protocol Command Reference 4225
Contents 4225

CHAPTER 1 LDP Commands 4227
advertise-labels 4229
advertise-label-for-default-route 4230
advertisement-mode 4231
clear ldp adjacency 4232
clear ldp session 4233
clear ldp statistics 4234
clear ldp statistics advertise-labels 4235
control-mode 4236
debug ldp advertise-labels 4237
debug ldp all 4238
debug ldp dsm 4239
debug ldp events 4240
debug ldp fsm 4241
debug ldp hexdump 4242
debug ldp inter-area 4243
debug ldp nsm 4244
debug ldp packet 4245
debug ldp usm 4246
debug ldp vc usm 4247
disable-ldp 4248
enable-ldp 4249
explicit-null 4250
global-merge-capability 4251
graceful-restart 4252
hello-interval 4253
hold-time 4254
import-bgp-routes 4255
inter-area-lsp 4256
keepalive-interval 4257
keepalive-timeout 4258
label-retention-mode 4259
ldp advertisement-mode 4260
ldp hello-interval 4261
ldp hold-time 4262
ldp keepalive-interval 4263
ldp keepalive-timeout 4264
ldp label-retention-mode 4265
ldp multicast-hellos 4266
ldp-optimization 4267
loop-detection 4268
loop-detection-hop-count 4269
loop-detection-path-vec-count 4270
mpls ldp-igp sync isis 4271

 © 2021 IP Infusion Inc. Proprietary

mpls ldp-igp sync ospf 4272
mpls ldp-igp sync-delay 4273
multicast-hellos 4274
neighbor 4275
propagate-release 4276
pw-status-tlv 4277
request-labels-for 4278
request-retry 4279
request-retry-timeout 4280
restart ldp graceful 4281
router ldp 4282
router-id 4283
snmp restart ldp 4284
targeted-peer ipv4 4285
targeted-peer-hello-interval 4286
targeted-peer-hold-time 4287
transport-address ipv4 4288

CHAPTER 2 LDP Show Commands 4289
show debugging ldp 4290
show ldp 4291
show ldp adjacency 4293
show ldp advertise-labels 4294
show ldp downstream 4295
show ldp fec 4297
show ldp igp sync 4299
show ldp interface 4300
show ldp lsp 4302
show ldp mpls-l2-circuit 4304
show ldp routes 4307
show ldp session 4308
show ldp statistics 4310
show ldp statistics advertise-labels 4312
show ldp targeted-peers 4313
show ldp upstream 4314
show mpls ldp discovery 4316
show mpls ldp neighbor 4317
show mpls ldp parameter 4318

RSVP-TE Command Reference 4321
Contents 4321

CHAPTER 1 RSVP-TE Commands 4323
A.B.C.D 4326
clear rsvp session 4327
clear rsvp trunk 4328
cspf 4329
debug rsvp all 4330

debug rsvp cspf 4331
debug rsvp events 4332
debug rsvp fsm 4333
debug rsvp hexdump 4334
debug rsvp nsm 4335
debug rsvp packet 4336
disable-rsvp 4337
elsp-signal-map 4338
enable-rsvp 4339
explicit-null 4340
ext-tunnel-id A.B.C.D 4341
ext-tunnel-id X:X::X:X 4342
from A.B.C.D 4343
from X:X::X:X 4344
graceful-restart 4345
graceful-restart recovery-time 4346
graceful-restart restart-time 4347
hello-interval 4348
hello-receipt 4349
hello-timeout 4350
keep-multiplier 4351
loop-detection 4352
map-route A.B.C.D 4353
map-route X:X::X:X 4354
neighbor A.B.C.D 4355
neighbor X:X::X:X 4356
no-cspf 4357
no-loop-detection 4358
no-php 4359
no-refresh-path-parsing 4360
no-refresh-resv-parsing 4361
php 4362
primary ADMIN-GROUP-NAME 4363
primary affinity 4364
primary bandwidth 4365
primary cspf 4366
primary cspf-retry-limit 4367
primary cspf-retry-timer 4368
primary filter 4369
primary hold-priority 4370
primary hop-limit 4371
primary label-record 4372
primary local-protection 4373
primary no-affinity 4374
primary no-cspf 4375
primary no-record 4376
primary path 4377

© 2021 IP Infusion Inc. Proprietary

primary policer 4378
primary record 4379
primary retry-limit 4380
primary retry-timer 4381
primary reuse-route-record 4382
primary setup-priority 4383
primary traffic 4384
refresh-time 4385
refresh-path-parsing 4386
refresh-resv-parsing 4387
restart rsvp graceful 4388
router rsvp 4389
rsvp hello-interval 4390
rsvp hello-receipt 4391
rsvp hello-timeout 4392
rsvp keep-multiplier 4393
rsvp refresh-time 4394
rsvp-path 4395
rsvp-trunk 4396
rsvp-trunk-restart 4397
secondary ADMIN-GROUP-NAME 4398
secondary bandwidth 4399
secondary cspf 4400
secondary cspf-retry-limit 4401
secondary cspf-retry-timer 4402
secondary filter 4403
secondary hold-priority 4404
secondary hop-limit 4405
secondary label-record 4406
secondary local-protection 4407
secondary no-affinity 4408
secondary no-cspf 4409
secondary no-record 4410
secondary path 4411
secondary policer 4412
secondary record 4413
secondary retry-limit 4414
secondary retry-timer 4415
secondary reuse-route-record 4416
secondary setup-priority 4417
secondary traffic 4418
snmp restart rsvp 4419
to A.B.C.D 4420
to X:X::X:X 4421
update-type 4422
X:X::X:X 4423

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Fast Reroute Commands 4425
detour-identification 4426
from X:X::X:X 4427
primary fast-reroute bandwidth 4428
primary fast-reroute hold-priority 4429
primary fast-reroute hop-limit 4430
primary fast-reroute node-protection 4431
primary fast-reroute protection 4432
primary fast-reroute setup-priority 4433

CHAPTER 3 Refresh Reduction Commands 4435
ack-wait-timeout 4436
message-ack 4437
refresh-reduction 4438
rsvp ack-wait-timeout 4439
rsvp message-ack 4440
rsvp refresh-reduction 4441

CHAPTER 4 Differentiated Services Commands 4443
map-route A.B.C.D 4444
map-route X:X::X:X 4445
override-diffserv 4446
primary map class 4447
primary elsp-signaled 4448
primary llsp 4449
secondary map class 4450
secondary elsp-signaled 4451
secondary llsp 4452
show rsvp diffserv-info 4453

CHAPTER 5 DiffServ-TE Commands 4455
primary class-type 4456
secondary class-type 4457
show rsvp dste-info 4458

CHAPTER 6 Point-to-Multipoint Commands 4459
affinity 4460
bandwidth 4461
class-type 4462
clear rsvp p2mp-session 4463
destination 4464
exit-p2mp-lsp 4465
ext-tunnel-id 4466
filter 4467
from 4468
hold-priority 4469
hop-limit 4470
label-record 4471
pack-affinity 4472

© 2021 IP Infusion Inc. Proprietary

primary-lsp 4473
retry-limit 4474
retry-timer 4475
route-record 4476
rsvp-trunk 4477
secondary-lsp 4478
setup-priority 4479
traffic 4480

CHAPTER 7 Show Commands 4481
show debugging rsvp 4482
show rsvp 4483
show rsvp admin-groups 4486
show rsvp control-adjacency 4487
show rsvp data-link 4489
show rsvp graceful-restart 4490
show rsvp dste-info 4491
show rsvp interface 4492
show rsvp neighbor 4494
show rsvp local-addresses 4495
show rsvp nexthop-cache 4497
show rsvp path 4498
show rsvp session 4500
show rsvp session count 4502
show rsvp session egress 4503
show rsvp session ingress 4507
show rsvp session LSP-NAME 4511
show rsvp session transit 4514
show rsvp summary-refresh 4517
show rsvp trunk 4518
show rsvp version 4520

Glossary 4523
Conventions 4523
Numbers 4525
A 4526
B 4528
C 4530
D 4534
E 4537
F 4539
G 4540
H 4540
I 4541
K 4544
L 4544
M 4547

© 2021 IP Infusion Inc. Proprietary

N 4550
O 4552
P 4553
Q 4557
R 4557
S 4560
T 4563
U 4565
V 4565
W 4567
Y 4568
Z 4568

Master Command Index 4573

Index. 4595

© 2021 IP Infusion Inc. Proprietary

Preface

This guide describes how to configure OcNOS.

Audience

This guide is intended for network administrators and other engineering professionals who configure OcNOS.

Conventions

Table P-1 shows the conventions used in this guide.

Table P-1: Conventions

Convention	Description
Italics	Emphasized terms; titles of books
Note:	Special instructions, suggestions, or warnings
`monospaced type`	Code elements such as commands, parameters, files, and directories

Chapter Organization

The chapters in command references are organized as described in Command Description Format.

The chapters in configuration guides are organized into these major sections:

- An overview that explains a configuration in words
- Topology with a diagram that shows the devices and connections used in the configuration
- Configuration steps in a table for each device where the left-hand side shows the commands you enter and the right-hand side explains the actions that the commands perform
- Validation which shows commands and their output that verify the configuration

Related Documentation

For information about installing of OcNOS, see the *Installation Guide* for your platform.

Migration Guide

Check the *Migration Guide* for configuration changes to make when migrating from one version of OcNOS to another.

© 2021 IP Infusion Inc. Proprietary

Feature Availability

The features described in this document that are available depend upon the OcNOS SKU that you purchased. See the *Application Notes* for a description of the OcNOS SKUs.

Support

For support-related questions, contact support@ipinfusion.com.

Comments

If you have comments, or need to report a problem with the content, contact techpubs@ipinfusion.com.

© 2021 IP Infusion Inc. Proprietary

Command Line Interface

This chapter introduces the OcNOS Command Line Interface (CLI) and how to use its features.

Overview

You use the CLI to configure, monitor, and maintain OcNOS devices. The CLI is text-based and each command is usually associated with a specific task.

You can give the commands described in this manual locally from the console of a device running OcNOS or remotely from a terminal emulator such as `putty` or `xterm`. You can also use the commands in scripts to automate configuration tasks.

Command Line Interface Help

You access the CLI help by entering a full or partial command string and a question mark “?”. The CLI displays the command keywords or parameters along with a short description. For example, at the CLI command prompt, type:

```
> show ?
```

The CLI displays this keyword list with short descriptions for each keyword:

```
show ?
  application-priority            Application Priority
  arp                             Internet Protocol (IP)
  bfd                             Bidirectional Forwarding Detection (BFD)
  bgp                             Border Gateway Protocol (BGP)
  bi-lsp                          Bi-directional lsp status and configuration
  bridge                          Bridge group commands
  ce-vlan                         COS Preservation for Customer Edge VLAN
  class-map                       Class map entry
  cli                             Show CLI tree of current mode
  clns                            Connectionless-Mode Network Service (CLNS)
  control-adjacency               Control Adjacency status and configuration
  control-channel                 Control Channel status and configuration
  cspf                            CSPF Information
  customer                        Display Customer spanning-tree
  cvlan                           Display CVLAN information
  debugging                       Debugging functions (see also 'undebug')
  etherchannel                    LACP etherchannel
  ethernet                        Layer-2
...
```

If you type the ? in the middle of a keyword, the CLI displays help for that keyword only.

```
> show de?
debugging  Debugging functions (see also 'undebug')
```

If you type the ? in the middle of a keyword, but the incomplete keyword matches several other keywords, OcNOS displays help for all matching keywords.

```
> show i? (CLI does not display the question mark).
interface  Interface status and configuration
ip         IP information
isis       ISIS information
```

© 2021 IP Infusion Inc. Proprietary

Command Completion

The CLI can complete the spelling of a command or a parameter. Begin typing the command or parameter and then press the tab key. For example, at the CLI command prompt type `sh`:

```
> sh
```

Press the tab key. The CLI displays:

```
> show
```

If the spelling of a command or parameter is ambiguous, the CLI displays the choices that match the abbreviation. Type `show i` and press the tab key. The CLI displays:

```
> show i
  interface  ip          ipv6       isis
> show i
```

The CLI displays the `interface` and `ip` keywords. Type `n` to select `interface` and press the tab key. The CLI displays:

```
> show in
> show interface
```

Type ? and the CLI displays the list of parameters for the `show interface` command.

```
> show interface
  IFNAME  Interface name
  |       Output modifiers
  >       Output redirection
  <cr>
```

The CLI displays the only parameter associated with this command, the `IFNAME` parameter.

Command Abbreviations

The CLI accepts abbreviations that uniquely identify a keyword in commands. For example:

```
> sh int xe0
```

is an abbreviation for:

```
> show interface xe0
```

Command Line Errors

Any unknown spelling causes the CLI to display the error `Unrecognized command` in response to the ?. The CLI displays the command again as last entered.

```
> show dd?
% Unrecognized command
> show dd
```

When you press the Enter key after typing an invalid command, the CLI displays:

```
(config)#router ospf here
                        ^
% Invalid input detected at '^' marker.
```

where the ^ points to the first character in error in the command.

© 2021 IP Infusion Inc. Proprietary

If a command is incomplete, the CLI displays the following message:

```
> show
% Incomplete command.
```

Some commands are too long for the display line and can wrap mid-parameter or mid-keyword, as shown below. This does *not* cause an error and the command performs as expected:

```
area 10.10.0.18 virtual-link 10.10.0.19 authent
ication-key 57393
```

Command Negation

Many commands have a `no` form that resets a feature to its default value or disables the feature. For example:

- The `ip address` command assigns an IPv4 address to an interface
- The `no ip address` command removes an IPv4 address from an interface

Syntax Conventions

Table P-2 describes the conventions used to represent command syntax in this reference.

Table P-2: Syntax conventions

Convention	Description	Example
`monospaced font`	Command strings entered on a command line	`show ip ospf`
`lowercase`	Keywords that you enter exactly as shown in the command syntax.	`show ip ospf`
`UPPERCASE`	See Variable Placeholders	`IFNAME`
`()`	Optional parameters, from which you must select one. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>)`
`()`	Optional parameters, from which you select one or none. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>|)`
`()`	Optional parameter which you can specify or omit. Do not enter the parentheses or vertical bar as part of the command.	`(IFNAME|)`
`{}`	Optional parameters, from which you must select one or more. Vertical bars delimit the selections. Do not enter the braces or vertical bars as part of the command.	`{intra-area <1-255>|inter-area <1-255>|external <1-255>}`

© 2021 IP Infusion Inc. Proprietary

Table P-2: Syntax conventions (Continued)

Convention	Description	Example
`[]`	Optional parameters, from which you select zero or more. Vertical bars delimit the selections. Do not enter the brackets or vertical bars as part of the command.	`[<1-65535>|AA:NN|internet|local-AS|no-advertise|no-export]`
`?`	Nonrepeatable parameter. The parameter that follows a question mark can only appear once in a command string. Do not enter the question mark as part of the command.	`?route-map WORD`
`.`	Repeatable parameter. The parameter that follows a period can be repeated more than once. Do not enter the period as part of the command.	`set as-path prepend .<1-65535>`

Variable Placeholders

Table P-3 shows the tokens used in command syntax use to represent variables for which you supply a value.

Table P-3: Variable placeholders

Token	Description
`WORD`	A contiguous text string (excluding spaces)
`LINE`	A text string, including spaces; no other parameters can follow this parameter
`IFNAME`	Interface name whose format varies depending on the platform; examples are: `eth0`, `Ethernet0`, `ethernet0`, `xe0`
`A.B.C.D`	IPv4 address
`A.B.C.D/M`	IPv4 address and mask/prefix
`X:X::X:X`	IPv6 address
`X:X::X:X/M`	IPv6 address and mask/prefix
`HH:MM:SS`	Time format
`AA:NN`	BGP community value
`XX:XX:XX:XX:XX:XX`	MAC address

`<1-5>`
`<1-65535>`
`<0-2147483647>`
`<0-4294967295>`
	Numeric range

© 2021 IP Infusion Inc. Proprietary

Command Description Format

Table P-4 explains the sections used to describe each command in this reference.

Table P-4: Command descriptions

Section	Description
Command Name	The name of the command, followed by what the command does and when should it be used
Command Syntax	The syntax of the command
Parameters	Parameters and options for the command
Default	The state before the command is executed
Command Mode	The mode in which the command runs; see Command Modes
Example	An example of the command being executed

Keyboard Operations

Table P-5 lists the operations you can perform from the keyboard.

Table P-5: Keyboard operations

Key combination	Operation
Left arrow or Ctrl+b	Moves one character to the left. When a command extends beyond a single line, you can press left arrow or Ctrl+b repeatedly to scroll toward the beginning of the line, or you can press Ctrl+a to go directly to the beginning of the line.
Right arrow or Ctrl-f	Moves one character to the right. When a command extends beyond a single line, you can press right arrow or Ctrl+f repeatedly to scroll toward the end of the line, or you can press Ctrl+e to go directly to the end of the line.
Esc, b	Moves back one word
Esc, f	Moves forward one word
Ctrl+e	Moves to end of the line
Ctrl+a	Moves to the beginning of the line
Ctrl+u	Deletes the line
Ctrl+w	Deletes from the cursor to the previous whitespace
Alt+d	Deletes the current word
Ctrl+k	Deletes from the cursor to the end of line
Ctrl+y	Pastes text previously deleted with Ctrl+k, Alt+d, Ctrl+w, or Ctrl+u at the cursor

© 2021 IP Infusion Inc. Proprietary

Table P-5: Keyboard operations (Continued)

Key combination	Operation
Ctrl+t	Transposes the current character with the previous character
Ctrl+c	Ignores the current line and redisplays the command prompt
Ctrl+z	Ends configuration mode and returns to exec mode
Ctrl+l	Clears the screen
Up Arrow or Ctrl+p	Scroll backward through command history
Down Arrow or Ctrl+n	Scroll forward through command history

Show Command Modifiers

You can use two tokens to modify the output of a `show` command. Enter a question mark to display these tokens:

```
# show users ?
  | Output modifiers
  > Output redirection
```

You can type the | (vertical bar character) to use output modifiers. For example:

```
> show rsvp | ?
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  last      Last few lines
  redirect  Redirect output
```

Begin Modifier

The `begin` modifier displays the output beginning with the first line that contains the input string (everything typed after the `begin` keyword). For example:

```
# show running-config | begin xe1
...skipping
interface xe1
 ipv6 address fe80::204:75ff:fee6:5393/64
!
interface xe2
 ipv6 address fe80::20d:56ff:fe96:725a/64
!
line con 0
 login
!
end
```

You can specify a regular expression after the `begin` keyword, This example begins the output at a line with either “xe2” or “xe4”:

```
# show running-config | begin xe[3-4]

...skipping
```


© 2021 IP Infusion Inc. Proprietary

```
interface xe3
 shutdown
!
interface xe4
 shutdown
!
interface svlan0.1
 no shutdown
!
route-map myroute permit 3
!
route-map mymap1 permit 10
!
route-map rmap1 permit 3
!
line con 0
 login
line vty 0 4
 login
!
end
```

Include Modifier

The `include` modifier includes only those lines of output that contain the input string. In the output below, all lines containing the word “input” are included:

```
# show interface xe1 | include input
    input packets 80434552, bytes 2147483647, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 1, missed 0
```

You can specify a regular expression after the `include` keyword. This examples includes all lines with “input” or “output”:

```
#show interface xe0 | include (in|out)put
    input packets 597058, bytes 338081476, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 613147, bytes 126055987, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
```

Exclude Modifier

The `exclude` modifier excludes all lines of output that contain the input string. In the following output example, all lines containing the word “input” are excluded:

```
# show interface xe1 | exclude input
Interface xe1
  Scope: both
  Hardware is Ethernet, address is 0004.75e6.5393
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet6 fe80::204:75ff:fee6:5393/64
    output packets 4438, bytes 394940, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

You can specify a regular expression after the `exclude` keyword. This example excludes lines with “output” or “input”:

```
# show interface xe0 | exclude (in|out)put
Interface xe0
  Scope: both
  Hardware is Ethernet  Current HW addr: 001b.2139.6c4a
  Physical:001b.2139.6c4a  Logical:(not set)
  index 2 metric 1 mtu 1500 duplex-full arp ageing timeout 3000
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 100m
  DHCP client is disabled.
  inet 10.1.2.173/24 broadcast 10.1.2.255
  VRRP Master of :  VRRP is not configured on this interface.
  inet6 fe80::21b:21ff:fe39:6c4a/64
    collisions 0
```

Redirect Modifier

The `redirect` modifier writes the output into a file. The output is not displayed.

```
# show cli history | redirect /var/frame.txt
```

The output redirection token (>) does the same thing:

```
# show cli history >/var/frame.txt
```

Last Modifier

The `last` modifier displays the output of last few number of lines (As per the user input). The last number ranges from 1 to 9999.

For example:

```
#show running-config | last 10
```

 © 2021 IP Infusion Inc. Proprietary

String Parameters

The restrictions in Table P-6 apply for all string parameters used in OcNOS commands, unless some other restrictions are noted for a particular command.

Table P-6: String parameter restrictions

Restriction	Description
Input length	1965 characters or less
Restricted special characters	: ? ' = , > |

Command Modes

Commands are grouped into modes arranged in a hierarchy. Each mode has its own set of commands. Table P-7 lists the command modes common to all protocols.

Table P-7: Common command modes

Name	Description
Executive mode	Also called *view* mode, this is the first mode to appear after you start the CLI. It is a base mode from where you can perform basic commands such as `show`, `exit`, `quit`, `help`, and `enable`.
Privileged executive mode	Also called *enable* mode, in this mode you can run additional basic commands such as `debug`, `write`, and `show`.
Configure mode	Also called *configure terminal* mode, in this mode you can run configuration commands and go into other modes such as interface, router, route map, key chain, and address family. Configure mode is single user. Only one user at a time can be in configure mode.
Interface mode	In this mode you can configure protocol-specific settings for a particular interface. Any setting you configure in this mode overrides a setting configured in router mode.
Router mode	This mode is used to configure router-specific settings for a protocol such as BGP or OSPF.

Command Mode Tree

The diagram below shows the common command mode hierarchy.

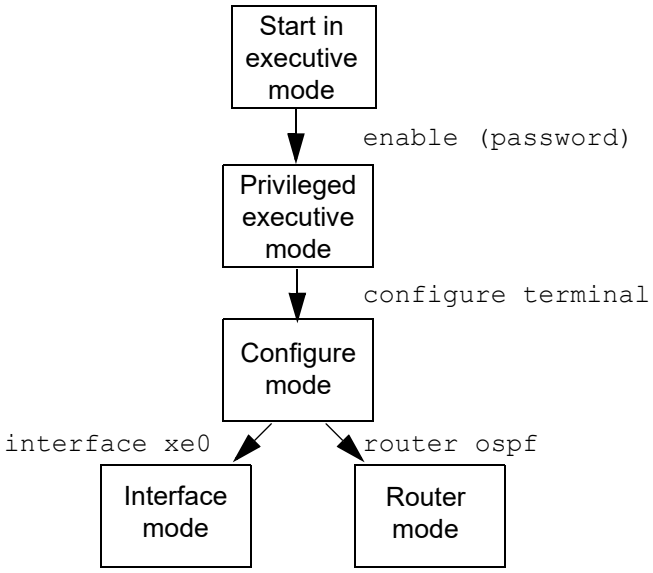


Figure P-1: Common command modes

To change modes:

1. Enter privileged executive mode by entering `enable` in Executive mode.
2. Enter configure mode by entering `configure terminal` in Privileged Executive mode.

The example below shows moving from executive mode to privileged executive mode to configure mode and finally to router mode:

```
> enable mypassword
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# router ospf
(config-router)#
```

Note: Each protocol can have modes in addition to the common command modes. See the command reference for the respective protocol for details.

© 2021 IP Infusion Inc. Proprietary

Transaction-based Command-line Interface

The OcNOS command line interface is transaction based:

- Any changes done in configure mode are stored in a separate *candidate* configuration that you can view with the show transaction current command.
- When a configuration is complete, apply the candidate configuration to the running configuration with the commit command.
- If a commit fails, no configuration is applied as the entire transaction is considered failed. You can continue to change the candidate configuration and then retry the commit.
- Discard the candidate configuration with the abort transaction command.
- Check the last aborted transaction with the show transaction last-aborted command.

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

SECTION 1

Architecture

Architecture Guide

Contents

This document contains this chapter:

- Chapter 1, *Architecture Overview*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Architecture Overview

This chapter introduces OcNOS and describes its high-level architecture.

OcNOS is an industry-standard network operating system with advanced networking features to meet the demands of data center, enterprise, and service provider networks.

The OcNOS networking protocol modules conform to leading IEEE, IETF, and other industry-specific standards:

- Layer 2 switching: VLANs, Spanning Tree
- Layer 3 routing: OSPFv2, OSPFv3, RIP, BGPv4, IS-IS
- Carrier Ethernet
- Data center Ethernet

OcNOS provides configuration management through these layers:

- Command line interface
- SNMP

© 2021 IP Infusion Inc. Proprietary

High-Level Architecture

Figure 1-1 shows the high-level architecture of OcNOS.

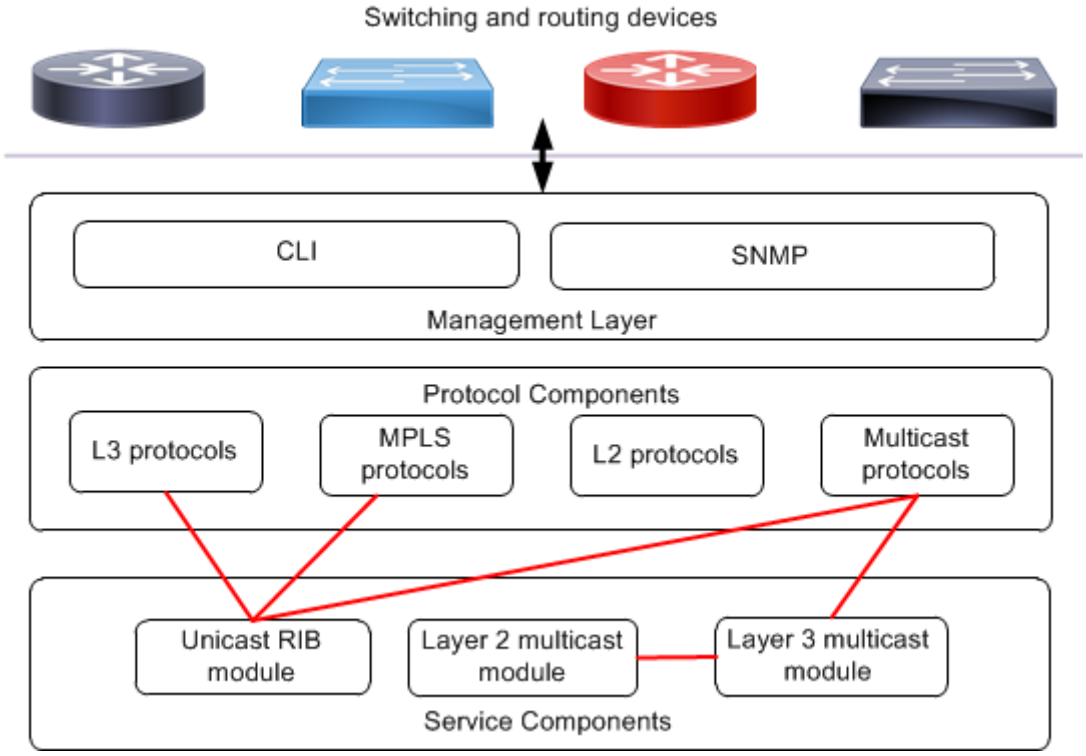


Figure 1-1: OcNOS high-level architecture

The major components of OcNOS are grouped into these categories:

- The Management Interface that is used to configure and operate the OcNOS routing and switching protocols.
- Protocol components, which include:
  - Layer 2 Protocols
  - Layer 3 Protocols
  - Multicast Protocols
- Service components, which include:
  - Unicast Routing Information Base Module
  - Layer 2 Multicast Module
  - Layer 3 Multicast Module

© 2021 IP Infusion Inc. Proprietary

Management Interface

OcNOS provides a comprehensive set of tools to manage, configure, and operate the routing and switching protocols.

The management interface includes:

- Command Line Interface
- Simple Network Management Protocol

Command Line Interface

The OcNOS command line interface (CLI) offers complete, unified management of OcNOS. Each command is usually associated with a specific task.

The IMI (Integrated Management Interface) shell is a interactive program for managing the OcNOS configuration. The IMI shell connects locally from the console of a device running OcNOS or remotely from a terminal emulator program such as `ssh` or `telnet`.

Through the IMI shell, a system administrator can configure and monitor all of the OcNOS protocols through one centralized connection. The IMI shell stores configuration data and offers extensive monitoring and logging capabilities.

The CLI can use the secure authentication methods of the operating system to manage and validate user names and passwords.

Note: The Linux `bash` shell can also be used to apply non-networking commands directly to the Linux system. However network-related commands such as `ifconfig`, `route`, `vconfig`, `iptunnel`, `brctl`, `ipmaddr`, or their iproute2 equivalents are not supported. The equivalent settings must be configured via the IMI shell in OcNOS.

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework has three parts:

- SNMP manager: A system used to control and monitor the activities of network devices.
- SNMP agent: The component within a managed device that maintains the data for the device and reports data to SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables on the managed device which network management agents can extract from the OcNOS protocols for all standard defined MIBs.

OcNOS supports the AgentX (Agent Extensibility) protocol defined by RFC 2741 to communicate between the subagent and the master agent. As shown in Figure 1-2, an SNMP manager on the network sends query packets to gather status data. Each OcNOS protocol responds to these queries as defined by the corresponding MIB for the protocol.

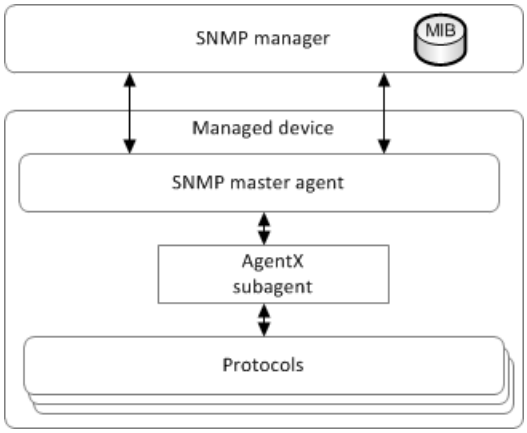


Figure 1-2: SNMP subagent

OcNOS can log both system events and errors.

For details about the MIBs that OcNOS supports, see the MIB compliance documents.

Layer 2 Protocols

OcNOS includes these Layer 2 features:

- Virtual Local Area Networks
- Spanning Tree
- Carrier Ethernet
- Port Authentication (802.1x)
- Link Aggregation (802.1AX)
- Multi-Chassis Link Aggregation

Virtual Local Area Networks

The VLAN modules offer consistent network-wide management tools to manage virtual LANs (Local Area Networks) and bridged VLANs:

- VLAN bridging divides a single physical LAN into two or more VLANs. Each VLAN is a collection of some of the LAN nodes grouped together to form individual broadcast domains.
- VLANs, in accordance with IEEE 802.1Q, enable multiple bridged LANs to transparently share the same physical network link without leaking information between LANs. Traffic between VLANs is restricted to bridges that forward unicast, multicast, or broadcast traffic only on the LAN segments that serve the VLAN to which the traffic belongs.

OcNOS VLAN modules make it easy to administer logical groups of stations that can communicate as if they were on the same LAN. They make it easier to manage a move, add, delete, or other updates to members of these groups.

The following highlights the features of the VLAN modules.

MAC Bridging (802.1d)

The OcNOS VLAN modules support all IEEE 802.1D LAN MAC (Media Access Control) protocols, shared media, and point-to-point LANs. MAC bridging allows multiple LANs to be connected together. MAC bridging filters data sent between LAN segments, reduces network congestion, and allows networks to be partitioned for administrative purposes.

© 2021 IP Infusion Inc. Proprietary

Provider Bridging (802.1ad)

Provider Bridging (PB) enables a service provider to use the architecture and protocols of 802.1Q to offer the equivalent of separate Local Area Networks (LANs), bridged LANs, or virtual bridged LANs to multiple customers. Provider bridging requires no active cooperation between customers and requires minimal cooperation between an individual customers and the service provider.

When VLANs were originally defined in the 802.1Q, the number of unique VLAN identifiers was limited to 4096. In large provider networks, each subscriber needs a separate address, thus this limit could prevent a provider from having more than 4096 subscribers.

To overcome the 4096 VLAN identifier limit, the frame format for 802.1ad inserts an additional VLAN header into a single 802.1Q Ethernet frame. There are two types of VLAN headers:

- The C-VLAN or inner header which is closest to the payload portion of the frame identifies the customer VLAN
- The S-VLAN or outer header which is closest to the Ethernet header identifier the provider VLAN

The frame format for 802.1ad is also called “Q-in-Q” or “double tagged”.

With the two VLAN identifiers in combination for each provider-customer pair, it is possible to define up to 16,777,216 labels.

VLAN Prioritization (802.1p/Q)

OcNOS includes priority signaling for traffic at the data-link layer. IEEE 802.1Q specifies a priority value of between 0 and 7 inclusive that can be used by QoS (Quality of Service) disciplines to differentiate traffic. Although this technique is often called “802.1p”, there is no standard by that name published by the IEEE. Instead, the technique is now incorporated into 802.1Q standard.

Spanning Tree

The OcNOS Spanning Tree support are a combination of these modules:

- Spanning Tree Protocol (STP)
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)

The following highlights the features of the Spanning Tree Protocol modules.

Note: All OcNOS spanning tree modules support 802.3x flow control, broadcast storm recovery, and port mirroring.

Spanning Tree Protocol (802.1d)

The OcNOS Spanning Tree Protocol (STP) module creates spanning trees within mesh networks of Layer 2 connected bridges, disabling any links that are not a part of the tree and leaving a single active connection between any two unique network nodes.

STP devices exchange BPDU (bridge protocol data unit) messages. The Spanning Tree Algorithm calculates the best path and prevents multiple paths between network segments. STP elects a root bridge, finds paths and determines the least cost path to the root bridge, then disables all other paths.

Network architects can design a topology that uses redundant links as automatic backup paths in the case of active link failure. Automatic backup takes place without the pitfalls of bridge loops, or the need to manually enable or disable backup links.

Rapid Spanning Tree Protocol (802.1w)

The Rapid Spanning Tree Protocol (RSTP) accelerates the re-configuration and restoration of a spanning tree after a link failure.

Multiple Spanning Tree Protocol (802.1s)

The Multiple Spanning Tree Protocol (MSTP) is a supplement to the IEEE 802.1ad standard. MSTP allows VLAN bridges to use multiple spanning trees, by providing the ability for traffic belonging to different VLANs to flow over potentially different paths within the virtual bridged LAN.

Carrier Ethernet

OcNOS offers a comprehensive set of Carrier Ethernet (CE) protocols from the IETF and IEEE.

Provider network operators can also benefit from Provider Bridging (802.1ad).

Link Level Discovery Protocol (802.1AB)

Link Layer Discovery Protocol (LLDP) is an agent running on an IEEE 802.1 bridge that provides a mechanism for all the bridges connected to the LAN to send and receive connectivity and management related information to each other.

Port Authentication (802.1x)

The OcNOS Layer 2 802.1x module provides port-based network access control (PNAC) for LAN devices. The IEEE 802.1x standard offers centralized control of user authentication and access.

Link Aggregation (802.1AX)

The link aggregation module allows one or more links to be aggregated together to form a Link Aggregation Group (LAG), such that a MAC client can treat the Link Aggregation Group as if it were a single link. The Link Aggregation Control Protocol (LACP) allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The system treats the aggregated interface as a single interface. When there is a failure in one physical interface, the remaining interfaces stay up, so there is no data traffic disruption. Link aggregation is defined in IEEE 802.1AX.

Multi-Chassis Link Aggregation

In data centers, spanning tree protocols like STP, RSTP, and MSTP create a loop-free topology that results in under-utilized physical links as well as redundant links between nodes that are in discarding state. As a result, more than 50% of the physical links are blocking. Link Aggregation (802.1AX) binds multiple physical links in a node into a single logical link, thereby increasing bandwidth and providing link-level redundancy. As a result, physical link utilization improves. However, a node failure in the network causes complete traffic loss as link aggregation does not provide any node-level redundancy.

The OcNOS implementation of multi-chassis link aggregation (MC-LAG) extends the link aggregation concept to ensure that connectivity between two networks can be maintained despite the failure of a node. MC-LAG provides node-level redundancy by allowing two or more nodes in the network to share a common LAG endpoint. MC-LAG emulates multiple nodes to represent a single logical node to the remote node running link aggregation. Even if one of the nodes is down, there exists a path to reach the destination via other nodes. MC-LAG allows you to use all interconnects in an active/active mode.

As shown in Figure 1-3, switch 2 and switch 3 share a common endpoint in switch 1. Switches 2 and 3 are a single logical node to switch 1. Even if switch 2 or switch 3 is down, there exists a path from switch 1 to reach other destinations. Switch 2 and switch 3 also share a common endpoint in switch 4.

© 2021 IP Infusion Inc. Proprietary

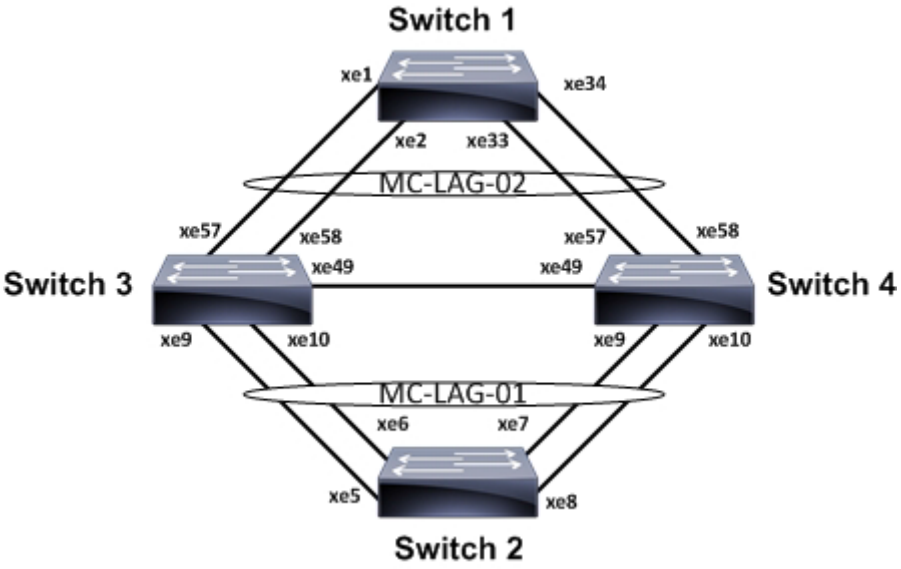


Figure 1-3: MC-LAG switching topology

With MC-LAG, at either one or both ends of a link aggregation group, a single aggregation system is replaced by a *portal* that is a collection of one to three portal systems. In Figure 1-3, switches 1, 2, and 3 are a portal system, each with physical links that together make up a link aggregation group. The portal's systems cooperate to emulate the presence of a single aggregation system to which the entire link aggregation group is attached. Switches 2, 3, and 4 are also a portal system.

MC-LAG is also called MLAG.

Layer 3 Protocols

OcNOS supports these IP protocols:

- Border Gateway Protocol
- Open Shortest Path First
- Full MIB support
- Intermediate System to Intermediate System
- Virtual Router Redundancy Protocol
- Bidirectional Forwarding Detection

In addition to the standard Layer 3 routing protocols, OcNOS offers:

- Virtual Routing (VR) support
- Virtual Routing and Forwarding (VRF) support
- Constrained Shortest Path First (CSPF) topology support for the Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) protocols

Unicast Routing Information Base Module

OcNOS maintains a central unicast Routing Information Base (RIB). A RIB is a data structure stored in a network device that lists the routes to particular network destinations and metrics (distances) associated with those routes. A RIB contains information about the topology of the network immediately around it. Maintaining a RIB by discovering

network topology is the primary purpose of dynamic routing protocols such as BGP, RIP and OSPF. Static fixed routes are added to a RIB by commands. (A RIB is also called a routing table.)

A Forwarding Information Base (FIB) is used to find the proper interface to which an input interface should forward a packet. In contrast to RIBs, FIBs are optimized for fast lookup of destination addresses. (A FIB is also called a forwarding table.)

Protocol modules create their own routes and communicate this protocol-specific information to the unicast RIB. The OcNOS unicast RIB contains all routing information received from routing peers, for example, destination prefix, nexthop information, and distance.

Figure 1-4 shows how the Layer 3 protocols and the unicast RIB communicate.

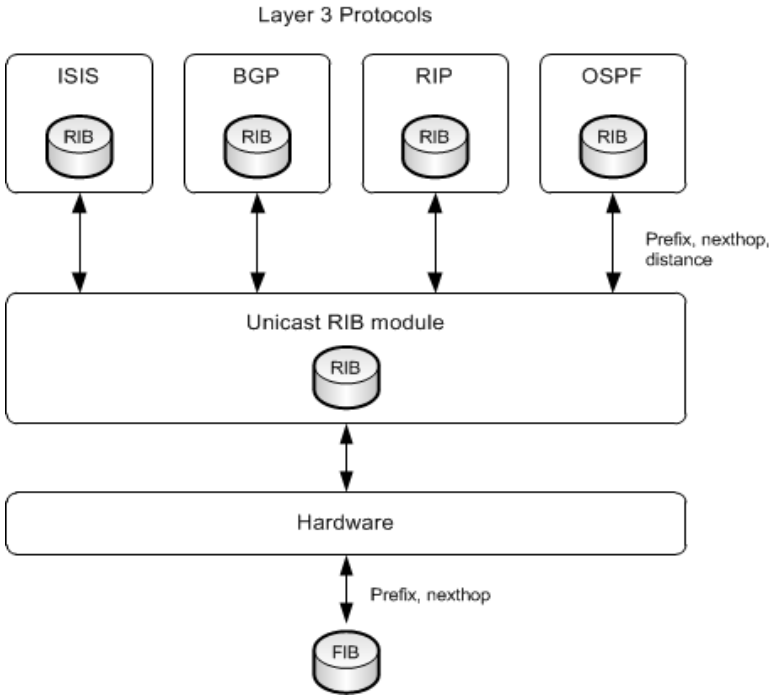


Figure 1-4: Protocol, unicast RIB, and kernel interaction

The unicast RIB performs these operations:

- Communicate with OcNOS routing and switching modules to get routing information updates
- Provide configuration for static routes
- Process the routing information and maintain all the received routes from clients as part of the RIB
- Maintain the FIB
- Process the routes and select the FIB route and program the kernel
- Redistribute routes
- Handle interface up and down events

For every known prefix, OcNOS maintains a route node entry in its RIB. OcNOS populates this table upon receiving routes from:

- Protocols such as BGP, RIP and OSPF
- Static routes configured using commands
- The kernel FIB
- Connected routes derived from interface information

© 2021 IP Infusion Inc. Proprietary

Routing protocols use different metrics to calculate the best path for a destination.The best path is sent to the RIB.

Border Gateway Protocol

Border Gateway Protocol (BGP) is a core exterior gateway protocol (EGP) used on the Internet. BGP maintains a table of IP networks, or prefixes, which designate network reachability among Autonomous Systems (AS). BGP is a path-vector protocol that makes routing decisions based on path, network policies, and/or rule sets.

OcNOS supports BGP version 4.

OcNOS BGP features include:

- IPv4 support
- Route Reflection
- Route Refresh
- Community Attributes
- Community Attributes in Multi-Home Routing
- Extended Communities
- Protection of BGP Session via the TCP MD5 Signature Option
- Capabilities Advertisement
- Route Flap Damping
- E-BGP Multi hop
- Stateful implementation
- Multi-protocol BGP (MP-BGP) extensions
- BGP VPNs
- BGP Graceful restart
- BGP Inter-Domain Routing (IDR):
    - Virtual Routing and Virtual Routing and Forwarding Support
    - Full MIB support

Open Shortest Path First

Open Shortest Path First (OSPF) is a link-state routing protocol that runs internally on a single autonomous IPv4 system. Each router designated to run OSPF maintains an identical database only within area. From this database, a routing table is calculated by constructing a shortest-path tree.

OcNOS OSPF features include:

- Opaque Link State Attributes (LSA)
- Link State Attributes (LSA) - Throttling
- Link Local Signaling
- Multiple Instance Support
- Intra- and inter-area routing
- Type 1/2 external routing
- Opaque link state availability (LSA) Option
- Manual and automatic virtual links

- Broadcast, point-to-point and point-to-multi-point models, NBMA network
- MD5 authentication
- Incremental SPF
- Traffic Engineering extensions
- Virtual Routing (VR) and Virtual Routing and Forwarding (VRF) support
- Graceful restart
- Virtual Private Network (VPN) support
- Constrained Shortest Path (CSPF) support
- Full MIB support

Routing Information Protocol

The Routing Information Protocol (RIP) version 2 is one of the most commonly used interior gateway protocols (IGP) for routing on internal IPv4 networks, and to a lesser extent, networks connected to the Internet. RIP employs a distributed variant of the Bellman-Ford algorithm to provide distance vector routing capabilities. RIP also supports subnet information, thus allowing Classless Inter-domain Routing (CIDR).

OcNOS RIP features include:

- Split horizons with poisoned reverse
- Triggered updates
- Full MIB support

Intermediate System to Intermediate System

Intermediate System-to-Intermediate-System (IS-IS) is a link-state routing protocol that runs internally on a single autonomous system. IS-IS routers maintain identical databases that describe the autonomous system's topology. A routing table is calculated from the database by constructing a shortest-path tree.

OcNOS IS-IS features includes:

- Use of OSI IS-IS for Routing in TCP/IP
- Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- IS-IS Exponential Back-off of SPF
- IS-IS external routes redistribution
- BFD over IS-IS (v4)
- Full MIB support

Virtual Router Redundancy Protocol

The Virtual Router Redundancy Protocol (VRRP) allows a virtual router composed of two or more routers on the same subnet to prevent failure by providing at least one standby virtual router if the master virtual router fails. VRRP eliminates the single point of failure most common in a static default routed environment.

In OcNOS, the VRRP module functions are to:

- Bring up or down VRRP sessions in the respective VR mode
- Create and delete VRRP sessions dynamically

© 2021 IP Infusion Inc. Proprietary

- Transmit and receive VRRP packets to and from the virtual-router peers based on the time-out value or the current state of the VRRP router

VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP addresses associated with a virtual router is called the master, and it forwards packets sent to these IP addresses. The election process manages dynamic fail-over in the forwarding responsibility should the master become unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first-hop router by end-hosts. The advantage of using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

OcNOS supports VRRP as specified in RFC 5798.

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) reduces the reliance upon the relatively slow Hello mechanism in routing protocols to detect failures where no hardware signaling is available to assist. BFD works with BGP, OSPFv2, and IS-IS to enable them to configure BFD sessions, and for the sessions to receive the bidirectional forwarding failure notifications.

BFD provides the following features:

- A single mechanism to detect liveliness over any media and in any protocol layer
- Rapid detection of communication failures between adjacent systems to quickly establish alternative paths
- Passive, Active, Synchronous, Asynchronous, and Demand modes of operation
- Improved system performance when faster detection is required, because data-plane reachability detection is detached from control-plane functionality
- OcNOS protocol modules support BFD irrespective of where BFD packet-sending operations take place: in the interfaces, data links, or to some extent, in the forwarding engines themselves
- BFD is Graceful-Restart unaware: whenever BFD timers expire, a session-down event is triggered to the protocol module, and BFD maintains sessions for the protocol while it undergoes Graceful Restart
- A fast mechanism to detect liveliness of static next-hops

Multicast Protocols

OcNOS provides these multicast protocols:

- Layer 2 Multicast Module
- Layer 3 Multicast Module
- Protocol-Independent Multicast Module

Layer 2 Multicast Module

Multicast packets are transmitted to a specific multicast address that represents a group of receivers that want to receive the packets. Through the Internet Group Management Protocol (IGMP), a host receiver can join and leave a multicast group.

IGMP snooping is the ability to passively listen for IGMP packets to learn IPv4 multicast group membership information. With IGMP snooping, multicast traffic for a group is only forwarded to ports that have members in that group. OcNOS supports IGMP snooping functionality for IGMP versions 1, 2, and 3.

Layer 3 Multicast Module

The multicast protocols communicate with the Layer 3 multicast module which communicates with the multicast forwarder. A common multicast routing information base allows multiple multicast protocols to function simultaneously.

Figure 1-5 shows the Layer 3 multicast architecture of OcNOS. The Layer 3 multicast module holds the multicast RIB and consolidates the routes from multicast routing protocols such as Protocol-Independent Multicast Module and installs them in the multicast FIB.

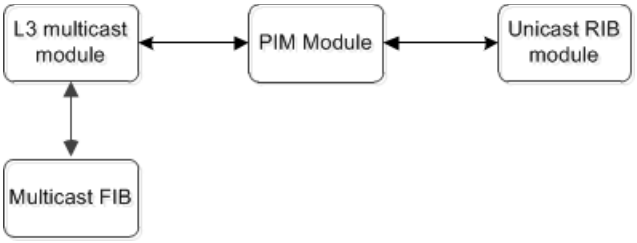


Figure 1-5: Layer 3 multicast architecture

Protocol-Independent Multicast Module

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for IP networks that provides one-to-many and many-to-many distribution of data over a network. PIM is termed *protocol-independent* because it does not have its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols.

OcNOS support these variants of PIM:

- PIM Sparse Mode (PIM-SM: RFC 4601) efficiently establishes distribution trees across wide area networks (WANs) by routing packets to multicast groups. PIM-SM constructs a tree from each sender to the receivers in a multicast group and packets from the sender follow the tree to interested recipients. PIM-SM is for situations where multicast groups are thinly populated across a large region. Although it can operate in LAN environments, it is most efficient in WAN environments.
- PIM Source-Specific Multicast (PIM-SSM: RFC 3569) is a subset of PIM-SM that allows deployment of SSM in a network with hosts that do not support IGMP version 3. PIM-SSM builds trees that are rooted in just one source, offering a more secure and scalable model for a limited amount of applications (mostly broadcasting of content). In PIM-SSM, an IP datagram is transmitted by a source S to an PIM-SSM destination address G, and receivers can receive this datagram by subscribing to channel (S,G).

PIM features include:

- Any Cast RP
- Bootstrap router
- PIM border

System Management

The system management module supports these host protocols:

- Authentication, Authorization, and Accounting
- Dynamic Host Configuration Protocol Client
- Dynamic Host Configuration Protocol Relay
- Domain Name System

© 2021 IP Infusion Inc. Proprietary

- Network Time Protocol
- Secure Shell
- Simple Network Management Protocol
- Syslog
- Telnet
- User Roles

Authentication, Authorization, and Accounting

The authentication, authorization, and accounting (AAA) commands provide these functions:

- *Authentication* identifies users by asking them to provide a user name and password. This information can be encrypted if required, depending on the underlying protocol.
- *Authorization* provides a method of authorizing commands and services on a per user profile basis.
- *Accounting* collects detailed system and command information and stores it on a central server where it can be used for security and quality assurance purposes.

The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing devices. The AAA feature works with Remote Authentication Dial In User Service.

Dynamic Host Configuration Protocol Client

The Dynamic Host Configuration Protocol (DHCP) client is used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). DHCP is implemented in a client-server model where DHCP clients request configuration data, such as an IP address, a default route, or DNS server addresses from a DHCP server.

Dynamic Host Configuration Protocol Relay

DHCP relay allows DHCP clients to communicate directly with DHCP servers in small networks with only one IP subnet. To allow DHCP clients on subnets not directly served by DHCP servers to communicate with DHCP servers, DHCP relay agents can be installed on these subnets. The DHCP client broadcasts on the local link and the relay agent receives the broadcast and transmits it to one or more DHCP servers using unicast. The DHCP server replies to the client and the relay agent then retransmits the response on the local network.

Domain Name System

The Domain Name System (DNS) translates easily-to-remember domain names into numeric IP addresses needed to locate computer services and devices. By providing a worldwide, distributed keyword-based redirection service, DNS is an essential component of the Internet.

Network Time Protocol

The Network Time Protocol (NTP) synchronizes computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.

Remote Authentication Dial In User Service

Remote Authentication Dial In User Service (RADIUS) provides centralized Authentication, Authorization, and Accounting management for users that connect to and use a network service. RADIUS is specified in RFC 2865.

Secure Shell

Secure Shell (SSH) is a cryptographic protocol for secure data communication, remote login, remote command execution, and other secure network services between two networked computers.

Simple Network Management Protocol

In SNMP, administration groups are known as *communities*. SNMP communities consist of one agent and one or more SNMP managers. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated and /or encrypted.

SNMP is defined in RFCs 3411-3418.

Syslog

Linux applications use the `syslog` utility to collect, identify, time-stamp, filter, store, alert, and forward logging data. The `syslog` utility can track and log all manner of system messages from informational to extremely critical. Each system message sent to a `syslog` server has two descriptive labels associated with it:

- The function (facility) of the application that generated it. For example, applications such as `mail` and `cron` generate messages with facilities named mail and cron.
- Eight degrees of severity (numbered 0-7) of the message.

Telnet

Telnet is a client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of functions.

User Roles

OcNOS provides four user roles:

- Network Administrator: all access permission to make permanent changes to the switch configuration. Changes are persistent across reset/reboot of switch.
- Network Engineer: all access permission to make permanent changes to the switch configuration. Changes are persistent across reset/reboot of switch. The `start-shell` and `hw-shell` commands are blocked for this role.

© 2021 IP Infusion Inc. Proprietary

- Network Operator: all access permission to make permanent changes to the switch configuration. Changes are not persistent across reset/reboot of switch.
- Network User: access permission to display information, but cannot modify any existing configuration.

Virtual Extensible Local Area Network

Virtual extensible LAN (VxLAN) interconnects Layer 2 networks using VxLAN tunnel end points (VTEPs) and a Layer 3 tunnel (segment). A VTEP has an IP address and interacts with a local LAN segment and an IP transport network. A VTEP can be a hypervisor, top-of-rack (TOR) switch, or a gateway. VxLAN can run between VTEPs within a data center or can interconnect different data centers. VxLAN labels Layer 2 segments with a network identifier (VNID) which provides up to 16 million tunnels in the same administrative domain.

VxLAN creates LAN segments using MAC Address-in-User Datagram Protocol (MAC-in-UDP) encapsulation.

Figure 1-6 shows VLANs 32 and 47 connected by a VxLAN tunnel named VNID 82.VTEP-14 routes packets from VLAN 32 to the transport network based on the IP address of VTEP-37. VTEP-37 receives the packets, strips the outer headers, and forwards the packets to a host identified by the destination MAC address on VLAN 47.

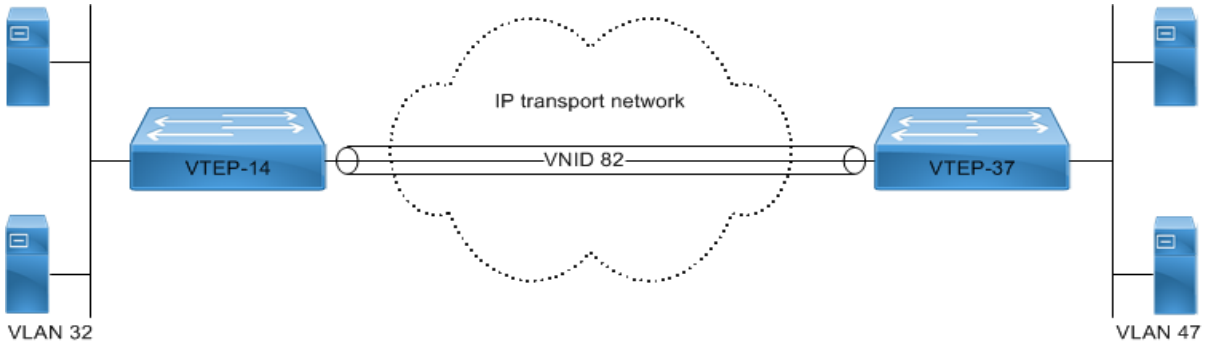


Figure 1-6: VxLAN High-level Architecture

VxLAN EVPN using MP-BGP

OcNOS supports VxLAN EVPN (Ethernet Virtual Private Network) using MP-BGP where the virtual machine MAC address learning happens in the control plane using MP-BGP and not in the data plane. This allows dynamic learning and provisioning of tunnels and hosts. BGP route reflectors can be deployed on the carrier backbone network. All provider edge devices maintain a peer relationship with the BGP route reflectors. The route reflectors distribute the EVPN routes.

© 2021 IP Infusion Inc. Proprietary

SECTION 2

System Management

System Management Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *Access Control Lists Configurations*
- Chapter 2, *Debounce Timer*
- Chapter 3, *DHCP Client Configuration*
- Chapter 4, *DHCP Relay Agent Configuration*
- Chapter 5, *DHCP Relay Agent Over L3VPN Configuration*
- Chapter 6, *DHCP Snooping*
- Chapter 7, *DHCP Snooping IP Source Guard*
- Chapter 8, *DHCP Snooping over MLAG*
- Chapter 9, *DHCPv6 Prefix Delegation*
- Chapter 10, *DHCPv6 Relay Prefix Delegation Route Injection Configuration*
- Chapter 11, *DNS Configuration*
- Chapter 12, *ErrDisable for Link-Flapping Configuration*
- Chapter 13, *Ethernet Interface Loopback Support Configurations*
- Chapter 14, *LAG with RTAG7 Hashing*
- Chapter 15, *Link Detection Debounce Timer*
- Chapter 16, *Max Session and Session Limit Configuration*
- Chapter 17, *NTP Client Configuration*
- Chapter 18, *Port Breakout Configuration*
- Chapter 19, *Proxy ARP and Local Proxy ARP*
- Chapter 20, *RADIUS Client Configuration*
- Chapter 21, *sFlow Configuration*
- Chapter 22, *Show Tech Support Configurations*
- Chapter 23, *Simple Network Management Protocol*
- Chapter 24, *Software Monitoring and Reporting*
- Chapter 25, *SSH Client Server Configuration*
- Chapter 26, *Syslog Configuration*
- Chapter 28, *TACACS Client Configuration*
- Chapter 27, *Telnet Configuration*
- Chapter 29, *Traffic Mirroring Configuration*
- Chapter 30, *Trigger Failover Configuration*
- Chapter 31, *User Configuration*
- Chapter 32, *Using the Management Interface*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Access Control Lists Configurations

This chapter contains a complete example of access control list (ACL) configuration.

Overview

An Access Control List is a list of Access Control Entries (ACE). Each ACE in ACL specifies the access rights allowed or denied.

Each packet that arrives at the device is compared to each ACE in each ACL in the order they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

Note: If there is no match, the packet is dropped (implicit deny). Therefore, an ACL intended to deny a few selected packets should have at least one permit filter of lower priority; otherwise, all traffic is dropped because of the default implicit deny filter.

Topology

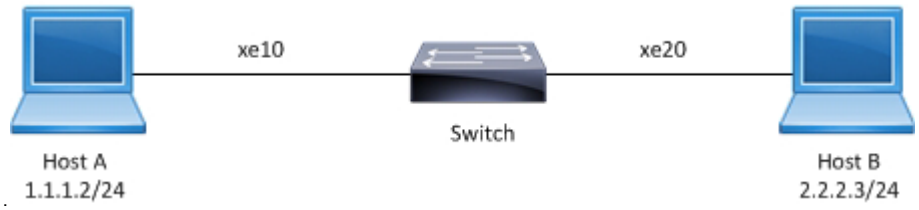


Figure 1-7: ACL sample topology

IPv4 ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ip access-list T1`	Create an IP access list named T1.
`(config-ip-acl)#deny any host 1.1.1.1 any`	Create an access rule to deny IP packets with source address 1.1.1.1.
`(config-ip-acl)#permit any host 1.1.1.1 any`	Create an access rule to permit IP packets with source address 1.1.1.1.
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ip address 1.1.1.3/24`	Assign an IP address.
`(config-if)#ip access-group T1 in`	Apply access group T1 for inbound traffic to the interface.
`(config-if)#exit`	Exit interface and configure mode.

© 2021 IP Infusion Inc. Proprietary

Validation

Use the commands below to verify the match count. When inbound IP packets reach interface xe10 with source address 1.1.1.1, then the match count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists T1
    IP access list T1
            10 deny any host 1.1.1.1 any [match=200]
            20 permit any 1.1.1.1/24 any
            default deny-all
```

When inbound IP packets reach interface xe10 with a source address in the range from 1.1.1.1 to 1.1.1.254, then the match count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists T1
    IP access list T1
        10 deny any host 1.1.1.1 any
        20 permit any 1.1.1.1/24 any [match=2000]
        default deny-all
```

Note: Use the command `clear ip access-list counters` to clear the statistics of all ACLs or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

ICMP ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ip access-list icmp-acl-01`	Create an IP access list named icmp-acl-01.
`(config-ip-acl)#deny icmp 1.1.1.1/24 2.2.2.2/24 fragments dscp af11`	Create an access rule with sequence number 10 to deny ICMP packets from a specific source towards a specific destination with a DSCP value of af11. Note: The sequence number is optional.
`(configip-acl)#20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash`	Create an access rule with sequence number 20 to permit ICMP packets from a specific source towards a specific destination with precedence as flash.
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ip address 1.1.1.3/24`	Assign an IP address.
`(config-if)#ip access-group icmp-acl-01 in`	Apply access group icmp-acl-01 for inbound traffic to the interface.
`(config-if)#exit`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound IP packets reach interface xe10 with source address 1.1.1.X, destination address 2.2.2.X, DSCP value af11, and are fragmented, then the count for access rule 10 increases equal to the number of packets sent.

```
    #show ip access-lists icmp-acl-01
    IP access-list icmp-acl-01
        deny icmp 1.1.1.1/24 2.2.2.2/24 precedence flash [match=200]
```

 © 2021 IP Infusion Inc. Proprietary

```
    20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
    default deny-all
```

When inbound IP packets reach interface xe10 with source address as 1.1.1.X, destination address 2.2.2.X, and precedence value flash, then the count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists icmp-acl-01
IP access-list icmp-acl-01
    deny icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
    20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash [match=200]
    default deny-all
```

Note: Use the command `clear ip access-list counters` to clear statistics of all ACLs configured or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

Access List Entry Sequence Numbering

You can change the sequence numbers of rules in an access list.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

`#configure terminal`	Enter configure mode.
`(config)#ip access-list icmp-acl-01`	Enter access list mode for ACL icmp-acl-01.
`(config-ip-acl)#resequence 100 200`	Re-sequence the access list, starting with sequence number 100 and incrementing by 200.
`(config-ip-acl)#1000 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11`	Re-sequencing specific access rule 100 with sequence number 1000
`(config-ip-acl)#exit`	Exit access list mode.

Validation

Before re-sequencing:

```
#show access-lists icmp-acl-01
IP access list icmp-acl-01
        deny icmp 1.1.1.1/24 2.2.2.2/24 precedence flash log
        20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
        default deny-all
```

After re-sequencing the access list, starting with sequence number 100 and incrementing by 200

```
#show access-lists icmp-acl-01
IP access list icmp-acl-01
        100 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
        300 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
        default deny-all
```

After re-sequencing specific access rule 100 with sequence number 1000

```
 #show access-lists icmp-acl-01
IP access list icmp-acl-01
300 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
1000 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
default deny-all
```

IPv6 ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ipv6 access-list ipv6-acl-01`	Create an IPv6 access list named as icmp-acl-01.
`(config-ipv6-acl)#11 deny ipipv6 any any flow-label 100deny ipipv6 any any flow-label 100`	Create access rule sequence number 11 to deny IPv4 encapsulated packets in IPv6 with any source address to any destination address with flow label 100.
`(config-ipv6-acl)#default permit-all`	Update the default rule to permit all.
`(config-ipv6-acl)#exit`	Exit access list mode
`(config)#interface xe10`	Enter interface mode.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ipv6 address 1:1::1:3/64`	Assign an IPv6 address.
`(config-if)# ipv6 access-group ipv6-acl-01 in`	Apply access group ipv6-acl-01 for inbound traffic to the interface.
`(config-if)#exit`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound IPv6 packets reach interface xe10 with IPv4 packets encapsulated with flow label 100, then count for access rule 11 increases equal to the number of packets sent.

```
#show ipv6 access-lists ipv6-acl-01
IPv6 access-list ipv6-acl-01
    11 deny ipipv6 any any flow-label 100 [match=1000]
    default permit all
```

For all other IPv6 packets, access rule 100 is invoked and the match counts increase equal to the number of packets sent.

```
#show ipv6 access-lists ipv6-acl-01
IPv6 access-list ipv6-acl-01
    11 deny ipipv6 any any flow-label 100
    default permit-all [match=2000]
```

Note: Use the command `clear ipv6 access-list counters` to clear statistics of all IPv6 ACLs configured or `clear ipv6 access-list <ipv6 access-list name> counters` to clear statistics of the particular IPv6 ACL.

MAC ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#mac access-list mac-acl-01`	Create a MAC access list named mac-acl-01.
`(config-mac-acl)#22 permit host 0000.0011.1212 host 0000.1100.2222 vlan 2`	Create an access rule with sequence number 22 to permit packets from a host with a specific MAC towards a host with a specific MAC with VLAN 2.
`(config-mac-acl)#exit`	Exit access list mode.

© 2021 IP Infusion Inc. Proprietary

`(config)#bridge 1 protocol rstp vlan-bridge`	Create a VLAN-aware RSTP bridge.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2.
`(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`(config-if)#switchport trunk allowed vlan all`	Enable all VLAN identifiers on this interface.
`(config-if)# mac access-group mac-acl-01 in`	Applies the MAC access list mac-acl-01 to ingress traffic.
`(config-if)#exit`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound packets reach interface xe10 with the specific source and destination MAC with the VLAN as 2, then the count for access rule 22 increases equal to the number of packets sent.

```
#show mac access-lists
    MAC access list mac-acl-01
        22 permit mac host 0000.0011.1212 host 0000.1100.2222 vlan 2 [match=3000]
        default deny-all
```

For all other packets, default rule is invoked and the match counts increases equal to the number of packets sent.

```
#show mac access-lists mac-acl-01
    MAC access list mac-acl-01
        22 permit mac host 0000.0011.1212 host 0000.1100.2222 vlan 2
        default deny-all [match=2000]
```

Note: As per the present design, ARP/ND packets will be filtered based on the source MAC address only (host mac address).

Note: Use the command `clear mac access-list counters` to clear statistics of all MAC ACLs or `clear mac access-list <mac access-list name> counters` to clear statistics of a particular MAC ACL.

Management ACL Overview

Management Port ACL can be used to provide basic level of security for accessing the management network. ACLs can also be used to decide which types of management traffic to be forwarded or blocked at the management port.

When configuring access list on a router or a switch, each access list needs to be identified by a unique name or a number. Each access list entry can have permit or deny actions. Each entry will be associated with a sequence number in the range of <1-268435453>. Lower the sequence number, higher the priority.

User should be able to configure the system to allow certain IP address for a protocol and don’t allow any other IP address matching for that protocol.

Note: If there is no match, the packet is dropped (implicit deny). Therefore, an ACL intended to deny a few selected packets should have at least one permit filter of lower priority; otherwise, all traffic is dropped because of the default implicit deny filter.

Topology

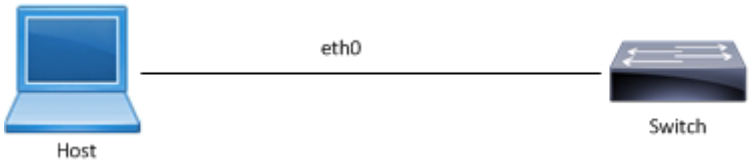


Figure 1-8: Management ACL Sample Topology

Management ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ip access-list mgmt`	Create an IP access list named mgmt
`(config-ip-acl)#permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh`	Create an access rule to permit TCP connection with source address 10.12.45.57 with destination address 10.12.29.49 on destination port equal to SSH.
`(config-ip-acl)#permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet`	Create an access rule to permit TCP connection with source address 10.12.45.58 with Destination address 10.12.29.49 on destination port equal to Telnet.
`(config-ip-acl)#permit udp any host 10.12.29.49 eq snmp`	Create an access rule to permit UDP packet with any source address with Destination address 10.12.29.49 on destination port equal to SNMP.
`(config-ip-acl)#permit udp any host 10.12.29.49 eq ntp`	Create an access rule to permit UDP packet with any source address with Destination address 10.12.29.49 on destination port equal to NTP.
`(config-ip-acl)#permit udp host 10.12.29.49 any eq snmptrap`	Create an access rule to permit UDP packet with source address 10.12.29.49 with any Destination address on destination port equal to SNMPTrap.
`(config-ip-acl)#permit tcp host 10.12.29.49 eq ssh host 10.12.45.57`	Create an access rule to permit TCP connection with source address 10.12.29.49 on source port equal to ssh with Destination address 10.12.45.57.
`(config-ip-acl)#deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh`	Create an access rule to deny TCP connection with source address 10.12.45.58 with Destination address 10.12.29.49 on destination port equal to SSH.
`(config-ip-acl)# deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet`	Create an access rule to deny TCP connection with source address 10.12.45.57 with Destination address 10.12.29.49 on destination port equal to Telnet.
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#interface eth0`	Enter interface mode of Management Interface.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ip address 10.12.29.49/24`	Assign an IP address.
`(config-if)#ip access-group mgmt in`	Apply access group mgmt for inbound traffic to the interface.
`(config-if)#exit`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When a TCP connection for Destination Port SSH reach interface eth0 with source address 10.12.45.57, then the match count for access rule 10 increases equal to the number of packets sent.

© 2021 IP Infusion Inc. Proprietary

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh [match=9]
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a TCP connection for Destination Port Telnet reach interface eth0 with source address 10.12.45.58, then the match count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet [match=10]
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a UDP packet for Destination Port SNMP reach interface eth0 with any source address, then the match count for access rule 30 increases equal to the number of packets sent. Prior to this SNMP should be configured on Device (10.12.29.49).

```
    Example:
    snmp-server community SNMPTEST group network-admin vrf management
    snmp-server host 10.12.6.86 traps version 2c SNMPTEST udp-port 162 vrf
    management
    snmp-server enable snmp  vrf management

    #show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp [match=50]
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a UDP packet for Destination Port NTP reach interface eth0 with any source address, then the match count for access rule 40 increases equal to the number of packets sent. Prior to this NTP should be configured on Device (10.12.29.49).

```
    Example:
    ntp enable vrf management
    ntp authenticate vrf management
    ntp authentication-key 123 md5 swwx 7 vrf management
    ntp trusted-key 123 vrf management
    ntp server 10.12.45.36 vrf management
    ntp server 10.12.16.16 prefer vrf management
```

```
    ntp server 10.12.16.16 key 123 vrf management

#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp [match=1]
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a TCP connection request for Destination Port SSH reach interface eth0 with source address 10.12.45.58, this should deny the connection and the match count for access rule 70 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh [match=1]
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a TCP connection request for Destination Port Telnet reach interface eth0 with source address 10.12.45.57, this should deny the connection and the match count for access rule 80 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet[match=1]
            default deny-all
```

To enable SNMPTRAPS, apply the ACL outbound to the Management interface.

`#configure terminal`	Exit access list mode.
`(config)#interface eth0`	Enter interface mode of Management Interface.
`(config-if)#ip access-group mgmt out`	Apply access group mgmt for outbound traffic to the interface.
`(config-if)#exit`	Exit interface and configure mode.

When a UDP packet for Destination Port SNMPTrap sends out of interface eth0 with any Destination address, then the match count for access rule 50 increases equal to the number of packets received. Prior to this SNMPTrap should be configured on Device (10.12.29.49) to listen to port 162.

```
    Example:
    snmp-server community SNMPTEST group network-admin vrf management
```


© 2021 IP Infusion Inc. Proprietary

```
    snmp-server host 10.12.6.86 traps version 2c SNMPTEST udp-port 162 vrf
    management
    snmp-server enable snmp  vrf management

#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap [match=5]
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When an ACL is applied on interface eth0 outbound and inbound together, then we must configure an ACL to establish a TCP connection between source 10.12.29.49 with source Port SSH to destination address 10.12.45.57. When a TCP connection is established on port SSH, then the match count for access rule 10 and 60 increases equal to the number of packets sent and received.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh [match=9]
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57[match=9]
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

Note: Use the command `clear ip access-list counters` to clear the statistics of all ACLs or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

```
#show access-lists
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet


#show access-lists summary
     IPV4 ACL mgmt
           statistics enabled
           Total ACEs Configured: 8
           Configured on interfaces:
              eth0 - ingress (Router ACL)
           Active on interfaces:
              eth0 - ingress (Router ACL)

#show access-lists expanded
```

```
IP access list mgmt
        10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
        20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
        30 permit udp any host 10.12.29.49 eq snmp
        40 permit udp any host 10.12.29.49 eq ntp
        50 permit udp host 10.12.29.49 any eq snmptrap
        60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
        70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
        80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
        default deny-all [match=4]
```

ARP ACL Overview

ARP ACL can be used to permit or deny the ARP packets, based on the ARP request or response option configured.

Topology



Figure 1-9: ARP ACL Sample Topology

ARP ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge4`	Enter interface mode.
`(config-if)#ip address`	Assign IPv4 address.
`(config-if)#exit`	Exit access list mode.
`(config)# mac access-list mac1`	Enter mac access list mode.
`(config-mac-acl)#permit 0000.3ae0.456d 0000.0000.0000 any arp request`	Create an access rule to permit specific ARP request.
`(config-mac-acl)#permit 0000.3ae0.456d 0000.0000.0000 any arp response`	Create an access rule to permit specific ARP response.
`(config-mac-acl)#permit any any ipv4`	Create an access rule to permit any IPv4 packet.
`(config-mac-acl)#exit`	Exit access list mode.
`(config)#interface ge4`	Enter interface mode.
`(config-if)#mac access-group mac1 in`	Apply access group mac1 for inbound traffic to the interface.
`(config-if)#exit`	Exit interface and configure mode.

Validation

Use the commands below to assign IP address on IXIA and ping from IXIA.

© 2021 IP Infusion Inc. Proprietary

```
#show mac access-lists
    MAC access list mac1
            10 permit host 0000.3AE0.456D any arp request [match=1]
            20 permit host 0000.3AE0.456D any arp response [match=1]
            30 permit any any ipv4 [match=1]
            default deny-all
```

ACL OVER LOOPBACK

The loopback interface ACL is the feature to be used to provide this basic level security for the management applications accessible through In-band interfaces.

Note: Refer to the command reference section for limitations, default behavior, and unsupported features.

Topology

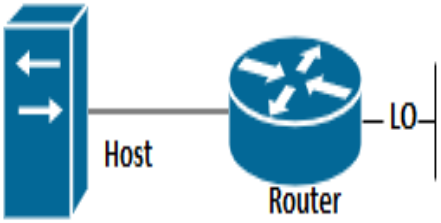


Figure 1-10: ACL Loopback Topology

Loopback ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 3.3.3.3/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 4.4.4.4/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 5.5.5.5/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 6.6.6.6/32 secondary`	Assign the IPv4 secondary address.
`(config-if)#ip address 7.7.7.7/32 secondary`	Assign the IPv4 secondary address.
`(config-if)# exit`	Exit interface mode.
`(config)#ip access-list loopback`	Create loopback access list
`(config-ip-acl)# 10 permit tcp any host 3.3.3.3 eq telnet`	Permit telnet session from any source with specific destination.
`(config-ip-acl)# 20 deny tcp any host 4.4.4.4 eq telnet`	Deny telnet session from any source with specific destination.

`(config-ip-acl)# 30 permit tcp any host 5.5.5.5 eq ssh`	Permit ssh session from any source with specific destination.
`(config-ip-acl)# 40 deny tcp any host 6.6.6.6 eq ssh`	Deny ssh session from any source with specific destination.
`(config-ip-acl)# 50 deny udp any host 6.6.6.6 eq snmp`	Deny udp from any source with specific destination.
`(config-ip-acl)# 60 deny udp any host 7.7.7.7 eq ntp`	Deny udp from any source with specific destination.
`(config-ip-acl)#exit`	Exit interface acl mode
`(config)#interface lo`	Enter interface lo mode
`(config-if)#ip access-group loopback in`	Associate loopback acl over lo interface
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit config mode

Validation

Use the commands below to validate ACL loopback.

```
OcNOS#show access-lists
IP access list loopback
        10 permit tcp any host 3.3.3.3 eq telnet [match=12]
        20 deny tcp any host 4.4.4.4 eq telnet [match=12]
        30 permit tcp any host 5.5.5.5 eq ssh
        40 deny tcp any host 6.6.6.6 eq ssh
        50 deny udp any host 6.6.6.6 eq snmp  [match=6]
        60 deny udp any host 7.7.7.7 eq ntp

OcNOS#show ip access-lists summary
 IPV4 ACL loopback
       statistics enabled
       Total ACEs Configured: 6
       Configured on interfaces:
          lo - ingress (Router ACL)
       Active on interfaces:
          lo - ingress (Router ACL)
       Configured on line vty:

OcNOS#show running-config aclmgr
ip access-list loopback
 10 permit tcp any host 3.3.3.3 eq telnet
 20 deny tcp any host 4.4.4.4 eq telnet
 30 permit tcp any host 5.5.5.5 eq ssh
 40 deny tcp any host 6.6.6.6 eq ssh
 50 deny udp any host 6.6.6.6 eq snmp
 60 deny udp any host 7.7.7.7 eq ntp
!
interface lo
 ip access-group loopback in
!
```


© 2021 IP Infusion Inc. Proprietary

ACL OVER VTY

When a telnet or ssh connection is made the OcNOS associates this connection with a virtual terminal (VTY) line. ACL over vty feature provides security for management features associated with vty.

Note: Refer to the command reference section for limitations, default behavior, and unsupported features.

Topology

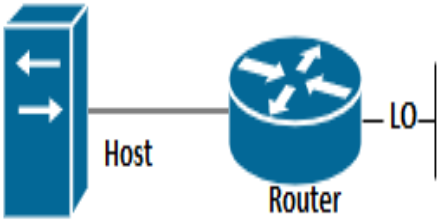


Figure 1-11: ACL VTY Topology

VTY ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 3.3.3.3/32 secondary`	Assign the IPv4 secondary address.
`(config-if)# exit`	Exit interface mode.
`(config)#ip access-list vty`	Create loopback access list
`(config-ip-acl)# 10 permit tcp any host 3.3.3.3 eq telnet`	Permit telnet session from any source with specific destination.
`(config-ip-acl)#exit`	Exit interface acl mode
`(config)#line vty`	Enter interface vty mode
`(config-all-line)#ip access-group vty in`	Associate acl over
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit config mode

Validation

```
OcNOS#sh access-lists
IP access list vty
       10 permit tcp any host 3.3.3.3 eq telnet

OcNOS#sh ip access-lists summary
IPV4 ACL vty
       statistics enabled
       Total ACEs Configured: 1
       Configured on interfaces:
       Active on interfaces:
       Configured on line vty:
       all vty lines - ingress

OcNOS#sh running-config access-list
ip access-list vty
10 permit tcp any host 3.3.3.3 eq telnet
!
line vty
ip access-group vty in
```

Timed ACL

The time range feature was introduced to be able to add a timing boundary for specified activities. The activity would start, end and repeat at the specific times set by the user. This time-range feature will enable creating "Timed ACLs". This will help service providers customize the internet data to customers based on time to increase the video traffic during weekends and reduce data traffic, restrict the internet traffic in school/college non-working hours etc.

Topology



Figure 1-12: Timed acl sample topology

Configuration with ipv4 Address

`#configure terminal`	Enter configure mode.
`(config)# time-range TIMER1`	Configure a timer
`(config-tr)#start-time 10:00 03 nov 2021`	Configure start time
`(config-tr)#end-time 18:00 03 nov 2021`	Configure end time
`(config-tr)#exit`	Exit timer
`(config)# ip access-list ACL1`	Create ip access list
`(config-ip-acl)# deny icmp host 10.1.1.1 host 10.1.2.2`	Create an acl rule to deny icmp

© 2021 IP Infusion Inc. Proprietary

(config-ip-acl)#exit	Exit Acl mode
(config)#hardware-profile filter egress-ipv4 enable	Hardware profile enable for the acl
(config)#int xe15	Enter into the interface mode
(config-if)#ip access-group ACL1 out time-range TIMER1	Apply the acl along with the timer.
(config-if)#commit	To save the changes
(config-if)#exit	Exit

Configuration with ipv6 Address

(config)# ipv6 access-list ACL1v6	Create ipv6 access list
(config-ipv6-acl)# deny any any any	Create an acl rule to deny
(config-ipv6-acl)#exit	Exit Acl mode
(config)# hardware-profile filter ingress-ipv6 enable	Hardware profile enable for the acl
(config)#int xe12	Enter into the interface mode
(config-if)# ipv6 access-group ACL1v6 in time-range TIMER1	Apply the acl along with the timer.
(config-if)#commit	To save the changes
(config-if)#exit	Exit

Configuration with mac

(config)# mac access-list ACL1mac	Create ip access list
(config-mac-acl)# deny 0000.0000.0000 1111.2222.3333 0000.0000.0000 4444.5555.6666	Create an acl rule to deny icmp
(config-mac-acl)#exit	Exit Acl mode
(config)# hardware-profile filter ingress-l2 enable	Hardware profile enable for the acl
(config)#int xe13	Enter into the interface mode
(config-if)# mac access-group ACL1mac in time-range TIMER1	Apply the acl along with the timer.
(config-if)#commit	To save the changes
(config-if)#exit	Exit

Validation

```
#sh running-config in xe15
!
interface xe15
 ip access-group ACL1 out time-range TIMER1
!
OcNOS#sh running-config in xe12
```

```
!
interface xe12
 ipv6 access-group ACL1v6 in time-range TIMER1
!
OcNOS#sh running-config in xe13
!
interface xe13
 mac access-group ACL1mac in time-range TIMER1


#sh time-range
====================================
TR handler interval: 10 seconds
====================================
TR entries: 1
Entry: 0
 name: TIMER1
 state: Pending
 frequency: none
 start time: Wed Nov  3 10:00:00 2021
 end time: Wed Nov  3 18:00:00 2021
====================================
RUNNING TR entries: 0
====================================
COMPLETED TR entries: 0
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Debounce Timer

Overview

The debounce timer avoids frequent updates (churn) to higher layer protocols during flapping of an interface. If the status of a link changes quickly from up to down and then back to up, the port debounce timer suppresses the link status notification. If the link transitions from up to down, but does not come back up, the port debounce timer delays the link status notification.

Note: Keep the following in mind when using the debounce timer:

- Debounce is not applicable for admin down operations.
- Debounce timer is supported only for physical L2 and L3 interfaces.
- The debounce flap-count refers to the number of flaps OcNOS receives while the debounce timer is running:
  - The flap-count is only updated if the timer is still running and OcNOS receives a link status event for the interface.
  - The flap-count is reset at the subsequent start of the debounce timer.
- Protocol-specific timers such as BFD which depend on the link status should be configured to minimum of 1.5 times the value of the debounce time. Otherwise it could affect the protocol states if the debounce timer is still running.

Topology

Figure 2-13 is a simple deployment using the debounce timer

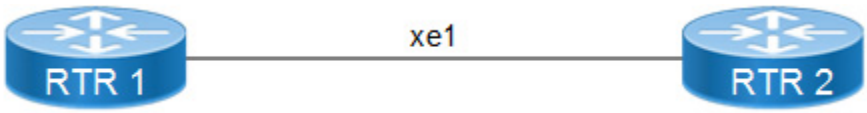


Figure 2-13: Debounce timer

Configuration

RTR 1

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Enter into interface mode
`(config)#debounce-time 4000`	Configure debounce-time as 4000ms
`(config)#exit`	Exit configure mode

RTR 2

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Enter into interface mode
`(config)#debounce-time 4000`	Configure debounce-time as 4000ms
`(config)#exit`	Exit configure mode.

Validation

```
#show running-config | i debounce
debounce-time 4000
#show interface xe1 i debounce
Debounce timer: enabled
Debounce-interval 4000 ms
Flap Count: 0
Debounce status : idle
```

RTR1 and RTR2 outputs after interface flap:

```
#show interface xe1 | i debounce
Debounce timer: enabled
Debounce-interval 4000 ms
Flap Count: 1
Last Debounce Flap : 2019 Aug 14 17:24:33 (00:00:10 ago)
Debounce status : idle

#show interface xe1 | i debounce
Debounce timer: enabled
Debounce-interval 4000 ms
Flap Count: 1
Last Debounce Flap : 2019 Aug 14 17:24:35 (00:00:16 ago)
Debounce status : idle
```

Log Messages

The following is a configuration example to log debounce timer activity:

`#configure terminal`	Enter Configure mode
`(config)#logging level nsm 7`	Enable operational log to display debounce start and end.

Example Log Messages

```
2019 Aug 14 17:24:32.532 : rtr1 : NSM : INFO : Start Debounce Timer on interface xe1,
prev_state UP new_state DOWN
2019 Aug 14 17:24:33.810 : rtr1 : NSM : INFO : Interface xe1 Flapped, prev_state UP
new_state UP,flap count 1
2019 Aug 14 17:24:36.532 : rtr1 : NSM : INFO : Debounce Timer Expired on interface xe1,
prev_state UP, new_state UP
```


© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 DHCP Client Configuration

Overview

Dynamic Host Configuration Protocol (DHCP) protocol is used for assigning dynamic IP addresses to systems on a network. Dynamic addressing allows a system to have an IP address each time it connects to the network. DHCP makes network administration easier by removing the need to manually assign a unique IP address every time a new system is added to the network. It is especially useful to manage mobile users. Once a system is configured to use DHCP, it can be automatically configured on any network that has a DHCP server.

DHCP uses a client-server model, in which the DHCP server centrally manages the IP addresses used in the network. DHCP clients obtain an IP address on lease from the DHCP server.

DHCP Client Configuration for IPv4

Before configuring the DHCP in client, make sure that DHCP server is ready and also dhcpd is running on the server machine.

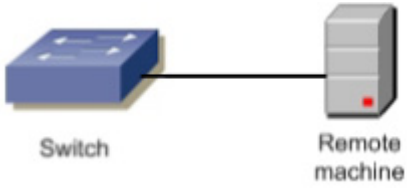


Figure 3-14: DHCP sample topology

`#configure terminal`	Enter configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This will be enabled by default.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
`(config if)#exit`	Exit interface mode.
`(config)#interface eth0`	Enter management interface mode.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the Acknowledgement from the server, it assigns the IP address to the management interface.
`(config if)#exit`	Exit interface mode.

Validation Commands

```
#show running-config dhcp
    interface xe2
     ip address dhcp
    !
    ip dhcp relay information option
```

```
#sh ip interface brief

Interface            IP-Address      Admin-Status         Link-Status
GMPLS Type
eth0                 10.12.44.20     up                   up
-
lo                   127.0.0.1       up                   up
-
lo.4                 127.0.0.1       up                   up
-
vlan1.1              unassigned      up                   down
-
xe1/1                2.2.2.3         up                   up
-
xe1/2                unassigned      down                 down
-
xe1/3                unassigned      down                 down
-
xe1/4                unassigned      up                   down
-
xe2                 *40.40.40.40     up                   down
-
xe3/1                20.20.30.1      up                   up
-
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 DHCP Relay Agent Configuration

Overview

The DHCP Relay feature was designed to forward DHCP broadcast requests as unicast packets to a configured DHCP server or servers for redundancy in different network segments.

DHCP Relay for IPv4

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.

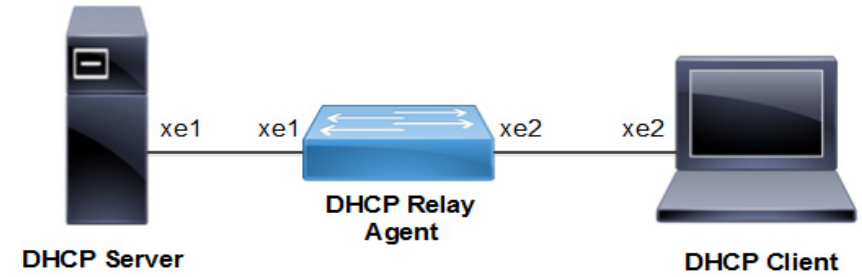


Figure 4-15: DHCP Relay Configuration

DHCP Agent

`#configure terminal`	Enter configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled by default.
`(config)#ip dhcp relay`	By default this will be enabled. It starts the ip dhcp relay service.
`(config)# ip dhcp relay address 10.10.10.2`	The relay address configured should be server interface address connected to DUT machine.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ip address 10.10.10.1/24`	Configure ipv4 address on the interface xe1.
`(config-if)#ip dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`(config if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure ipv4 address on the interface xe2.
`(config-if)#ip dhcp relay`	Relay should be configured on the interface connecting to the client.
`(config if)#exit`	Exit interface mode.

Validation Commands

```
#show running-config dhcp

ip dhcp relay address 10.10.10.2
interface xe2
```

© 2021 IP Infusion Inc. Proprietary

```
 ip dhcp relay
!
interface xe1
 ip dhcp relay uplink
!

#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
  Option 82: Disabled
  DHCP Servers configured: 10.10.10.2
  Interface                Uplink/Downlink
  ---------                -------------
  xe2                      Downlink
  xe1                      Uplink

#show ip dhcp relay address
 VRF Name: default
  DHCP Servers configured: 10.10.10.2
```

DHCP Relay for IPv6 Configuration

DHCP Agent

`#configure terminal`	Enter configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled in default.
`(config)#ipv6 dhcp relay`	By default this will be enabled. It starts the ipv6 dhcp relay service.
`(config)#ipv6 dhcp relay address 2001::2`	The relay address configured should be server interface address connected to DUT machine.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ipv6 address 2001::1/64`	Configure ipv6 address on the interface xe1.
`(config-if)#ipv6 dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`(config if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ipv6 address 2002::1/64`	Configure ipv6 address on the interface xe2.
`(config-if)#ipv6 dhcp relay`	Relay should be configured on the interface connecting to the client.
`(config if)#exit`	Exit interface mode.

Validation Commands

```
#sh ipv6 dhcp relay address

VRF Name: default
  DHCPv6 Servers configured: 2001::2

#show running-config dhcp
```


© 2021 IP Infusion Inc. Proprietary

```
Ipv6 dhcp relay address 2001::2
 interface xe2
 ipv6 dhcp relay
!
interface xe1
 ipv6 dhcp relay uplink
!
```

DHCP Relay option 82

This section contains examples of DHCP Relay option-82 configuration. DHCP option 82 (Agent Information Option) provides additional security when DHCP is used to allocate network addresses. It enables the DHCP relay agent to prevent DHCP client requests from untrusted sources. Service Providers use remote identifier (option 82 sub option 2) for troubleshooting, authentication, and accounting. The **DHCP Option 82 Remote ID** Format feature adds support for the interpretation of **remote-IDs** that are inserted by end users. On the relay agent, you can configure information option to add option 82 information to DHCP requests from the clients before forwarding the requests to the DHCP server. When configured with option 82 and remote-id, the server will receive the DHCP request packet with Agent Circuit ID and remote-id.

The two examples below, show how to configure the DHCP Relay option 82:

- Configuration of DHCP Relay option 82 on a physical interface with Agent information and remote-id.
- Configuration of DHCP Relay option 82 on a VLAN interface with Agent information and remote-id.

Topology

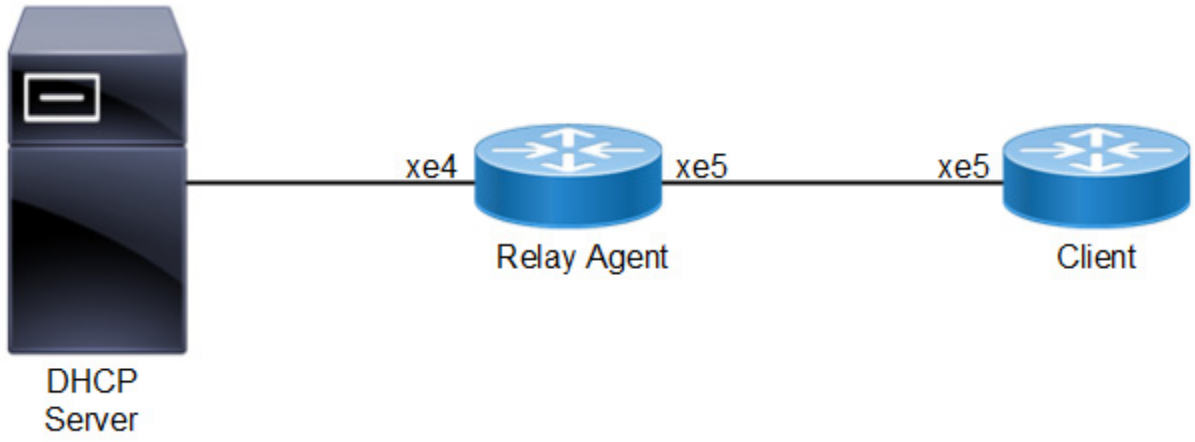


Figure 4-16: DHCP 82 interface topology

Physical Interface Configuration

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnet 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for `DHCP OFFER` packets to reach the Relay Agent.

Relay agent

`#configure terminal`	Enter configure mode.
`(config)#ip dhcp relay`	Enable DHCP Relay
`(config)#ip dhcp relay information option remote-id hostname`	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82. String support is also provided for remote-id.
`(config)#interface xe5`	Enter interface mode.
`(config-if)#ip address 10.10.20.2/24`	Add IP address
`(config-if)#ip dhcp relay`	Configure DHCP relay for the interface connecting to client.
`(config-if)#exit`	Exit from interface mode
`(config)#interface xe4`	Enter interface mode
`(config-if)#ip dhcp relay uplink`	Configure DHCP relay uplink for the interface connecting to server.
`(config-if)#exit`	Exit interface mode.

Client

`#configure terminal`	Enter configure mode.
`(config)#interface xe5`	Enter interface mode.
`(config-if)#ip address dhcp`	Configure IP address DHCP
`(config-if)#exit`	Exit from interface mode

Validation

Relay Agent

```
#show running-config dhcp
!
ip dhcp relay information option remote-id hostname
ip dhcp relay address 192.168.1.2
interface xe5
 ip dhcp relay
!
interface xe4
 ip dhcp relay uplink
!

#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
  Option 82: Enabled
  Remote Id: OcNOS
  DHCP Servers configured: 192.168.1.2
  Interface               Uplink/Downlink
  ---------               -------------
  xe5                     Downlink
  xe4                     Uplink
```


© 2021 IP Infusion Inc. Proprietary

Client

```
#show ip interface brief | include xe5
xe5            *10.10.20.10     up                    up

Packet captured at DHCP Server

Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x4e61176c
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.10.20.2 (10.10.20.2)
    Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Discover)
        Length: 1
        DHCP: Discover (1)
    Option: (55) Parameter Request List
        Length: 3
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (28) Broadcast Address
        Parameter Request List Item: (3) Router
    Option: (60) Vendor class identifier
        Length: 39
        Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
    Option: (82) Agent Information Option
        Length: 12
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 3
            Agent Circuit ID: 786535
         Option 82 Suboption: (2) Agent Remote ID
            Length: 5
            Agent Remote ID: 4f634e4f53
    Option: (255) End
        Option End: 255
    Padding
```

Physical Interface Configuration with non-default vrf.

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnet 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for DHCP OFFER packets to reach the Relay Agent.

Relay agent

`#configure terminal`	Enter configure mode.
`(config)#ip dhcp relay`	Enable DHCP Relay.
`(config)#ip vrf vrf_dhcp`	Configuring non default vrf vrf_dhcp
`(config-vrf)#ip dhcp relay information option remote-id hostname`	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82 on non default vrf.. String support is also provided for remote-id.
`(config-vrf)#ip dhcp relay address 192.168.1.2`	Configure DHCP relay address in non default vrf.
`(config)#interface xe5`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf_dhcp`	Configure vrf forwarding for vrf_dhcp.
`(config-if)#ip address 10.10.20.2/24`	Add IP address.
`(config-if)#ip dhcp relay`	Configure DHCP relay for the interface connecting to client.
`(config-if)#exit`	Exit from interface mode
`(config)#interface xe4`	Enter interface mode
`(config-if)#ip vrf forwarding vrf_dhcp`	Configure vrf forwarding for vrf_dhcp.
`(config-if)#ip dhcp relay uplink`	Configure DHCP relay uplink for the interface connecting to server.
`(config-if)#ip address 192.168.1.4/24`	Add IP address.
`(config-if)#exit`	Exit interface mode.

Client

`#configure terminal`	Enter configure mode.
`(config)#interface xe5`	Enter interface mode.
`config-if)#ip vrf forwarding vrf_dhcp`	Configure ip vrf forwarding for non default vrf.
`(config-if)#ip address dhcp`	Configure IP address DHCP.
`(config-if)#exit`	Exit from interface mode.

Validation

Relay Agent

```
#show running-config dhcp
!
ip vrf vrf_dhcp
 ip dhcp relay information option remote-id hostname
 ip dhcp relay address 192.168.1.2
interface xe5
 ip dhcp relay
!
interface xe4
 ip dhcp relay uplink
!
```


© 2021 IP Infusion Inc. Proprietary

```
#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: vrf_dhcp
  Option 82: Enabled
  Remote Id: OcNOS
  DHCP Servers configured: 192.168.1.2
  Interface                Uplink/Downlink
  ---------                -------------
  xe5                      Downlink
  xe4                      Uplink
```

Client

```
#show ip interface brief | include xe5
xe5            *10.10.20.10     up                    up

Packet captured at DHCP Server

Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x4e61176c
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.10.20.2 (10.10.20.2)
    Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Discover)
        Length: 1
        DHCP: Discover (1)
    Option: (55) Parameter Request List
        Length: 3
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (28) Broadcast Address
        Parameter Request List Item: (3) Router
    Option: (60) Vendor class identifier
        Length: 39
        Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
    Option: (82) Agent Information Option
        Length: 12
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 3
            Agent Circuit ID: 786535
         Option 82 Suboption: (2) Agent Remote ID
            Length: 5
            Agent Remote ID: 4f634e4f53
```

```
        Option: (255) End
            Option End: 255
        Padding

    Sample DHCP configuration for using Remote-id

    class "remote-id" {
            match if option agent.remote-id = OcNOS
    } # remote-id

    subnet 10.10.20.0 netmask 255.255.255.0 {
            pool {
                    allow members of                "remote-id";
                    default-lease-time               600;
                    max-lease-time                    7200;
                    range                           10.10.20.3 10.10.10.100;
                    option routers                  10.10.20.2;
                    option broadcast-address        10.10.20.255;
                    option subnet-mask              255.255.255.0;
                    option domain-name-servers      4.2.2.2;
    }
```

VLAN Interface Configuration

Topology



Figure 4-17: DHCP 82 vlan topology

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnets 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for DHCP OFFER packets to reach the Relay Agent. In the above topology, vlan 20 is part of interface xe5 in relay Agent and xe5 in Client.

Relay Agent

t

`#configure terminal`	Enter configure mode.
`(config)#ip dhcp relay`	Enable DHCP Relay

© 2021 IP Infusion Inc. Proprietary

(config)#ip dhcp relay information option remote-id hostname	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82. String support is also provided for remote-id.
(config)#ip dhcp relay address 192.168.1.2	Configure DHCP relay address
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge
(config)#vlan 2-100 bridge 1 state enable	Enable some VLANs
(config)#interface xe5	Enter interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode hybrid	Configure switchport mode
(config-if)#switchport hybrid allowed vlan all	Enable vlan
(config-if)#exit	Exit from interface mode
(config)#interface vlan1.20	Enter interface mode for the vlan interface towards client.
(config-if)#ip address 10.10.20.2/24	Add IP address
(config-if)#ip dhcp relay	Configure DHCP relay on the vlan interface connecting to client.
(config-if)#exit	Exit from interface mode
(config)#interface xe4	Enter interface mode
(config-if)#ip dhcp relay uplink	Configure DHCP relay uplink for the interface connecting to server.
(config-if)#ip address 192.168.1.4/24	Add IP address
(config-if)#exit	Exit interface mode.

Client

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge
(config)#vlan 2-100 bridge 1 state enable	Enable VLANs
(config)#interface xe5	Enter interface mode.
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode hybrid	Configure switchport mode
(config-if)#switchport hybrid allowed vlan add 20 egress-tagged enable	Enable vlan
(config-if)#exit	Exit from interface mode
(config)#interface vlan1.20	Enter interface mode for the vlan interface which connects relay.
(config-if)#ip address dhcp	Configure IP address DHCP
(config-if)#exit	Exit from interface mode

Validation

Relay Agent

```
#show running-config dhcp
!
ip dhcp relay information option remote-id hostname
ip dhcp relay address 192.168.1.2
!
interface vlan1.20
 ip dhcp relay
!
interface xe4
 ip dhcp relay uplink
!


#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
  Option 82: Enabled
  Remote Id: ocnos
  DHCP Servers configured: 192.168.1.2
  Interface                Uplink/Downlink
  ---------                -------------
  Vlan1.20                 Downlink
  xe4                      Uplink
```

Client

```
#show ip interface brief |include vlan1.20
vlan1.20            *10.10.20.10     up                    up

Packet captured at DHCP Server

Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x59591459
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.10.20.2 (10.10.20.2)
    Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Discover)
        Length: 1
```


© 2021 IP Infusion Inc. Proprietary

```
    DHCP: Discover (1)
 Option: (55) Parameter Request List
    Length: 3
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (28) Broadcast Address
    Parameter Request List Item: (3) Router
 Option: (60) Vendor class identifier
    Length: 39
    Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
 Option: (82) Agent Information Option
    Length: 17
    Option 82 Suboption: (1) Agent Circuit ID
        Length: 8
        Agent Circuit ID: 766c616e312e3230
    Option 82 Suboption: (2) Agent Remote ID
        Length: 5
        Agent Remote ID: 4f634e4f53

Option: (255) End
    Option End: 255
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 DHCP Relay Agent Over L3VPN Configuration

The DHCP Relay feature was designed to forward DHCP broadcast requests as unicast packets to a configured DHCP server or servers for redundancy. In the L3VPN case, there is a special tunnel which gets created through which all the communication happens. In OcNOS, the interface created is named as tunmpls. This tunnel name is not exposed to the OcNOS control plane .This interface is directly created in the kernel.

DHCP Relay Over L3 VPN for IPv4

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.

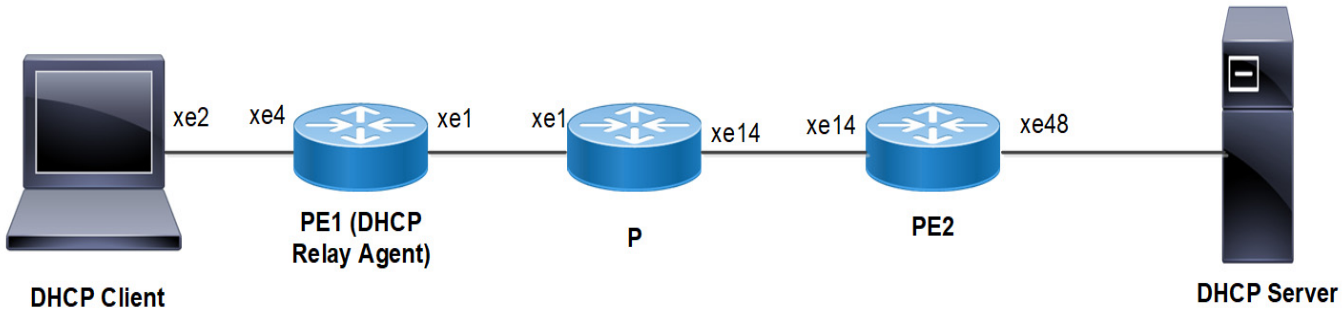


Figure 5-18: DHCP Relay Over L3 VPN Configuration

DHCP Client

`#configure terminal`	Enter configure mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ip address dhcp`	Enable DHCP on interface
`(config-if)#commit`	Commit the candidate configuration to the running configuration

PE1(DHCP Relay Agent)

`#configure terminal`	Enter configure mode.
`(config)#ip dhcp relay`	By default this will be enabled. It starts the ip dhcp relay service.
`(config)#ip vrf vrf1`	Configuring non default vrf vrf1
`(config-vrf)# rd 10:10`	Assign a route distinguisher to VRF
`(config-vrf)# route-target both 10:10`	Configure a route target for vrf1.
`(config-vrf)#ip dhcp relay address 11.11.0.1`	Configure DHCP server address.
`(config-vrf)# ip dhcp relay uplink l3vpn`	configure IPv4 DHCP Relay over L3VPN.
`(config)#interface xe4`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf1`	Configure vrf forwarding for vrf1
`(config-if)#ip address 50.50.50.1/24`	Add IP address.
`(config-if)#ip dhcp relay`	Configure DHCP relay for the interface connecting to client.
`(config-if)#exit`	Exit from interface mode
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 1.1.1.1/32 secondary`	Set an IP address on the interface
`(config-if)#exit`	Exit from interface mode
`(config)#router ldp`	Enter the Router LDP mode.
`(config-router)#router-id 1.1.1.1`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode
`(config)#interface xe1`	Enter interface mode
`(config-if)# ip address 10.1.1.1/24`	Add IP address.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from interface mode
`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 1.1.1.1/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`(config-router)#network 10.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.
`(config)# router bgp 100`	Enter the Router BGP mode, ASN: 100
`(config-router)# bgp router-id 1.1.1.1`	Configure a fixed Router ID (1.1.1.1)
`(config-router)# neighbor 3.3.3.3 remote-as 100`	Configuring PE2 as iBGP neighbor using it's loopback IP
`(config-router)# neighbor 3.3.3.3 update-source lo`	Source of routing updates as loopback
`(config-router)# address-family ipv4 unicast`	Entering into IPV4 unicast address family
`(config-router-af)# neighbor 3.3.3.3 activate`	Activate the neighbor in the IPV4 address family
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)# address-family vpnv4 unicast`	Entering into address family mode as vpnv4

© 2021 IP Infusion Inc. Proprietary

(config-router-af)# neighbor 3.3.3.3 activate	Activate the neighbor in the vpnv4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv4 vrf vrf1	Entering into address family mode as ipv4 vrf vrf1
(config-router-af)# redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# commit	Commit the candidate configuration to the running configuration

P

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 2.2.2.2/32 secondary	Set an IP address on the interface
(config-if)#exit	Exit from interface mode
(config)#router ldp	Enter the Router LDP mode.
(config-router)#router-id 2.2.2.2	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode
(config)#interface xe14	Enter interface mode
(config-if)# ip address 20.1.1.1/24	Add IP address.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#interface xe1	Enter interface mode
(config-if)# ip address 10.1.1.2/24	Add IP address.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#network 3.3.3.3/32 area 0.0.0.0	Advertise loopback address in OSPF.
(config-router)#network 20.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#network 10.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.
(config)# commit	Commit the candidate configuration to the running configuration

PE2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrf1`	Configuring non default vrf vrf1
`(config-vrf)# rd 10:10`	Assign a route distinguisher to VRF
`(config-vrf)# route-target both 10:10`	Configure a route target for vrf1.
`(config)#interface xe48`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf1`	Configure vrf forwarding for vrf1
`(config-if)# commit`	Commit the candidate config
`(config-if)#ip address 11.11.0.2/24`	Add IP address.
`(config-if)#exit`	Exit from interface mode
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 3.3.3.3/32 secondary`	Set an IP address on the interface
`(config-if)#exit`	Exit from interface mode
`(config)#router ldp`	Enter the Router LDP mode.
`(config-router)#router-id 3.3.3.3`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode
`(config)#interface xe14`	Enter interface mode
`(config-if)# ip address 20.1.1.2/24`	Add IP address.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from interface mode
`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 3.3.3.3/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`(config-router)#network 20.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.
`(config)# router bgp 100`	Enter the Router BGP mode, ASN: 100
`(config-router)# bgp router-id 3.3.3.3`	Configure a fixed Router ID (3.3.3.3)
`(config-router)# neighbor 1.1.1.1 remote-as 100`	Configuring PE1 as iBGP neighbor using it's loopback IP
`(config-router)# neighbor 1.1.1.1 update-source lo`	Source of routing updates as loopback
`(config-router)# address-family ipv4 unicast`	Entering into IPV4 unicast address family
`(config-router-af)# neighbor 1.1.1.1 activate`	Activate the neighbor in the IPV4 address family
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)# address-family vpnv4 unicast`	Entering into address family mode as vpnv4
`(config-router-af)# neighbor 1.1.1.1 activate`	Activate the neighbor in the vpnv4 address family
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)# address-family ipv4 vrf vrf1`	Entering into address family mode as ipv4 vrf vrf1

© 2021 IP Infusion Inc. Proprietary

`(config-router-af)# redistribute connected`	Redistribute connected routes.
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)# commit`	Commit the candidate configuration to the running configuration

Validation

PE1 (DHCP Relay Agent)

```
PE1#show running-config dhcp
ip vrf vrf1
 ip dhcp relay address 11.11.0.1
 ip dhcp relay uplink l3vpn
interface xe4
 ip dhcp relay

PE1#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: vrf1
  Option 82: Disabled
  DHCP Servers configured: 11.11.0.1

  Interface                Uplink/Downlink
  ---------                ---------------
  xe4                      Downlink
  l3vpn                    uplink
Incoming DHCPv4 packets which already contain relay agent option are FORWARDED u
nchanged.
```

PE1#show ip dhcp relay address

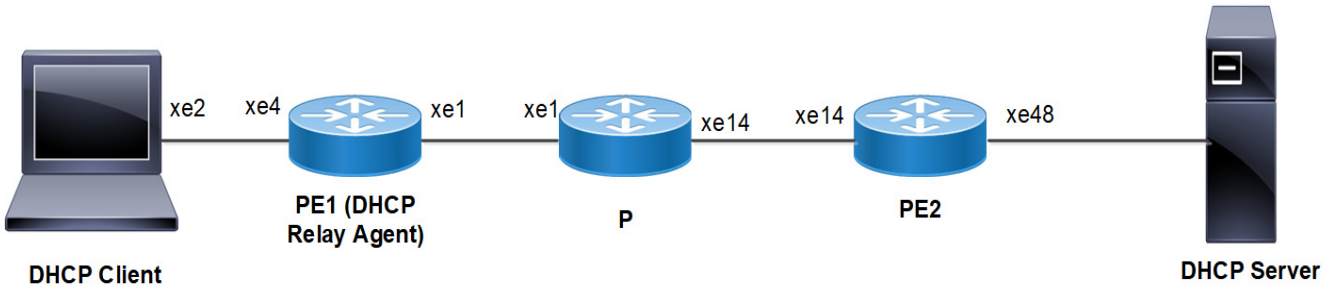
```
VRF Name: vrf1
  DHCP Servers configured: 11.11.0.1

Incoming DHCPv4 packets which already contain relay agent option are FORWARDED u
nchanged.
```

DHCP Client

```
#show ip interface brief | include xe2
  xe5   *50.50.50.2  up     up
```

DHCP Relay Over L3 VPN for IPv6

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.



.

Figure 5-19: Figure 6-7: DHCP Relay Over L3 VPN Configuration

DHCP Client

`#configure terminal`	Enter configure mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ipv6 address dhcp`	Enable DHCP on interface
`(config-if)#commit`	Commit the candidate configuration to the running configuration

© 2021 IP Infusion Inc. Proprietary

PE1(DHCP Relay Agent)

`#configure terminal`	Enter configure mode.
`(config)#ipv6 dhcp relay`	By default this will be enabled. It starts the ipv6 dhcp relay service.
`(config)#ip vrf vrf1`	Configuring non default vrf vrf1
`(config-vrf)# rd 10:10`	Assign a route distinguisher to VRF
`(config-vrf)# route-target both 10:10`	Configure a route target for vrf1.
`(config-vrf)# ipv6 dhcp relay address 2002::1`	Configure DHCP server address.
`(config-vrf)# ipv6 dhcp relay uplink l3vpn`	configure IPv6 DHCP Relay over L3VPN.
`(config)#interface xe4`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf1`	Configure vrf forwarding for vrf1
`(config-if)# ipv6 address 2001::1/64`	Add IPv6 address.
`(config-if)#ipv6 dhcp relay`	Configure DHCP relay for the interface connecting to client.
`(config-if)#exit`	Exit from interface mode
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 1.1.1.1/32 secondary`	Set an IP address on the interface
`(config-if)#exit`	Exit from interface mode
`(config)#router ldp`	Enter the Router LDP mode.
`(config-router)#router-id 1.1.1.1`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode
`(config)#interface xe1`	Enter interface mode
`(config-if)# ip address 10.1.1.1/24`	Add IP address.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from interface mode
`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 1.1.1.1/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`(config-router)#network 10.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.
`(config)# router bgp 100`	Enter the Router BGP mode, ASN: 100
`(config-router)# bgp router-id 1.1.1.1`	Configure a fixed Router ID (1.1.1.1)
`(config-router)# neighbor 3.3.3.3 remote-as 100`	Configuring PE2 as iBGP neighbor using it's loopback IP
`(config-router)# neighbor 3.3.3.3 update-source lo`	Source of routing updates as loopback
`(config-router)# address-family ipv4 unicast`	Entering into IPV4 unicast address family
`(config-router-af)# neighbor 3.3.3.3 activate`	Activate the neighbor in the IPV4 address family
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)# address-family vpnv4 unicast`	Entering into address family mode as vpnv4

`(config-router-af)# neighbor 3.3.3.3 activate`	Activate the neighbor in the vpnv4 address family
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)# address-family vpnv6 unicast`	Entering into address family mode as vpnv6
`(config-router-af)# neighbor 3.3.3.3 activate`	Activate the neighbor in the vpnv6 address family
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)# address-family ipv4 vrf vrf1`	Entering into address family mode as ipv4 vrf vrf1
`(config-router-af)# redistribute connected`	Redistribute connected routes.
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)# address-family ipv6 vrf vrf1`	Entering into address family mode as ipv6 vrf vrf1
`(config-router-af)# redistribute connected`	Redistribute connected routes.
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)# commit`	Commit the candidate configuration to the running configuration

© 2021 IP Infusion Inc. Proprietary

P

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 2.2.2.2/32 secondary`	Set an IP address on the interface
`(config-if)#exit`	Exit from interface mode
`(config)#router ldp`	Enter the Router LDP mode.
`(config-router)#router-id 2.2.2.2`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode
`(config)#interface xe14`	Enter interface mode
`(config-if)# ip address 20.1.1.1/24`	Add IP address.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from interface mode
`(config)#interface xe1`	Enter interface mode
`(config-if)# ip address 10.1.1.2/24`	Add IP address.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from interface mode
`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 3.3.3.3/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`(config-router)#network 20.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`(config-router)#network 10.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.
`(config)# commit`	Commit the candidate configuration to the running configuration

PE2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrf1`	Configuring non default vrf vrf1
`(config-vrf)# rd 10:10`	Assign a route distinguisher to VRF
`(config-vrf)# route-target both 10:10`	Configure a route target for vrf1.
`(config)#interface xe48`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf1`	Configure vrf forwarding for vrf1
`(config-if)# commit`	Commit the candidate config
`(config-if)# ipv6 address 2002::2/64`	Add IPv6 address.
`(config-if)#exit`	Exit from interface mode
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 3.3.3.3/32 secondary`	Set an IP address on the interface
`(config-if)#exit`	Exit from interface mode
`(config)#router ldp`	Enter the Router LDP mode.
`(config-router)#router-id 3.3.3.3`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode
`(config)#interface xe14`	Enter interface mode
`(config-if)# ip address 20.1.1.2/24`	Add IP address.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from interface mode
`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 3.3.3.3/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`(config-router)#network 20.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.
`(config)# router bgp 100`	Enter the Router BGP mode, ASN: 100
`(config-router)# bgp router-id 3.3.3.3`	Configure a fixed Router ID (3.3.3.3)
`(config-router)# neighbor 1.1.1.1 remote-as 100`	Configuring PE1 as iBGP neighbor using it's loopback IP
`(config-router)# neighbor 1.1.1.1 update-source lo`	Source of routing updates as loopback
`(config-router)# address-family ipv4 unicast`	Entering into IPV4 unicast address family
`(config-router-af)# neighbor 1.1.1.1 activate`	Activate the neighbor in the IPV4 address family
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)# address-family vpnv4 unicast`	Entering into address family mode as vpnv4
`(config-router-af)# neighbor 1.1.1.1 activate`	Activate the neighbor in the vpnv4 address family
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)# address-family vpnv6 unicast`	Entering into address family mode as vpnv6

© 2021 IP Infusion Inc. Proprietary

(config-router-af)# neighbor 1.1.1.1 activate	Activate the neighbor in the vpnv6 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv4 vrf vrf1	Entering into address family mode as ipv4 vrf vrf1
(config-router-af)# redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv6 vrf vrf1	Entering into address family mode as ipv6 vrf vrf1
(config-router-af)# redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# commit	Commit the candidate configuration to the running configuration

Validation

PE1 (DHCP Relay Agent)

```
PE1#show running-config dhcp
ip vrf vrf1
 ipv6 dhcp relay address 2002::1
 ipv6 dhcp relay uplink l3vpn
interface xe4
 ipv6 dhcp relay

PE1#show ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: vrf1
  Option 82: Enabled
  DHCPv6 Servers configured: 2002::1
  DHCPv6 IA_PD Route injection: Disabled
  Interface                Uplink/Downlink
  ---------                -------------
  xe4                      Downlink
  l3vpn                    uplink
PE1#show ip dhcp relay address
VRF Name: vrf1
  DHCPv6 Servers configured: 2002::1
```

DHCP Client

```
#show ipv6 interface brief | include xe2
  xe5   *2001::200  up     up
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 6 DHCP Snooping

Overview

DHCP snooping is a series of techniques applied to ensure the security of an existing DHCP infrastructure. It is a security feature that acts like a fire wall between untrusted hosts and trusted DHCP servers. It is a layer-2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable.

The fundamental use case of DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. Rogue DHCP servers are often used in ‘man-in the middle’ or ‘Denial of Service’ attacks from malicious purpose. Similarly DHCP clients (rogue) can also cause ‘Denial of Service’ attacks by continuously requesting for IP addresses causing address depletion in the DHCP server.

The DHCP snooping feature performs the following activities:

- Validates DHCP messages received from un-trusted sources and filters out invalid messages.
- Rate-limits DHCP traffic from trusted and un-trusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about un-trusted hosts with leased IP addresses.
- Utilizes the DHCP snooping binding database to validate subsequent requests from un-trusted hosts.
- To retain the DHCP snooping bindings database across reloads, it is stored in a persistent file on switch itself. Upon reload, the switch restores binding database from the persistent file. On NTP sync, the lease time of the binding entries gets re-adjusted based on the timestamp that was written in the persistent file. The switch keeps the file updated by writing to the file periodically (default interval 300 seconds).

  Note: To ensure the accuracy of lease time adjustment, NTP should be configured on the snooper.
- When DHCP snooping is used over MLAG, the DHCP snooping binding database syncing will be happening among the peers via IDL.

DHCP snooping with provider bridge is not supported.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

Topology

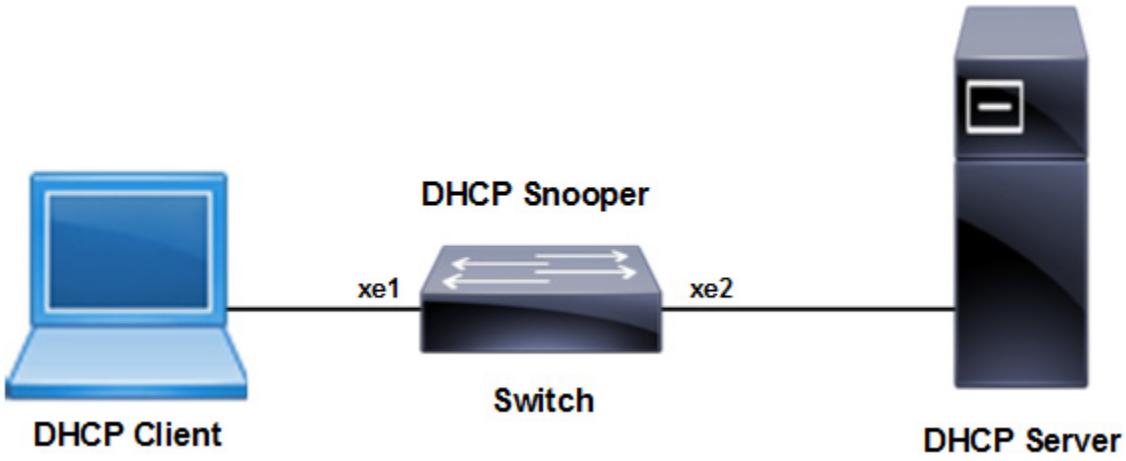


Figure 6-20: DHCP snooping

Configuration Guidelines

When configuring DHCP snooping, follow these guidelines:

- DHCP snooping is not active until you enable the feature on at least one VLAN, and enable DHCP snooping globally on the switch.
- Before globally enabling DHCP snooping on the switch, make sure that the device acting as the DHCP server is configured and enabled.
- If a Layer 2 LAN port is connected to a DHCP server, configure the port as trusted by entering the `ip dhcp snooping trust interface` configuration command.
- If a Layer 2 LAN port is connected to a DHCP client, configure the port as un-trusted by entering the `no ip dhcp snooping trust interface` configuration command.

Procedures

The following subsections provide examples of how to enable and configure DHCP Snooping.

Enable DHCP Snooping Globally

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Create mstp or ieee vlan-bridge.
`(config)#ip dhcp snooping bridge 1`	Enable DHCP Snooping on the bridge

© 2021 IP Infusion Inc. Proprietary

Enable DHCP Snooping on a VLAN

`configure terminal`	Enter configure mode.
`(config)#vlan 2 bridge 1`	Configure a vlan for the bridge.
`(config)#ip dhcp snooping vlan 2 bridge 1`	Enable DHCP Snooping on the vlan 2

Configure Ports connected to DHCP Sserver and DHCP Client

`#configure terminal`	Enter the configure mode
`(config)#interface xe1`	Specify the interface xe1 to be configured, and Enter interface mode
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate the interface `xe1` with bridge-group `1`.
`(config-if)#switchport mode access`	Configure the port as an access port
`(config-if)#switchport access vlan 2`	Bind the interface vlan 2 to the port.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Specify interface `xe2` to be configured connected to server.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate interface `xe2` with bridge-group `1`.
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#switchport access vlan 2`	Bind the interface vlan 2 to the port.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit the config mode.

Configure Trusted and Untrusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as untrusted port

In this example, xe1 is connected to the DHCP client and xe2 is connected to the DHCP server.

- Configure xe1 connected to DHCP client as un-trusted port.
- Configure xe2 connected to the DHCP server as trusted port.

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Specify the interface to be configured
`(config-if)#no ip dhcp snooping trust`	Disable the port as trusted.

DHCP Snooping Operation

1. Configure DHCP server that is connected to DHCP Snooper through trusted port.
2. Request an ip address from the DHCP client connected through the un-trusted port.

3. DHCP client broadcast the DHCP DISCOVER message to the switch.
4. DHCP server responds to the DHCP DISCOVER message with DHCP offer message to the client.
5. Once the DHCP OFFER is received by the client, it sends an DHCP REQUEST to the server.
6. DHCP server validates the request from the client and sends DHCP ACK with the offered ip address to the client with the lease time.
7. DHCP Snooper creates an entry for the above operation into the binding table which includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.
8. DHCP Snooper clears the entry in the binding table once the client sends the DHCP RELEASE or lease time is expired.

Note: On snooper once lease time becomes 0 for an entry, it is removed from the bind table within 10 sec.

Validation

The `show running-config ip dhcp snooping` command displays the DHCP snooping commands configured on the device in question.

```
#show running-config ip dhcp snooping
!
!
ip dhcp snooping bridge 1
ip dhcp snooping vlan 2 bridge 1
interface xe2
 ip dhcp snooping trust
!
```

The `show ip dhcp snooping bridge 1` command displays the configured information about DHCP Snooping.

```
#show ip dhcp snooping bridge 1

Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Disabled
Verification of hwaddr field is                       : Disabled
Strict validation of DHCP packet is                   : Disabled
Rate limit(pps)                                       : 200
DB Write Interval(secs)                               : 300
DHCP snooping is configured on following VLANs        : 2
DHCP snooping is operational on following VLANs       : 2


DHCP snooping IP Source Guard is configured on the following Interface

Interface               Trusted
---------------         -------
xe2                     Yes
```

 © 2021 IP Infusion Inc. Proprietary

The `show ip dhcp snooping binding bridge 1` command displays the binding table entries associated with un-trusted interfaces.

```
#show ip dhcp snooping bridge 1

Bridge Group                                    : 1
DHCP snooping is                                : Enabled
DHCP snooping option82 is                       : Disabled
Verification of hwaddr field is                 : Disabled
Strict validation of DHCP packet is             : Disabled
Rate limit(pps)                                 : 200
DB Write Interval(secs)                         : 300
DHCP snooping is configured on following VLANs  : 2
DHCP snooping is operational on following VLANs : 2
DHCP snooping trust is configured on the following Interfaces
Interface  Trusted
--------   -------
  xe2        Yes
DHCP snooping IP Source Guard is configured on the following Interfaces
Interface               Source Guard
---------------         ------------
```

DHCP Snooping with Option-82

When DHCP snooping with Option-82 is enabled on the switch, following behavior is expected:

1. The host generates a DHCP request and broadcasts it on the network.
2. When the switch receives DHCP request, it adds option-82 information in the packet.
3. If the IP address of the relay agent is configured, the switch adds the IP address in the DHCP packet.
4. The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
5. The DHCP server receives the packet. If the server is option-82 capable, it can use the information in the option-82 fields to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. The DHCP server then echoes the option-82 field in the DHCP reply.
6. The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch verifies that it originally inserted the option-82 data by inspecting the remote id and circuit id fields. The switch removes the option-82 field and forwards the packet to the switch port that connects to DHCP client that sent the DHCP request.

Procedures

The following subsections provide examples of how to configure DHCP snooping with option-82.

The topology is the same as Figure 6-20.

Enable DHCP Snooping Globally

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Create mstp or ieee vlan-bridge.
`(config)#ip dhcp snooping bridge 1`	Enable DHCP Snooping on the bridge

Enable DHCP Snooping on a VLAN

`configure terminal`	Enter configure mode.
`(config)#vlan 2 bridge 1`	Configure a vlan for the bridge.
`(config)#ip dhcp snooping vlan 2 bridge 1`	Enable DHCP Snooping on the vlan 2

Configure Ports connected to DHCP Server and DHCP Client

`#configure terminal`	Enter the configure mode
`(config)#interface xe1`	Specify the interface xe1 to be configured, connected to client and Enter interface mode
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate the interface xe1 with bridge-group 1.
`(config-if)#switchport mode access`	Configure the port as an access port
`(config-if)#switchport access vlan 2`	Bind the interface vlan 2 to the port.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Specify interface xe2 to be configured connected to server.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate interface xe2 with bridge-group 1.
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#switchport access vlan 2`	Bind the interface vlan 2 to the port.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit the config mode.

Configure Trusted and Untrusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as untrusted port

In this example, xe1 is connected to the DHCP client and xe2 is connected to the DHCP server.

- Configure xe1 connected to DHCP client as un-trusted port.
- Configure xe2 connected to the DHCP server as trusted port.

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Specify the interface to be configured
`(config-if)#no ip dhcp snooping trust`	Disable the port as trusted.
`#configure terminal`	Enter configure mode.
`(config)#interface xe2`	Specify the interface to be configured
`(config-if)#ip dhcp snooping trust`	Enable the port as trusted.

© 2021 IP Infusion Inc. Proprietary

Enable option-82

`#configure terminal`	Enter configure mode.
`(config)# ip dhcp snooping information option bridge 1`	Configure DHCP snooping information option-82

Validation

The `show running-config ip dhcp snooping` command displays the DHCP snooping commands configured on the device.

```
#show running-config ip dhcp snooping
!
!
ip dhcp snooping bridge 1
ip dhcp snooping information option bridge 1
ip dhcp snooping vlan 2 bridge 1
interface xe2
 ip dhcp snooping trust
!

#show ip dhcp snooping bridge 1

Bridge Group                                    : 1
DHCP snooping is                                : Enabled
DHCP snooping option82 is                       : Enabled
Verification of hwaddr field is                 : Disabled
Strict validation of DHCP packet is             : Disabled
Rate limit(pps)                                 : 200
DB Write Interval(secs)                         : 300
DHCP snooping is configured on following VLANs  : 2
DHCP snooping is operational on following VLANs : 2

DHCP snooping trust is configured on the following Interfaces

Interface               Trusted
---------------         -------
xe2                     Yes

DHCP snooping IP Source Guard is configured on the following Interfaces

Interface               Source Guard
---------------             ------------

#show ip dhcp snooping binding bridge 1

Total number of static IPV4 entries               : 0
Total number of dynamic IPV4 entries              : 1
Total number of static IPV6 entries               : 0
Total number of dynamic IPV6 entries              : 0
```

```
MacAddress           IpAddress         Lease (sec) Type            VLAN   Interface
------------------           ---------------      ----------     -----------------  ---
----   -----------
6400.6afc.3ba1       192.168.1.2       600         dhcp-snooping   2         xe1
```

Sample server dhcpd.conf for option-82

This example shows a server `dhcpd.conf` file for option-82 with `remote-id` and `circuit-id` suboptions.

```
Remote-id :
class "remote-id" {
match if option agent.remote-id = cc:37:ab:56:6d:80;--->Points to Snooping switch eth0
Mac address.
} # remote-id
subnet 192.168.1.0 netmask 255.255.255.0 {
pool {
        option subnet-mask 255.255.255.0;
        allow members of "remote-id";
        range 192.168.1.2 192.168.1.100;
        default-lease-time 600;
        max-lease-time 600;
        option subnet-mask 255.255.255.0;
        option domain-name "Domain1.com";
        option domain-name-servers 23.32.23.32,4.4.4.2;
        option ntp-servers 19.91.19.91,45.54.45.54,localhost1,19.91.19.91;
        option log-servers 10.12.16.17,10.12.16.16;
        option bootfile-name "Bootfile1";
        option tftp-server-name "Tftpserver1";
        option host-name "Omega";
}
}

Circuit-id:

class "circuit-id" {
match if option agent.circuit-id = 00:00:13:b6:00:02;---->Points to vlan and interface
index value.
} # circuit-id

subnet 192.168.1.0 netmask 255.255.255.0 {
pool {
        option subnet-mask 255.255.255.0;
        allow members of "circuit-id";
        range 192.168.1.2 192.168.1.100;
        default-lease-time 600;
        max-lease-time 600;
        option subnet-mask 255.255.255.0;
        option domain-name "Domain1.com";
        option domain-name-servers 23.32.23.32,4.4.4.2;
        option ntp-servers 19.91.19.91,45.54.45.54,localhost1,19.91.19.91;
```


© 2021 IP Infusion Inc. Proprietary

```
        option log-servers 10.12.16.17,10.12.16.16;
        option bootfile-name "Bootfile1";
        option tftp-server-name "Tftpserver1";
        option host-name "Omega";
}
}
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 7 DHCP Snooping IP Source Guard

Overview

IPSG is a security feature that restricts IP traffic on non-routed, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. Use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor.

Enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

Topology

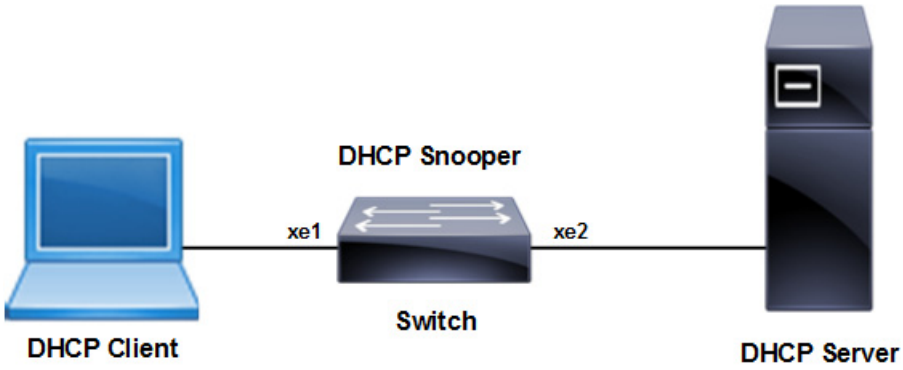


Figure 7-21: IP Source Guard Topology

Configuration

`#configure terminal`	Enter the configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create IEEE VLAN bridge 1.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)# ip dhcp snooping bridge 1`	Configure DHCP snooping for bridge 1
`(config)# ip dhcp snooping information option bridge 1`	Configure DHCP snooping information option 82
`(config)# ip dhcp snooping ratelimit 0` bridge 1	Configure DHCP snooping ratelimit. Default value is 100
`(config)# ip dhcp snooping vlan 2 bridge 1`	Configure DHCP snooping for vlan 2 for bridge 1
`(config)# ip dhcp snooping verify mac-address bridge 1`	Configure DHCP snooping verify mac-address
`(config)#interface xe2`	Enter Interface Mode
`(config-if)#switchport`	Configure the interface as Layer 2

(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip dhcp snooping trust	Configuring the interface as Trust. Basically this is configured on the interface which is connected to Server Side.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip verify source dhcp-snooping-vlan	Configuring IP source guard at Interface level and configured on the interface which is connected to client side
(config-if)#ip verify source access-group mode merge	Merge IPSG policy with other ACL
(config-if)#exit	Exit interface mode
(config)#ip dhcp snooping binding bridge 1 0011.1111.2222 2 ipv4 1.1.1.1 xe1	Configure Ipv4 Static Entry For DHCP snooping with MAC address and Source Address for an interface and vlan configured
(config)#ip dhcp snooping binding bridge 1 0022.2222.3333 2 ipv6 3ffe::1 xe1	Configure Ipv6 Static Entry For DHCP snooping with MAC address and Source Address for an interface and vlan configured
(config)#ip source binding ipv4 1.1.1.1 0011.1111.2222 vlan 2 interface xe1 bridge 1	Configure static IP source guard entry for ipv4 entries
(config)#ip source binding ipv6 3ffe::2 0022.2222.3333 vlan 2 interface xe1 bridge 1	Configure static IP source guard entry for ipv6 entries
(config)#exit	Exit config mode
#clear ip dhcp snooping binding bridge 1	Clear DHCP binding tables which are learned dynamically

Validation

Verify that DHCP snooping is enabled on the bridge:

```
#sh ip dhcp snooping bridge 1
Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Enabled
Verification of hwaddr field is                       : Enabled
Rate limit (pps)                                      : 0
DHCP snooping is configured on following VLANs        : 2
DHCP snooping is operational on following VLANs       : 2
DHCP snooping trust is configured on the following Interfaces
Interface               Trusted
---------------         -------
xe2                      Yes
DHCP snooping IP Source Guard is configured on the following Interfaces
```


© 2021 IP Infusion Inc. Proprietary

```
Interface                Source Guard
---------------          ------------
xe1                       Yes
```

Configuring Trusted and Un-trusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as untrusted port

In this example, xe1 is connected to the DHCP client and xe2 is connected to the DHCP server.

- Configure xe1 connected to DHCP client as un-trusted port.
- Configure xe2 connected to the DHCP server as trusted port.

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Specify the interface to be configured
`(config-if)#no ip dhcp snooping trust`	Disable the port as trusted.
`(config-if)#exit`	Exit interface mode
`(config)#interface xe2`	Specify the interface to be configured
`(config-if)#ip dhcp snooping trust`	Enable the port as trusted.
`(config-if)#exit`	Exit interface mode

Validation

Verify that static DHCP snooping entries are configured for the bridge:

```
#sh ip dhcp snooping binding bridge 1
Total number of static IPV4 entries                    : 1
Total number of dynamic IPV4 entries                   : 0
Total number of static IPV6 entries                    : 1
Total number of dynamic IPV6 entries                   : 0

MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   ---------------
0011.1111.2222       1.1.1.1           0          static          2      xe1
0022.2222.3333       3ffe::1           0          static          2      xe1
```

Verify that static IP DHCP snooping source guard entries are configured for the bridge:

```
#sh ip dhcp snooping source binding bridge 1
Total number of static source IPV4 entries             : 1
Total number of static source IPV6 entries             : 1
MacAddress           IpAddress         Lease (sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   --------------
----
0011.1111.2222       1.1.1.1           0          static          2      xe1
0022.2222.3333       3ffe::2           0          static          2      xe1
```

Configuring IP Source Guard on LAG Port

In this example, the LAG port (sa2) is created, then physical interfaces are added.

`#configure terminal`	Enter the configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create IEEE VLAN bridge 1.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)# ip dhcp snooping bridge 1`	Configure DHCP snooping for bridge 1
`(config)# ip dhcp snooping information option bridge 1`	Configure DHCP snooping information option 82
`(config)# ip dhcp snooping ratelimit 0 bridge 1`	Configure DHCP snooping ratelimit. Default value is 100
`(config)# ip dhcp snooping vlan 2 bridge 1`	Configure DHCP snooping for vlan 2 for bridge 1
`(config)# ip dhcp snooping verify mac-address bridge 1`	Configure DHCP snooping verify mac-address
`(config)#interface sa2`	Enter Interface Mode
`switchport`	Configure the interface as Layer 2
`bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)#ip verify source dhcp-snooping-vlan`	Configuring IP source guard at Interface level and configured on the interface which is connected to client side
`(config-if)#ip verify source access-group mode merge`	Merge IPSG policy with other ACL
`(config-if)#exit`	Exit interface mode
`(config)#interface xe2`	Enter Interface Mode
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)#switchport mode access`	Set the Layer2 interface as Access. (It can be Trunk mode also)
`(config-if)#switchport access vlan 2`	Set the default VLAN for the interface
`(config-if)#ip dhcp snooping trust`	Configuring the interface as Trust. Basically this is configured on the interface which is connected to Server Side.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter Interface Mode
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)#switchport mode access`	Set the Layer2 interface as Access. (It can be Trunk mode also)
`(config-if)#switchport access vlan 2`	Set the default VLAN for the interface
`(config-if)#static-channel-group 2`	Configure Static Channel lag on the interface
`(config-if)#exit`	Exit interface mode
`(config)#ip dhcp snooping binding bridge 1 0011.1111.2222 2 ipv4 1.1.1.1 sa2`	Configure Ipv4 Static Entry For DHCP snooping with MAC address and Source Address for lag interface and vlan configured

© 2021 IP Infusion Inc. Proprietary

`(config)#ip dhcp snooping binding bridge 1 0022.2222.3333 2 ipv6 3ffe::1 sa2`	Configure Ipv6 Static Entry For DHCP snooping with MAC address and Source Address for lag interface and vlan configured
`(config)#ip source binding ipv4 1.1.1.1 0011.1111.2222 vlan 2 interface sa2 bridge 1`	Configure static IP source guard entry for ipv4 entries with lag interface
`(config)#ip source binding ipv6 3ffe::2 0022.2222.3333 vlan 2 interface sa2 bridge 1`	Configure static IP source guard entry for ipv6 entries with lag interface
`(config)#exit`	Exit config mode
`#clear ip dhcp snooping binding bridge 1`	Clear DHCP binding tables which are learned dynamically

Validation

Verify that DHCP snooping is enabled on the bridge with the static LAG interface:

```
#sh ip dhcp snooping bridge 1
Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Enabled
Verification of hwaddr field is                       : Enabled
Rate limit(pps)                                       : 0
DHCP snooping is configured on following VLANs        : 2
DHCP snooping is operational on following VLANs       : 2
DHCP snooping trust is configured on the following Interfaces
Interface               Trusted
---------------         -------
Xe2                    Yes
DHCP snooping IP Source Guard is configured on the following Interfaces
Interface               Source Guard
---------------         ------------
sa2                     Yes
```

Verify that static DHCP snooping or source guard entries are configured for the bridge with the LAG interface:

```
#sh ip dhcp snooping binding bridge 1
Total number of static IPV4 entries                   : 1
Total number of dynamic IPV4 entries                  : 0
Total number of static IPV6 entries                   : 1
Total number of dynamic IPV6 entries                  : 0
MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   --------------
----
0011.1111.2222       1.1.1.1           0          static          2      sa2
0022.2222.3333       3ffe::1           0          static          2      sa2

#sh ip dhcp snooping source binding bridge 1
Total number of static source IPV4 entries            : 1
Total number of static source IPV6 entries            : 1
MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   --------------
----
0011.1111.2222       1.1.1.1           0          static          2      sa2
0022.2222.3333       3ffe::2           0          static          2      sa2
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 8 DHCP Snooping over MLAG

Overview

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. It is a layer-2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. With DHCP snooping, the physical location of hosts can be tracked, only the IP addresses assigned for the hosts can be used, only the authorized DHCP servers are accessible. DHCP snooping can prevent attackers from adding their own DHCP servers to the network. DHCP snooping allows only clients with specific IP/MAC addresses to have access to the network.

The DHCP snooping over MLAG feature synchronizes the DHCP snooping binding database between the MLAG peers. If one of the MLAG peer node or MLAG link is down, the DHCP request / reply messages should be honoured by the partner.

DHCP snooping is supported over Active-Active MLAG mode using Static & Dynamic Channel group while Active-Standby MLAG mode using Static Channel group.

Topology

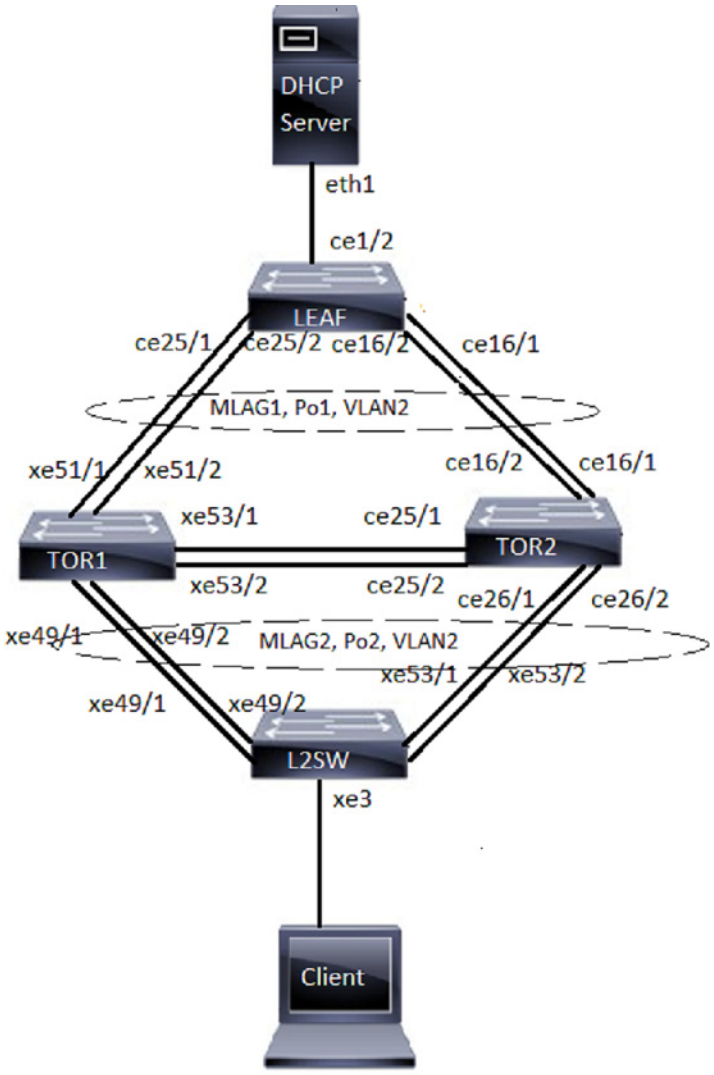


Figure 8-22: DHCP Snooping over MLAG

© 2021 IP Infusion Inc. Proprietary

Configuration

LEAF:

`#configure terminal`	Configure terminal.
`(config)#bridge 1 protocol rstp vlan-bridge`	Configuring the rstp vlan bridge
`(config)#vlan 2 bridge 1 state enable`	Configure VLAN for the bridge
`(config)#interface po1`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface ce1/2`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface ce16/1`	Enter interface mode
`(config-if)#channel-group 1 mode active`	Enable channel-group 1
`(config-if)#exit`	Exit interface mode
`(config)#interface ce16/2`	Enter interface mode
`(config-if)#channel-group 1 mode active`	Enable channel-group 1
`(config-if)#exit`	Exit interface mode
`(config)#interface ce25/1`	Enter interface mode
`(config-if)#channel-group 1 mode active`	Enable channel-group 1
`(config-if)#exit`	Exit interface mode
`(config)#interface ce25/2`	Enter interface mode
`(config-if)#channel-group 1 mode active`	Enable channel-group 1
`(config-if)#exit`	Exit the configure mode

TOR1:

`#configure terminal`	Configure terminal.
`(config)#bridge 1 protocol rstp vlan-bridge`	Configuring the rstp vlan bridge
`(config)#vlan 2 bridge 1 state enable`	Configure VLAN for the bridge
`(config)#ip dhcp snooping bridge 1`	Enable DHCP Snooping on the bridge
`(config)#ip dhcp snooping vlan 2 bridge 1`	Enable DHCP Snooping on the vlan 2
`(config)#interface mlag1`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2

(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#ip dhcp snooping trust	Enable the port as trusted.
(config-if)#exit	Exit interface mode
(config)#interface mlag2	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode trunk	Configure the mode as trunk
(config-if)# switchport trunk allowed vlan add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#interface po1	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#mlag 1	Map po1 to mlag1
(config-if)#exit	Exit interface mode
(config)#interface po2	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#mlag 2	Map po2 to mlag2
(config-if)#exit	Exit interface mode
(config)#interface po5	Enter Interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode trunk	Configure the mode as trunk
(config-if)#switchport trunk allowed add 2	Allow vlan 2 on the interface
(config-if)#exit	Exit interface mode
(config)#interface xe49/1	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit interface mode
(config)#interface xe49/2	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit interface mode
(config)#interface xe51/1	Enter Interface mode
(config-if)#channel-group 1 mode active	Enable channel-group 1
(config-if)#exit	Exit interface mode
(config)#interface xe51/2	Enter Interface mode
(config-if)#channel-group 1 mode active	Enable channel-group 1
(config-if)#exit	Exit interface mode
(config)#interface xe53/1	Enter Interface mode
(config-if)#channel-group 5 mode active	Enable channel-group 5

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit interface mode
(config)#interface xe53/2	Enter Interface mode
(config-if)#channel-group 5 mode active	Enable channel-group 5
(config-if)#exit	Exit interface mode
(config)#mcec domain configuration	Enter MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the mlag domain
(config-mcec-domain)#domain-system-number 2	Configure the domain system number
(config-mcec-domain)#intra-domain-link po5	Specify the intra domain link for MLAG communication
config-mcec-domain)#end	Exit the configure mode

TOR2:

`#configure terminal`	Configure terminal.
`(config)#bridge 1 protocol rstp vlan-bridge`	Configuring the rstp vlan bridge
`(config)#vlan 2 bridge 1 state enable`	Configure VLAN for the bridge
`(config)#ip dhcp snooping bridge 1`	Enable DHCP Snooping on the bridge
`(config)#ip dhcp snooping vlan 2 bridge 1`	Enable DHCP Snooping on the vlan 2
`(config)#interface mlag1`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#ip dhcp snooping trust`	Enable the port as trusted.
`(config-if)#exit`	Exit interface mode
`(config)#interface mlag2`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface po1`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#mlag 1`	Map po1 to mlag1
`(config-if)#exit`	Exit interface mode
`(config)#interface po2`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#mlag 2`	Map po2 to mlag2
`(config-if)#exit`	Exit interface mode
`(config)#interface po5`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface ce16/1`	Enter Interface mode
`(config-if)#channel-group 1 mode active`	Enable channel-group 1
`(config-if)#exit`	Exit interface mode
`(config)#interface ce16/2`	Enter Interface mode
`(config-if)#channel-group 1 mode active`	Enable channel-group 1
`(config-if)#exit`	Exit interface mode

© 2021 IP Infusion Inc. Proprietary

(config)#interface ce25/1	Enter Interface mode
(config-if)#channel-group 5 mode active	Enable channel-group 5
(config-if)#exit	Exit interface mode
(config)#interface ce25/2	Enter Interface mode
(config-if)#channel-group 5 mode active	Enable channel-group 5
(config-if)#exit	Exit interface mode
(config)#interface ce26/1	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit interface mode
(config)#interface ce26/2	Enter Interface mode
(config-if)#channel-group 2 mode active	Enable channel-group 2
(config-if)#exit	Exit interface mode
(config)#mcec domain configuration	Enter MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the mlag domain
(config-mcec-domain)#domain-system-number 1	Configure the domain system number
(config-mcec-domain)#intra-domain-link po5	Specify the intra domain link for MLAG communication
(config-mcec-domain)#end	Exit the configure mode

L2SW:

`#configure terminal`	Configure terminal.
`(config)#bridge 1 protocol rstp vlan-bridge`	Configuring the rstp vlan bridge
`(config)#vlan 2 bridge 1 state enable`	Configure VLAN for the bridge
`(config-if)#interface po2`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe3`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe49/1`	Enter Interface mode
`(config-if)#channel-group 2 mode active`	Enable channel-group 2
`(config-if)#exit`	Exit interface mode
`(config)#interface xe49/2`	Enter Interface mode
`(config-if)#channel-group 2 mode active`	Enable channel-group 2
`(config-if)#exit`	Exit interface mode
`(config)#interface xe53/1`	Enter Interface mode
`(config-if)#channel-group 2 mode active`	Enable channel-group 2
`(config-if)#exit`	Exit interface mode
`(config)#interface xe53/2`	Enter Interface mode
`(config-if)#channel-group 2 mode active`	Enable channel-group 2
`(config-if)#exit`	Exit the configure mode

Static MLAG configuration for TOR1 and TOR2

Note: Only mlag related configs for static MLAG is provided. While rest of the configuration is similar to dynamic.

© 2021 IP Infusion Inc. Proprietary

TOR1:

`#configure terminal`	Configure terminal.
`(config)#interface mlag1`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#mode active-standby`	Configure mlag mode for mlag1
`(config-if)#ip dhcp snooping trust`	Enable the port as trusted.
`(config-if)#exit`	Exit interface mode
`(config)#interface mlag2`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#mode active-active`	Configure mlag mode for mlag2
`(config-if)#exit`	Exit interface mode
`(config)#interface sa1`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#mlag 1`	Map sa1 to mlag1
`(config-if)#exit`	Exit interface mode
`(config)#interface sa2`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#mlag 2`	Map sa2 to mlag2
`(config-if)#exit`	Exit interface mode
`(config)#interface sa5`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#exit`	Exit interface mode
`(config)#mcec domain configuration`	Enter MCEC mode
`(config-mcec-domain)#domain-address 1111.2222.3333`	Domain address for the mlag domain
`(config-mcec-domain)#domain-system-number 1`	Configure the domain system number
`(config-mcec-domain)#intra-domain-link sa5`	Specify the intra domain link for MLAG communication
`(config-mcec-domain)#end`	Exit the configure mode

TOR2:

`#configure terminal`	Configure terminal.
`(config)#interface mlag1`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#mode active-standby`	Configure mlag mode for mlag1
`(config-if)#ip dhcp snooping trust`	Enable the port as trusted.
`(config-if)#exit`	Exit interface mode
`(config)#interface mlag2`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#mode active-active`	Configure mlag mode for mlag2
`(config-if)#exit`	Exit interface mode
`(config)#interface sa1`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#mlag 1`	Map sa1 to mlag1
`(config-if)#exit`	Exit interface mode
`(config)#interface sa2`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#mlag 2`	Map sa2 to mlag2
`(config-if)#exit`	Exit interface mode
`(config)#interface sa5`	Enter Interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode trunk`	Configure the mode as trunk
`(config-if)#switchport trunk allowed vlan add 2`	Allow vlan 2 on the interface
`(config-if)#exit`	Exit interface mode
`(config)#mcec domain configuration`	Enter MCEC mode
`(config-mcec-domain)#domain-address 1111.2222.3333`	Domain address for the mlag domain
`(config-mcec-domain)#domain-system-number 2`	Configure the domain system number
`(config-mcec-domain)#intra-domain-link sa5`	Specify the intra domain link for MLAG communication
`(config-mcec-domain)#end`	Exit the configure mode

© 2021 IP Infusion Inc. Proprietary

Validation

1. Verify Dhcps Sync PDUs:

```
TOR1#show mcec statistics

Unknown MCCPDU received on the system            : 0

-------------------------------------
IDP po5
-------------------------------------
   Valid RX Hello PDUs                           : 2373
   Valid TX Hello PDUs                           : 2373
   Valid RX Info PDUs                            : 12
   Valid TX Info PDUs                            : 20

   Valid RX Mac Sync PDUs                        : 20
   Valid TX Mac Sync PDUs                        : 20

   Valid RX Dhcps Sync PDUs                      : 1
   Valid TX Dhcps Sync PDUs                      : 3

MLAG 1
  Valid RX Info PDUs                             : 6
  Valid TX Info PDUs                             : 10

MLAG 2
  Valid RX Info PDUs                             : 6
  Valid TX Info PDUs                             : 10

TOR1#
TOR2#show mcec statistics

Unknown MCCPDU received on the system            : 0

-------------------------------------
IDP po5
-------------------------------------
   Valid RX Hello PDUs                           : 2384
   Valid TX Hello PDUs                           : 2385
   Valid RX Info PDUs                            : 18
   Valid TX Info PDUs                            : 12

   Valid RX Mac Sync PDUs                        : 20
   Valid TX Mac Sync PDUs                        : 16

   Valid RX Dhcps Sync PDUs                      : 3
   Valid TX Dhcps Sync PDUs                      : 1
```

```
MLAG 1
  Valid RX Info PDUs                          : 9
  Valid TX Info PDUs                          : 6

MLAG 2
  Valid RX Info PDUs                          : 9
  Valid TX Info PDUs                          : 6
```

2. Verify dhcp binding entires:

```
TOR2#
TOR1# show ip dhcp snooping binding bridge 1

Total number of static IPV4 entries                    : 0
Total number of dynamic IPV4 entries                   : 1
Total number of static IPV6 entries                    : 0
Total number of dynamic IPV6 entries                   : 0

MacAddress           IpAddress         Lease(sec) Type            VLAN   Interfa
ce
------------------   ---------------   ---------- -------------   ----   -------
-----------
80a2.35e9.8323       20.20.20.2        315        dhcp-snooping   2      mlag2

TOR1#

TOR2#show ip dhcp snooping binding bridge 1

Total number of static IPV4 entries                    : 0
Total number of dynamic IPV4 entries                   : 1
Total number of static IPV6 entries                    : 0
Total number of dynamic IPV6 entries                   : 0

MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   --------------
----
80a2.35e9.8323       20.20.20.2        315        dhcp-snooping   2      mlag2
```

3. Verify that DHCP snooping is enabled on the bridge

```
TOR2#

TOR1#show ip dhcp snooping bridge 1

Bridge Group                                           : 1
DHCP snooping is                                       : Enabled
DHCP snooping option82 is                              : Disabled
Verification of hwaddr field is                        : Disabled
Strict validation of DHCP packet is                    : Disabled
DB Write Interval(secs)                                : 300
```


© 2021 IP Infusion Inc. Proprietary

```
DHCP snooping is configured on following VLANs          : 2
DHCP snooping is operational on following VLANs         : 2

DHCP snooping trust is configured on the following Interfaces

Interface               Trusted
---------------         -------
mlag1                   Yes
po5                     Yes

DHCP snooping IP Source Guard is configured on the following Interfaces

Interface               Source Guard
---------------         ------------

TOR1#

TOR2#show ip dhcp snooping bridge 1

Bridge Group                                            : 1
DHCP snooping is                                        : Enabled
DHCP snooping option82 is                               : Disabled
Verification of hwaddr field is                         : Disabled
Strict validation of DHCP packet is                     : Disabled
DB Write Interval(secs)                                 : 300
DHCP snooping is configured on following VLANs          : 2
DHCP snooping is operational on following VLANs         : 2

DHCP snooping trust is configured on the following Interfaces

Interface               Trusted
---------------         -------
mlag1                   Yes
po5                     Yes

DHCP snooping IP Source Guard is configured on the following Interfaces

Interface               Source Guard
---------------         ------------
TOR2#
```

4. Verify dhcp snooping running configs

```
TOR1#show running-config ip dhcp snooping
!
debug ip dhcp snooping all
!
ip dhcp snooping bridge 1
ip dhcp snooping vlan 2 bridge 1
interface mlag1
```

```
 ip dhcp snooping trust
!
interface po5
 ip dhcp snooping trust
!
TOR1#

TOR2#show running-config ip dhcp snooping
!
debug ip dhcp snooping all
!
ip dhcp snooping bridge 1
ip dhcp snooping vlan 2 bridge 1
interface mlag1
 ip dhcp snooping trust
!
interface po5
 ip dhcp snooping trust
!
TOR2#
```

5. Verify mlag details:

```
TOR2#show mlag domain details

-----------------------------------
Domain Configuration
-----------------------------------

Domain System Number           : 1
Domain Address                 : 1111.2222.3333
Domain Priority                : 32768
Intra Domain Interface         : po5

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Admin Key                    : 16385
  Oper Key                     : 16385
  Physical properties Digest   : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22
```


© 2021 IP Infusion Inc. Proprietary

```
  Neigh Admin Key              : 32769
  Neigh Physical Digest        : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Total Bandwidth              : 40g
  Mlag Sync                    : IN_SYNC
  Mlag Mode                    : Active-Active
  Mlag State                   : UP

MLAG-2
  Mapped Aggregator            : po2
  Admin Key                    : 16386
  Oper Key                     : 16386
  Physical properties Digest   : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22

  Neigh Admin Key              : 32770
  Neigh Physical Digest        : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Total Bandwidth              : 40g
  Mlag Sync                    : IN_SYNC
  Mlag Mode                    : Active-Active
  Mlag State                   : UP

TOR2#

TOR1#show mlag domain details

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number           : 2
Domain Address                 : 1111.2222.3333
Domain Priority                : 32768
Intra Domain Interface         : po5

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Admin Key                    : 32769
```

```
  Oper Key                    : 16385
  Physical properties Digest  : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22


  Neigh Admin Key             : 16385
  Neigh Physical Digest       : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22

  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC
  Mlag Mode                   : Active-Active
  Mlag State                  : UP

MLAG-2
  Mapped Aggregator           : po2
  Admin Key                   : 32770
  Oper Key                    : 16386
  Physical properties Digest  : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22


  Neigh Admin Key             : 16386
  Neigh Physical Digest       : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22

  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC
  Mlag Mode                   : Active-Active
  Mlag State                  : UP

TOR1#
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 9 DHCPv6 Prefix Delegation

Overview

The prefix delegation feature lets a DHCP server assign prefixes chosen from a global pool to DHCP clients, that is how the Customer Premise Equipment (CPE) learns the prefix. The learnt prefix shall be used by the user to configure the IPv6 address on its LAN interface along with subnet prefix. The LAN hosts are learning the subnetted prefix through router advertisement (NDP protocol) messages, which enables the device to auto configure its own IPv6 addresses.

This feature would enable service providers to assign IP for the Customer Premise Equipment acting as a router between the service providers core network and subscribers internal network.

Topology

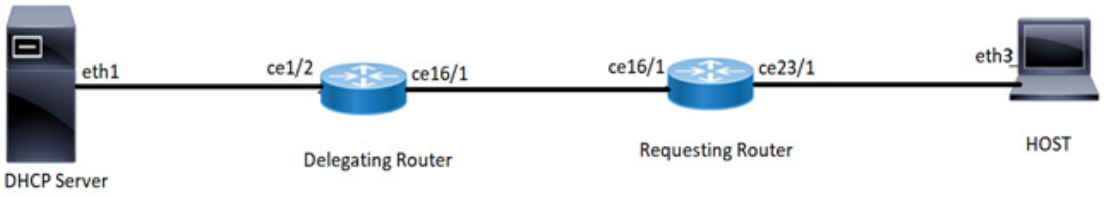


Figure 9-23: DHCPv6 Prefix Delegation

Configuration

DHCP RELAY-Delegating router(DR):

`#configure terminal`	configure terminal.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled in default.
`(config)#ipv6 dhcp relay`	By default, this will be enabled. It starts the ipv6 dhcp relay service.
`(config)#ipv6 dhcp relay address 2001:101:0:1::131`	The relay address configured should be server interface address connected to Delegating router.
`(config)#interface ce1/2`	Enter interface mode.
`(config-if)#ipv6 address 2001:101:0:1::130/64`	Configure ipv6 address on the interface ce1/2
`(config-if)#ipv6 dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`(config if)#exit`	Exit interface mode.
`(config)#interface ce16/1`	Enter interface mode.
`(config-if)#ipv6 address 3001:101:0:1::135/64`	Configure ipv6 address on the interface ce16/1
`(config-if)#ipv6 dhcp relay`	Relay should be configured on the interface connecting to the client.
`(config if)#exit`	Exit interface mode.
`(config)#ipv6 route 1212:501:102:1::/64 3001:101:0:1::254`	Configure static route towards Host where next-hop address is address allocated on RR is learnt from DHCP server(IA_NA) and destination network configured by the user using learnt prefix(IA_PD)

© 2021 IP Infusion Inc. Proprietary

Requesting Router(RR):

`#configure terminal`	configure terminal.
`(config)#interface ce16/1`	Enter interface mode.
`(config-if)#ipv6 dhcp address-prefix-len 64`	Addition of address length option
`(config-if)#ipv6 address dhcp`	Configure IPv6 address DHCP.
`(config-if)# ipv6 dhcp prefix-delegation DHCPv6_PREFIX`	Include DHCPv6 prefix option in the DHCPv6 client request
`(config if)#exit`	Exit interface mode.
`(config)#interface ce23/1`	Enter interface mode.
`(config-if)#ipv6 address DHCPv6_PREFIX ::1:0:0:0:1/64`	Configure IPv6 address from the prefix learnt where "::1" is the subnet ID and last 64 bits are host ID.
`(config-if)#no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config if)#exit`	Exit interface mode.
`(config)#ipv6 route 2001:101:0:1::/64 3001:101:0:1::135`	Configure static route towards server.

HOST :

Note: CLI "ipv6 address autoconfig" is hidden and experimental as the host portion of ipv6 autoconfiguration using NDP is not fully implemented.

`#configure terminal`	configure terminal.
`(config)#interface ce23/1`	Enter interface mode.
`(config-if)#ipv6 address autoconfig`	Configure IPv6 autoconfig
`(config-if)#no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config if)#exit`	Exit interface mode.

Linux host:

`IPV6_AUTOCONF=yes`	IPv6 autoconfig should be set to yes in interface config file.

DHCP SERVER:

`ifconfig eth1 inet6 add 2001:101:0:1::131/64`	Configure ipv6 address on client facing interface
`dhcpd -d -6 -cf /etc/dhcp/dhcpd6.conf eth1`	Start server
`ipv6 route 1212:501:102:1::/64 2001:101:0:1::130`	Configure static route towards Requesting Router

Sample dhcpd6.conf file:

Note: Preferred and Max lifetimes must not be configured with same values.

```
#
   # DHCPv6 Server Configuration file.
   #   see /usr/share/doc/dhcp*/dhcpd6.conf.sample
   #   see dhcpd.conf(5) man page
   #
   preferred-lifetime 600;
   default-lease-time 600;
```

```
 subnet6 2001:101:0:1::/64 {
 range6 2001:101:0:1::129 2001:101:0:1::254;
 }
subnet6 3001:101:0:1::/64 {
range6 3001:101:0:1::129 3001:101:0:1::254;
prefix6 1212:501:101:: 1212:501:102:: /48;
option dhcp6.name-servers fec0:0:0:1::1;
option dhcp6.domain-search "domain.example";
}
```

Validation

Delegation Router:

```
DR#show ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: default
DHCPv6 Servers configured: 2001:101:0:1::131
Interface                Uplink/Downlink
---------                -------------
ce1/2                    Uplink
ce16/1                   Downlink
```

Requesting Router:

```
RR#show ipv6 dhcp interface

ce16/1 is in client mode
prefix name: DHCPv6_PREFIX
learned prefix: 1212:501:102::/48
preferred lifetime 600, valid lifetime 600
interfaces using the learned prefix
      ce23/1    1212:501:102:1::1

RR#show int ce23/1
Interface ce23/1
Scope: both
Flexport: Breakout Control Port (Active): Break Out Enabled
Hardware is ETH  Current HW addr: cc37.abc9.7426
Physical:cc37.abc9.743f  Logical:(not set)
Port Mode is Router
Interface index: 10025
Metric 1 mtu 1500 duplex-full link-speed 1g
Debounce timer: disable
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2021 Mar 02 09:44:05 (00:03:55 ago)
Statistics last cleared: 2021 Mar 02 09:44:05 (00:03:55 ago)
inet6 1212:501:102:1::1/64
```


© 2021 IP Infusion Inc. Proprietary

```
inet6 fe80::ce37:abff:fec9:7426/64
ND router advertisements are sent approximately every 571 seconds
ND next router advertisement due in 434 seconds.
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
  5 minute input rate 2 bits/sec, 0 packets/sec
  5 minute output rate 23 bits/sec, 0 packets/sec
```

HOST:

```
[root@localhost ~]# ifconfig -a
     eth3      Link encap:Ethernet  HWaddr 00:07:E9:A5:23:4C
     inet6 addr: 1212:501:102:1:207:e9ff:fea5:234c/64 Scope:Global
     inet6 addr: fe80::207:e9ff:fea5:234c/64 Scope:Link
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:196985 errors:0 dropped:0 overruns:0 frame:0
     TX packets:5733 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:23542362 (22.4 MiB)  TX bytes:710558 (693.9 KiB)
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 10 DHCPv6 Relay Prefix Delegation Route Injection Configuration

Overview

The prefix delegation feature lets a DHCP server assign prefixes chosen from a global pool to DHCP clients. The DHCP client can then configure an IPv6 address on its LAN interface using the prefix it received. It will then send router advertisements including the prefix, allowing other devices to auto-configure their own IPv6 addresses.

If the network topology where Prefix Delegation is running has a Relay agent, then a route needs to be injected in Delegating Router, so that the traffic from the DHCP server-side shall be forwarded towards the Requesting Router.

Topology

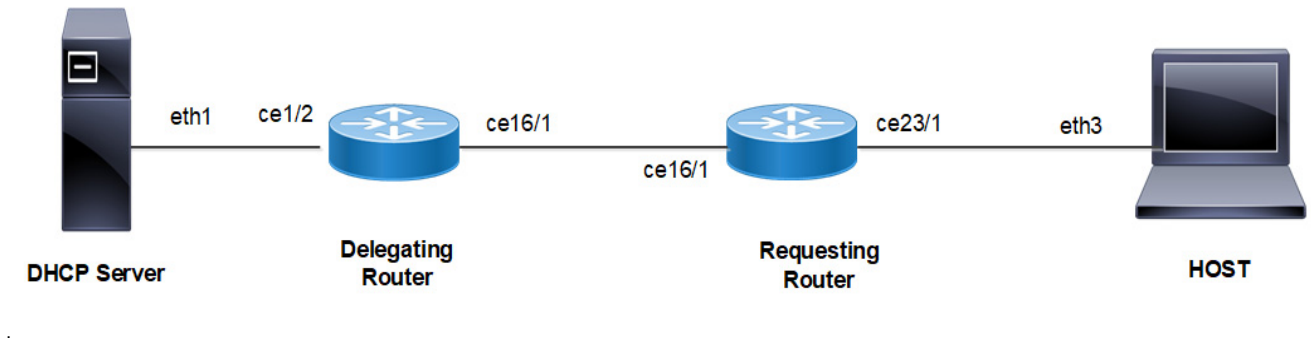


Figure 10-24: DHCPv6 Relay Delegating Configuration

DHCP Relay - Delegating Router (DR)

`#configure terminal`	Enter configure mode.
`(config)#feature dhcp`	Enable the feature DHCP. This is enabled by default.
`(config)#ipv6 dhcp relay`	By default, this will be enabled. It starts the IPv6 DHCP relay service.
`(config)#ipv6 dhcp relay address 2001:101:0:1::131`	The relay address configured should be server interface address connected to Delegating Router.
`(config)#interface ce1/2`	Enter interface mode.
`(config-if)#ipv6 address 2001:101:0:1::130/64`	Configure IPv6 address on the interface ce1/2
`(config-if)#ipv6 dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`(config-if)#exit`	Exit interface mode.
`(config)#interface ce16/1`	Enter interface mode.
`(config-if)#ipv6 address 3001:101:0:1::135/64`	Configure IPv6 address on the interface ce16/1

© 2021 IP Infusion Inc. Proprietary

`(config-if)#ipv6 dhcp relay`	Relay should be configured on the interface connecting to the client.
`(config-if)#exit`	Exit interface mode.
`(config)#ipv6 dhcp relay pd-route-injection`	Configure to enable auto route injection.

Requesting Router (RR)

`#configure terminal`	Enter configure mode.
`(config)#interface ce16/1`	Enter interface mode.
`(config-if)#ipv6 address dhcp`	Configure IPv6 address DHCP.
`(config-if)#ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER`	Configure IPv6 DHCP prefix-delegation
`(config-if)#exit`	Exit interface mode.
`(config)#interface ce23/1`	Enter interface mode.
`(config-if)#ipv6 address PREFIX_FROM_SERVER ::1:0:0:0:1/64`	Configure IPv6 address from the prefix learnt
`(config-if)#ipv6 nd ra-interval 4`	Configure ra-interval
`(config-if)#no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config-if)#exit`	Exit interface mode.
`(config)#ipv6 route 2001:101:0:1::/64 3001:101:0:1::135`	Configure static route towards server

HOST

`#configure terminal`	Enter configure mode.
`(config)#interface ce23/1`	Enter interface mode.
`(config-if)#ipv6 address autoconfig`	Configure IPv6 autoconfig
`(config-if)#no ipv6 nd suppress-ra`	Enable Router Advertisement transmission.
`(config if)#exit`	Exit interface mode.
`(config)#ipv6 route 2001:101:0:1::/64 fe80::ce37:abff:fec9:7426 ce23/1`	Configure static route towards server

Linux Host

`IPV6_AUTOCONF=yes`	IPv6 autoconfig should be set to yes in interface config file.

DHCP Server

`ifconfig eth1 inet6 add 2001:101:0:1::131/64`	Configure IPv6 address on client facing interface
`dhcpd -d -6 -cf /etc/dhcp/dhcpd6.conf eth1`	Start server
`ipv6 route 1212:501:102:1::/64 2001:101:0:1::130`	Configure static route towards Requesting Router

© 2021 IP Infusion Inc. Proprietary

Sample dhcpd6.conf file

```
#
#DHCPv6 Server Configuration file.
#see /usr/share/doc/dhcp*/dhcpd6.conf.sample
#see dhcpd.conf(5) man page
#
preferred-lifetime 400;
default-lease-time 600;

subnet6 2001:101:0:1::/64 {
range6 2001:101:0:1::129 2001:101:0:1::254;
}
subnet6 3001:101:0:1::/64 {
range6 3001:101:0:1::129 3001:101:0:1::254;
prefix6 1212:501:101:: 1212:501:102:: /48;
option dhcp6.name-servers fec0:0:0:1::1;
option dhcp6.domain-search "domain.example";
}
```

Validation

Delegation Router (DR)

```
DR#sh ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: default
  DHCPv6 Servers configured: 2001:101:0:1::131
  DHCPv6 IA_PD Route injection: Enabled
  Interface               Uplink/Downlink
  ---------               -------------
  ce1/2                     Downlink
  ce16/1                    Uplink

DR#sh ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, D- DHCP, R - RIP,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 19:24:04
D      1212:501:102::/48 [80/0] via fe80::eac5:7aff:fe64:4a20, ce16/1, 00:00:01
C      2001:101:0:1::/64 via ::, xe4, 03:42:58
C      3001:101:0:1::/64 via ::, xe2, 02:51:04
C      4001:101:0:1::/64 via ::, xe5, 03:14:41
C      fe80::/64 via ::, xe9, 00:41:39

OcNOS#sh ipv6 dhcp pd-route
VRF : default
```

```
  1212:501:102::/48 via fe80::eac5:7aff:fe64:4a20, ce16/1, (2019-05-30 14:02:50 - 2
019-05-30 14:04:50)
```

Requesting Router (RR)

```
RR#show ipv6 dhcp interface

ce16/1 is in client mode
prefix name: PREFIX_FROM_SERVER1
learned prefix: 1212:501:102::/48
preferred lifetime 600, valid lifetime 600
interfaces using the learned prefix
ce23/1    1212:501:102:1::1

RR#sh ipv6 interface ce23/1 brief
Interface            IPv6-Address                                    Admin-Status
Ce23/1               *1212:501:102:1::1
                     fe80::ce37:abff:fec9:7426                       [up/up]

RR#show int ce23/1
Interface ce23/1
Scope: both
Flexport: Breakout Control Port (Active): Break Out Enabled
Hardware is ETH  Current HW addr: cc37.abc9.7426
Physical:cc37.abc9.743f  Logical:(not set)
Port Mode is Router
Interface index: 10025
Metric 1 mtu 1500 duplex-full link-speed 1g
Debounce timer: disable
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2021 Mar 02 09:44:05 (00:03:55 ago)
Statistics last cleared: 2021 Mar 02 09:44:05 (00:03:55 ago)
inet6 1212:501:102:1::1/64
inet6 fe80::ce37:abff:fec9:7426/64
ND router advertisements are sent approximately every 571 seconds
ND next router advertisement due in 434 seconds.
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
5 minute input rate 2 bits/sec, 0 packets/sec
5 minute output rate 23 bits/sec, 0 packets/sec
```

HOST

```
[root@localhost ~]#ifconfig -a
eth3      Link encap:Ethernet  HWaddr 00:07:E9:A5:23:4C
inet6 addr: 1212:501:102:1:207:e9ff:fea5:234c/64 Scope:Global
inet6 addr: fe80::207:e9ff:fea5:234c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:196985 errors:0 dropped:0 overruns:0 frame:0
```


© 2021 IP Infusion Inc. Proprietary

```
TX packets:5733 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:23542362 (22.4 MiB)  TX bytes:710558 (693.9 KiB)

N4#show ipv6 interface xe7 brief
Interface            IPv6-Address                                    Admin-Status
ce23/1               *1212:501:102:1:6821:5fff:fe55:4a27
                     fe80::6a21:5fff:fe55:4a27                       [up/up]
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 11 DNS Configuration

Overview

The Domain Name System (DNS) is an Internet service that translates domain names into IP addresses. When a domain name is used, DNS service translates the name into the corresponding IP address. If one DNS server does not know how to translate a particular domain name, it gathers information from other Domain Name Systems to obtain the correct IP address.

Support for In-band Management over default VRF

OcNOS offers support for DNS over default and management VRFs via in-band management interface & OOB management interface, respectively.

The feature can be enabled to run on default and management VRF simultaneously. By default, it runs on management VRF.

Topology

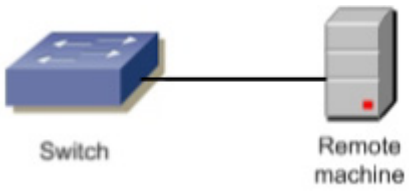


Figure 11-25: DNS sample topology

Configuration

`#configure terminal`	Enter Configure mode.
`(config)#ip name-server vrf management 10.12.17.11 10.1.1.2`	This add a IPv4 Name Server to the DNS.
`(config)#ip host vrf management BINGO 10.1.1.1`	This will add IPv4 host to the DNS
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode.

Validation Commands

```
#show hosts vrf management
         VRF: default

 DNS lookup is disabled
 Default domain is empty
 DNS domain list is empty

 Name Servers        : 10.12.17.11 10.1.1.2
```

```
Host                                                                    Address

----                                                                    -------

BINGO                                                                   10.1.1.1


 * - Values assigned by DHCP Client.
```

Configuration

`#configure terminal`	Enter Configure mode.
`(config)#ip name-server vrf management 3001::1`	This add a IPv6 Name Server to the DNS.
`(config)#ip host vrf management bingo 5001::1`	This will add IPv6 host to the DNS
`(config)#commit`	Commit the Candidate configuration to the running configuration
`(config)#exit`	Exit configure mode.

Validation Commands

```
OcNOS#show hosts vrf management
       VRF: management

DNS lookup is enabled
 Default domain is empty
 DNS domain list is empty

 Name Servers        : 3001::1
Host                                                                    Address
----                                                                    -------
bingo                                                                   5001::1

 * - Values assigned by DHCP Client.
OcNOS#
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 12 ErrDisable for Link-Flapping Configuration

If a link flaps continuously, the interface goes into ErrDisable state. When a port is the ErrDisable state, it is effectively shut down and no traffic is sent or received on that port. The port can be recovered from the ErrDisable state manually (shutting down the interface) or automatically (setting a timeout value).

Note:

- An interface should change state as up-down to complete one cycle of a link flap.
- The LED does not glow when an interface is in the errdisable state.
- Errdisable is supported only on physical interfaces.
- A LAG interface does not go into the errdisable state when all of its member ports are in the errdisable state
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. If the accumulated link flap count reaches the maximum flap count for a particular sliding window, a link flap error disable fault is triggered.

Topology

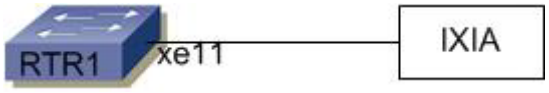


Figure 12-26: ErrDisable

Automatic Recovery

By default, an interface goes into the ErrDisable state when a link flaps 5 times in 10 seconds. An interface is recovered from the ErrDisable state when the configured non-zero errdisable time-out interval value expires.

RTR1

`#configure terminal`	Enter configure mode.
`(config)#errdisable cause link-flap`	Enable ErrDisable due to link-flap
`(config)#errdisable link-flap-setting max-flaps 2 time 30`	Configure Link flap settings. Max link flap count and interval for linkFlap Timer
`(config)#errdisable timeout interval 50`	Configure interval to recover from error disable state

Note: Automatic recovery timeout is disabled, if you configure `errdisable timeout interval 0`

Validation

```
#show errdisable details

 Error Disable Recovery Timeout Interval : 50 secs
 Link Flap Timer Interval : 30 secs
 Link Flaps allowed Max. count : 2
```

```
ErrDisable Cause     Status
---------------      ------
Link-Flap            Enabled
Lag-Mismatch         Disabled
Stp-Bpdu-Guard       Enabled
```

Note: Stp-Bpdu-Guard is enabled by default.

```
#show interface errdisable status
Interfaces that will be enabled at the next timeout
Interface    ErrDisable Cause   Time left(secs)
---------    ----------------   ---------------
xe11         link-flap          38

#show interface brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
xe11       ETH   --    --                down    ED      10g   --       No  No
#
```

Note: Interface xe11 went into the ErrDisable state after flapping 2 times in 30 seconds.

Log Message

`Edge1-SiteX#configure terminal`	Enter configure mode.
`Edge1-SiteX(config)#logging level nsm 4`	Enable Operational log to display recovery message

```
2017 Sep 18 11:52:12 : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface xe11 changed state to
down
(config-if)#no shut
(config-if)#2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe11 changed
state to up
2017 Sep 18 11:52:15 : NSM : WARN : [VXLAN_OPR_ACCESSPORT_UP_4]: VXLAN Access port on
xe11 is up
2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_ERR_DISABLE_DOWN_2]: Interface xe11 moved to
errdisable state due to link-flap
2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface xe11 changed state to
down
```

Note: Interface xe11 recovered from the ErrDisable state after a 50 second time-out.

To get the log messages displayed , change the logging leve to same on the console/monitor.

Manual Recovery

An interface can be recovered manually from the Errdisable state, when configure shutdown followed by no shutdown using CLI. Shutdown will recover the interface from errdisable state and No shutdown will make the interface up state.

© 2021 IP Infusion Inc. Proprietary

RTR1

`#configure terminal`	Enter configure mode.
`(config)#errdisable cause link-flap`	Enable errdisable due to link-flap
`(config)#errdisable link-flap-setting max-flaps 3 time 20`	Configure Link flap settings. Max link flap count and interval for linkFlap Timer

```
#show running-config | include errdisable
errdisable cause link-flap
errdisable link-flap-setting max-flaps 3 time 20
errdisable cause stp-bpdu-guard

#show errdisable details
 Error Disable Recovery Timeout Interval : 50 secs
 Link Flap Timer Interval : 20 secs
 Link Flaps allowed Max. count : 3

ErrDisable Cause     Status
----------------     ------
Link-Flap            Enabled
Lag-Mismatch         Disabled
Stp-Bpdu-Guard       Enabled
```

Note: Interface xe11 went into the ErrDisable state after flapping 3 times in 20 seconds.

```
(config)#do show interface errdisable status
Interfaces that will be enabled at the next timeout
Interface    ErrDisable Cause   Time left(secs)
---------    ----------------   ---------------
xe11         link-flap          NA
(config)#do show int brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
xe11       ETH   --    --                down    ED      10g   --       No  No
```

Note: Interface xe11 recovered from the ErrDisable state after entering `shutdown` followed by `no shutdown`.

```
(config)#interface xe11
(config-if)#shutdown
2017 Sep 18 13:02:20 : NSM : WARN : [IFMGR_ERR_DISABLE_UP_4]: Interface xe11 recovered
from link-flap errdisable
(config-if)#no shut
(config-if)#2017 Sep 18 13:02:21 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe11 changed
state to up
2017 Sep 18 13:02:21 : NSM : WARN : [VXLAN_OPR_ACCESSPORT_UP_4]: VXLAN Access port on
xe11 is up

config)#do show interface errdisable
(config)#do show interface brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
```

```
(config)#
```

If you configure `no errdisable cause link-flap`, at the global level, it recovers all the interfaces from the ErrDisable state

For transaction clients (such as NetConf), to recover a port from an error disable state manually, use this command/ RPC call:

- Command: `clear interface IFNAME error-disable`
- NetConf RPC: `interface-clear-interface-error-disable`

Note: This command/RPC applies only for an error disable state caused by an administrative shutdown. For an error disable state due to peer flapping or any other reason, recover from the error disable state by entering `shutdown` followed by `no shutdown`.

Errdisable at the Interface Level

If you enable errdisable globally, by default all physical interfaces enable link-flap errdisable. To turn off errdisable for an interface, configure the commands below.

`#configure terminal`	Enter configure mode.
`(config)#interface xe11`	Enter into interface level
`(config-if)#no link-flap errdisable`	Disable link-flap errdisable for interface

Note: If you configure “no link-flap errdisable” in interface level, either it won’t allow the interface move to errdisable state or it will recover interface from errdisable state

Validation

```
#show run int xe11
!
interface xe11
 description *1/2 member of PO3 - Connected to IXIA 6/6*
 channel-group 3 mode active
 no link-flap errdisable
!
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 13 Ethernet Interface Loopback Support Configurations

This section contains the Ethernet Interface Loopback Support configuration example.

Overview

This feature support is to provide additional hardware diagnostic functionality for physical ports on boards. This feature will enable the user to determine if there are any issues in the physical port at the MAC and the PHY layer.

To achieve this functionality, the Ethernet interfaces can be configured as the loopback interfaces. Looping back the packets are possible either at MAC layer or at PHY layer. Also packets can be looped either from Egress to Ingress or Ingress to Egress. On enabling this feature, if all the TX packets are looped back to RX, it indicates there is no issue with the hardware at the particular layer configured, either MAC or PHY.

Topology

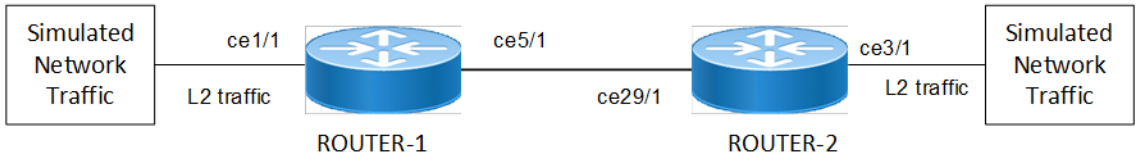


Figure 13-27: Ethernet Interface Loopback Support

Scenario-1: PHY level Tx Loopback

Configuration of ROUTER-1 device

`#configure terminal`	Enter Configure mode.
`(config)#hostname ROUTER-1`	Configure the hostname
`(config)#commit`	Commit the configuration
`(config)#end`	Exit configuration mode
`#configure terminal`	Enter into the configure terminal mode
`(config)#bridge 1 protocol rstp vlan-bridge`	Configure bridge
`(config)#vlan database`	Enter into VLAN database
`(config-vlan)#vlan 2 bridge 1`	Configure VLAN
`(config-vlan)#exit`	Exit the VLAN database mode
`(config)#interface ce1/1`	Enter into interface ce1/1
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Configure bridge-group
`(config-if)#switchport mode trunk`	Configure switchport mode as trunk

© 2021 IP Infusion Inc. Proprietary

(config-if)#switchport trunk allowed vlan add 2	Add all the VLANs to the interface
(config-if)#exit	Exit the interface mode
(config)#interface ce5/1	Enter into interface ce1/1
(config-if)# port breakout enable 4*10g	Configure port breakout
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode trunk	Configure switchport mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Add all the VLANs to the interface
(config-if)#loopback tx phy	Configure loopback Tx PHY
(config-if)#exit	Exit the interface level
(config)#no mac-address-table learning bridge 1 interface ce1/1	Disable the MAC-learning on the device
(config)#no mac-address-table learning bridge 1 interface ce5/1	Disable the MAC-learning on the device
(config)#commit	Commit the configuration
(config)#exit	Exit from configuration mode

Configuration of ROUTER-2 device

#conf terminal	Enter into the configure terminal mode
(config)#hostname ROUTER-2	Configure the hostname
(config)#commit	Commit the configuration
(config)#exit	Exit configuration mode
#conf terminal	Enter into the configure terminal mode
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge
(config)#vlan database	Enter into VLAN database
(config-vlan)#vlan 2 bridge 1	Configure VLAN
(config-vlan)#exit	Exit the VLAN database mode
(config)#interface ce3/1	Enter into interface ce3/1
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode trunk	Configure switchport mode as trunk
(config-if)#switchport trunk allowed vlan add 2	Add the VLAN to the interface
(config-if)#exit	Exit the interface mode
(config-if)#interface ce29/1	Enter into interface ce29/1
(config-if)# Port breakout enable 4*10g	Configure port breakout
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Configure bridge-group
(config-if)#switchport mode trunk	Configure switchport mode as trunk

© 2021 IP Infusion Inc. Proprietary

`(config-if)#switchport trunk allowed vlan add 2`	Add the VLAN to the interface
`(config-if)#exit`	Exit from interface level
`(config)#no mac-address-table learning bridge 1 interface ce3/1`	Disable the MAC-learning on the device
`(config)#no mac-address-table learning bridge 1 interface ce29/1`	Disable the MAC-learning on the device
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit from configuration mode

Validation

On ROUTER-1 Device:

```
#show running-config interface ce1/1
!
interface ce1/1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
!

#show running-config interface ce5/1
!
interface ce5/1
port breakout enable 4X10g
switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
 loopback tx phy
!

#show interface ce5/1
Interface ce5/1
  Flexport: Breakout Control Port (Active): Break Out Enabled
  Hardware is ETH  Current HW addr: 34ef.b689.e04a
  Physical:34ef.b689.e04a  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Interface index: 5045
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
  Loopback Type: PHY
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2021 Oct 23 15:57:01 (00:08:51 ago)
  Statistics last cleared: 2021 Oct 23 15:54:44 (00:11:08 ago)
  5 minute input rate 255 bits/sec, 0 packets/sec
  5 minute output rate 255 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 2272 broadcast packets 0
    input packets 2272 bytes 153730
```

```
        jumbo packets 0
        undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
        input error 0
        input with dribble 0 input discard 7
        Rx pause 0
      TX
        unicast packets 0 multicast packets 4333 broadcast packets 0
        output packets 4333 bytes 293304
        jumbo packets 0
        output errors 0 collision 0 deferred 0 late collision 0
        output discard 0
        Tx pause 0

# show interface brief
--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu  Loopbk
Interface                                                             Ch #
--------------------------------------------------------------------------------
ce5/1        ETH          1     trunk            up      none    10g   --      Br  Yes PHY
```

On ROUTER-2 Device:

```
#show running-config interface ce3/1
!
interface ce3/1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
!

#show running-config interface ce29/1
!
interface ce29/1
port breakout enable 4X10g
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan add 2
!
```

Interface counters before configuring loopback on both the devices:

```
=======================================================
#show interface counters rate gbps
+------------------+-------------+-------------+-------------+-------------
+
|     Interface     |    Rx gbps   |    Rx pps    |    Tx gbps   |    Tx pps
|
+------------------+-------------+-------------+-------------+-------------
+
 ce1/1               8.65           8446138       0.00           0
 ce5/1               0.00           0             8.65           8446125

#show interface counters rate gbps
+------------------+-------------+-------------+-------------+-------------
+
|     Interface     |    Rx gbps   |    Rx pps    |    Tx gbps   |    Tx pps
|
```


© 2021 IP Infusion Inc. Proprietary

```
+------------------+-------------+------------+-------------+------------
+
 ce3/1               0.00          0             8.65          8446188
 ce29/1              8.65          8446254       0.00          0
```

Interface counters after configuring loopback Tx PHY on ROUTER-1 device:

```
#show interface counters rate gbps
+------------------+-------------+------------+-------------+------------
+
|     Interface    |    Rx gbps  |    Rx pps  |    Tx gbps  |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 ce1/1               8.65          8446147       8.65          8446319
 ce5/1               8.65          8446194       8.65          8446194

#show interface counters rate gbps
+------------------+-------------+------------+-------------+------------
+
|     Interface    |    Rx gbps  |    Rx pps  |    Tx gbps  |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 ce3/1               0.00          0             0.00          0
```

Un-Config the Loopback

`#configure terminal`	Enter into configure terminal mode
`(config)#in ce5/1`	Enter into interface level
`(config-if)#no loopback`	Un-configure the loopback
`(config-if)#commit`	Commit the configuration
`(config-if)#end`	Exit from the configuration mode

Scenario-2 Loopback Tx MAC

`#configure terminal`	Enter into configure terminal mode
`(config)#in ce5/1`	Enter into interface level
`(config-if)# loopback tx mac`	Configure loopback Tx MAC
`(config-if)#commit`	Commit the configuration
`(config-if)#end`	Exit from the configuration mode

Validation

On ROUTER-1 Device:

```
#show running-config interface ce1/1
!
interface ce1/1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
!
```

```
#show running-config interface ce5/1
!
interface ce5/1
port breakout enable 4X10g
switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
 loopback tx mac
!

#show interface ce5/1
Interface ce5/1
  Flexport: Breakout Control Port (Active): Break Out Enable
  Hardware is ETH  Current HW addr: 34ef.b689.e04a
  Physical:34ef.b689.e04a  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Interface index: 5045
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
  Loopback Type: MAC
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2021 Oct 23 15:57:01 (00:08:51 ago)
  Statistics last cleared: 2021 Oct 23 15:54:44 (00:11:08 ago)
  5 minute input rate 255 bits/sec, 0 packets/sec
  5 minute output rate 255 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 2272 broadcast packets 0
    input packets 2272 bytes 153730
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 7
    Rx pause 0
  TX
    unicast packets 0 multicast packets 4333 broadcast packets 0
    output packets 4333 bytes 293304
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show interface brief
--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu  Loopbk
Interface                                                             Ch #
--------------------------------------------------------------------------------
ce5/1        ETH          1     trunk            up      none    10g   --      Br  Yes MAC
```

On ROUTER-2 device:

```
#show running-config interface ce3/1
!
interface ce3/1
```

 © 2021 IP Infusion Inc. Proprietary

```
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
!

#show running-config interface ce29/1
!
interface ce29/1
switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
!
```

Interface counters before configuring loopback on both the devices:

```
#show interface counters rate gbps
+------------------+-------------+------------+-------------+------------
+
|     Interface    |    Rx gbps  |    Rx pps  |    Tx gbps  |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 ce1/1               8.65          8432138       0.00          0
 ce5/1               0.00          0             8.65          8430125

#show interface counters rate gbps
+------------------+-------------+------------+-------------+------------
+
|     Interface    |    Rx gbps  |    Rx pps  |    Tx gbps  |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 ce3/1               0.00          0             8.65          8429188
 ce29/1              8.65          8430254       0.00          0
```

Interface counters after configuring loopback Tx PHY on ROUTER-1 devices:

```
#sh interface counters rate gbps
+------------------+-------------+------------+-------------+------------
+
|     Interface    |    Rx gbps  |    Rx pps  |    Tx gbps  |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 ce1/1               8.65          8446147       8.65          8446319
 ce5/1               8.65          8446194       8.65          8446194

#show interface counters rate gbps
+------------------+-------------+------------+-------------+------------
+
|     Interface    |    Rx gbps  |    Rx pps  |    Tx gbps  |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 ce3/1               0.00          0             0.00          0
ce29/1              0.00          0             0.00          0
```

Un-Config the Loopback

#configure terminal	Enter into configure terminal mode
(config)#in ce5/1	Enter into interface level
(config-if)#no loopback	UnConfigure loopback
(config-if)#commit	Commit the configuration
(config-if)#end	Exit from the configuration mode

Scenario-3 Loopback Rx PHY

#configure terminal	Enter into configure terminal mode
(config)#in ce29/1	Enter into interface level
(config-if)#loopback rx phy	Configure loopback Rx PHY
(config-if)#commit	Commit the configuration
(config-if)#end	Exit from the configuration mode

Validation

On ROUTER-2 device:

```
#show interface ce29/1
Interface ce29/1
  Flexport: Breakout Control Port (Active): Break Out Enabled
  Hardware is ETH  Current HW addr: 80a2.357f.4ebd
  Physical:80a2.357f.4ebd  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
  Loopback Type: R-PHY
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2019 Apr 30 10:03:23 (00:00:58 ago)
  Statistics last cleared: 2019 Apr 30 09:43:30 (00:20:51 ago)
  30 second input rate 8648972937 bits/sec, 8446291 packets/sec
  30 second output rate 20723 bits/sec, 38 packets/sec
  RX
    unicast packets 3390485528 multicast packets 6205 broadcast packets 0
    input packets 3390494721 bytes 433982963744
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 1 jabbers 0
    input error 1
    input with dribble 0 input discard 39330
    Rx pause 0
  TX
    unicast packets 0 multicast packets 6009 broadcast packets 0
    output packets 6009 bytes 408564
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
```


© 2021 IP Infusion Inc. Proprietary

```
    Tx pause 0

#show interface brief
--------------------------------------------------------------------------------
--
Ethernet   Type          PVID  Mode              Status  Reason  Speed Port
Ctl Br/Bu  Loopbk
Interface                                                                  Ch #
--------------------------------------------------------------------------------
--
ce29/1        ETH          1     trunk             up      none    10g   --
Br  Yes              R-PHY
```

Interface counters after configuring loopback Rx PHY on ROUTER-2 device

```
#show interface counters rate gbps
+------------------+-------------+-------------+-------------+-------------
+
|     Interface    |    Rx gbps  |    Rx pps   |    Tx gbps  |    Tx pps
|
+------------------+-------------+-------------+-------------+-------------
+
 ce1/1               8.65           8446140       8.65           8446141
 ce5/1               8.65           8446058       8.65           8446058

#show interface counters rate gbps
+------------------+-------------+-------------+-------------+-------------
+
|     Interface    |    Rx gbps  |    Rx pps   |    Tx gbps  |    Tx pps
|
+------------------+-------------+-------------+-------------+-------------
+
 ce3/1               0.00           0             8.65           8446218
 ce29/1              8.65           8446222       0.00
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 14 LAG with RTAG7 Hashing

Overview

Traffic can be load balanced within an LACP trunk group and within an ECMP in a controlled manner using the RTAG7 hashing algorithm.

Topology

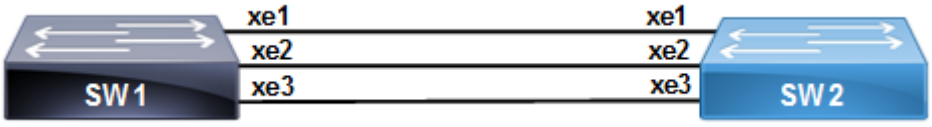


Figure 14-28: LACP with RTAG7 Configuration

Dynamic LAG with RTAG7

SW1

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)#vlan 2-10 bridge 1`	Configure VLANS.
`(config)#load-balance rtag7`	Enable load-balance for rtag7 globally.
`(config)#load-balance rtag7 l2 src-mac dest-mac ether-type vlan`	Enabling load-balance rtag7 for l2 with all options.
`(config)#load-balance rtag7 ipv4 dest-ipv4 src-ipv4 destl4-port srcl4-port protocol-id`	Enabling load-balance rtag7 for ipv4 with all options.
`(config)#interface po1`	Enter into port channel interface po1.
`(config-if)#switchport`	Configure po1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#port-channel load-balance rtag7`	Enable rtag7 load-balancing method.
`(config-if)#exit`	Exit the po1 interface mode.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.

© 2021 IP Infusion Inc. Proprietary

(config-if)#channel-group 1 mode active	Make port as part of port channel
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a layer 2 port.
(config-if)#bridge-group 1	Associate bridge to an interface.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe2 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel..
(config-if)#exit	Exit the xe2 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a layer 2 port .
(config-if)#bridge-group 1	Associate bridge to an interface.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel.
(config-if)#exit	Exit the xe3 interface mode.

SW2

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)#vlan 2-10 bridge 1	Configure VLANS.
(config)#interface po1	Enter interface mode
(config-if)#switchport	Configure po1 as a layer 2 port
(config-if)#bridge-group 1	Associate bridge to an interface
(config-if)#switchport mode trunk	Configure port as a trunk
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the po1 interface
(config-if)#exit	Exit the interface mode
(config)#interface xe1	Enter interface mode.
(config-if)#switchport	Configure xe1 as a layer 2 port.
(config-if)#bridge-group 1	Associate bridge to an interface.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe1 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel.
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a layer 2 port.
(config-if)#bridge-group 1	Associate bridge to an interface.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe2 interface.

© 2021 IP Infusion Inc. Proprietary

(config-if)#channel-group 1 mode active	Make port as part of port channel.
(config-if)#exit	Exit the xe2 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a layer 2 port.
(config-if)#bridge-group 1	Associate bridge to an interface.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#channel-group 1 mode active	Make port as part of port channel.

Validation

```
SW1#show etherchannel summary
Aggregator po1 100010
Aggregator Type: Layer2
Admin Key: 0010 - Oper Key 0010
Link: xe1 (5061) sync: 1
Link: xe2 (5062) sync: 1
Link: xe3 (5063) sync: 1

SW2#show etherchannel summary
Aggregator po1 7
Aggregator Type: Layer2
Admin Key: 0010 - Oper Key 0010
Link: xe1 (5013) sync: 1
Link: xe2 (5014) sync: 1
Link: xe3 (5015) sync: 1

SW1#show etherchannel detail
Aggregator po1 100001
Aggregator Type: Layer2
 Mac address: 3c:2c:99:28:52:1e
 Admin Key: 0001 - Oper Key 0001
  Actor LAG ID- 0x8000,3c-2c-99-7a-b2-e0,0x0001
  Receive link count: 3 - Transmit link count: 3
  Individual: 0 - Ready: 1
 Partner LAG ID- 0x8000,00-18-23-30-20-ce,0x0001
  Link: xe1 (5061) sync: 1
  Link: xe2 (5062) sync: 1
  Link: xe3 (5063) sync: 1
Collector max delay: 5
```

Static LAG with RTAG7

SW1

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)#vlan 2-10 bridge 1`	Configure VLANS
`(config)#load-balance rtag7`	Enable load-balance for rtag7 globally.
`(config)#load-balance rtag7 l2 src-mac dest-mac ether-type vlan`	Enabling load-balance rtag7 for l2 with all options.
`(config)#load-balance rtag7 ipv4 dest-ipv4 src-ipv4 destl4-port srcl4-port protocol-id`	Enabling load-balance rtag7 for ipv4 with all options .
`(config)#interface sa1`	Enter into port channel interface sa1.
`(config-if)#switchport`	Configuresa1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the sa1 interface.
`(config-if)#port-channel load-balance rtag7`	Enable rtag7 load-balancing method.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe2 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe2 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe3 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe3 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe3 interface mode.

© 2021 IP Infusion Inc. Proprietary

SW2

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)#vlan 2-10 bridge 1`	Configure VLANS.
`(config)#interface sa1`	Enter interface mode
`(config-if)#switchport`	Configure sa1 as a layer 2 port
`(config-if)#bridge-group 1`	Associate bridge to an interface
`(config-if)#switchport mode trunk`	Configure port as a trunk
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the sa1 interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface xe1`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe2 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe2 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe3 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe3 interface.
`(config-if)#static-channel-group 1`	Make port as part of Static port channel.
`(config-if)#exit`	Exit the xe3 interface mode.

Validation

```
SW1#show static-channel-group
 Static Aggregator: sa1
 Member Status
  xe1          up
  xe2          up
  xe3          up
SW1#
```

```
#show running-config interface sa1
!
interface sa1
load-interval 30
ip address 14.4.1.2/24
mtu 1600
port-channel load-balance rtag7
port-channel min-links 4
ip ospf network point-to-point
ip ospf cost 1000
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 15 Link Detection Debounce Timer

The link debounce timer avoids frequent updates (churn) to higher layer protocols during flapping of an interface. The initial link state is UP. The link goes DOWN. And if the Link comes UP and goes DOWN ,The link DOWN AND link UP timer is started and being restarted on each flap (link comes up and goes down again). For each link DOWN, link down timer will start and it restarts on flap within the link debounce interval. For each link UP, link up timer will start and it restarts on flap within the link debounce interval

Note:Keep the following in mind when using the Link detection debounce timer:

- Link debounce timer is supported only for physical L2 and L3 interfaces.
- When debounce timer is configured we won't be able to configure the link-debounce-timer config and viceversa.
- The link debounce flap-count refers to the number of flaps OcNOS receives while the debounce timer is running:
- The flap-count is only updated if the timer is still running and OcNOS receives a link status event for the interface.
- The flap-count is reset at the subsequent start of the link debounce timer.
- Protocol-specific timers such as BFD which depend on the link status should be configured to minimum of 1.5 times the value of the link debounce time. Otherwise it could affect the protocol states if the link debounce timer is still running.
- Protocols such as PO, OSPF, BFD, ISIS, BGP which depends on the link status, in this case we should ensure on both the connected interfaces we need to configure the link-debounce timer.

Topology

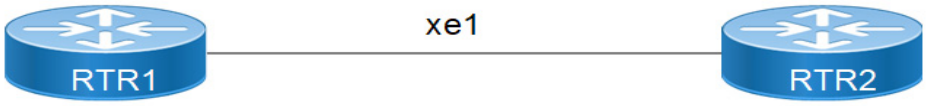


Figure 15-29: Link detection debounce timer topology

Configuration

RTR 1

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Enter into interface mode
`(config)#link-debounce-time 4000 5000`	Configure link-debounce-time where link-up timer is 4000ms and link-down timer is 5000ms
`(config)#exit`	Exit configure mode

RTR 2

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Enter into interface mode
`(config)# link-debounce-time 4000 5000`	Configure link-debounce-time where link-up timer is 4000ms and link-down timer is 5000ms
`(config)#exit`	Exit configure mode.

© 2021 IP Infusion Inc. Proprietary

Validation

```
#show running-config | i debounce link-debounce-time 4000 5000

#show interface xe1 | i Debounce Link Debounce timer: enable
    Linkup Debounce time 4000 ms Linkdown Debounce time 5000 ms
    Linkup Debounce status : idle
    Linkdown Debounce status : idle
```

RTR1 and RTR2 outputs after interface flap:

```
#show interface xe1 | i debounce Link Debounce timer: enable
Linkup Debounce time 4000 ms Linkdown Debounce time 5000 ms
Flap Count: 1
Last Debounce Flap :
Linkup Debounce status : idle
Linkdown Debounce status : idle

#show interface xe1 | i debounce
  Link Debounce timer: enable
    Linkup Debounce time 4000 ms Linkdown Debounce time 5000 ms
    Flap Count: 1
    Last Debounce Flap :    Linkup Debounce status : idle
 Linkdown Debounce status : idle
```

Log Messages

The following is a configuration example to log link debounce timer activity:

`#configure terminal`	Enter Configure mode
`(config)#logging level nsm 7`	Enable operational log to display debounce start and end.

Example Log Messages

```
2019 Feb 28 02:50:40.761 : OcNOS : NSM : INFO : Start UP->DOWN Link Debounce Timer on
interface xe1
2019 Feb 28 02:50:40.761 : OcNOS : NSM : NOTIF : [DEBOUNCE_EVENT_4]: Interface xe1
changed state from up to down
2019 Feb 28 02:50:43.543 : OcNOS : NSM : INFO : Start DOWN->UP Link Debounce Timer on
interface xe1
2019 Feb 28 02:50:43.543 : OcNOS : NSM : INFO : Interface xe1 Flapped, prev_state DOWN
new_state UP,flap count 1
2019 Feb 28 02:50:43.543 : OcNOS : NSM : NOTIF : [DEBOUNCE_EVENT_4]: Interface xe1
changed state from down to up
2019 Feb 28 02:50:45.761 : OcNOS : NSM : INFO : Link Debounce Timer Expired on interface
xe1 (initiated transition up->down), prev_state UP, new_state UP

2019 Feb 28 02:50:47.544 : OcNOS : NSM : INFO : Link Debounce Timer Expired on interface
xe1 (initiated transition down->up), prev_state UP, new_state UP
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 16 Max Session and Session Limit Configuration

Overview

User can configure session-limit for Telnet and SSH sessions separately but this max-session parameter value takes the precedence to restrict the maximum number of sessions. If user configured this max-session to be 4, then the device would allow only maximum of 4 SSH and Telnet sessions collectively irrespective of the individual SSH and Telnet max-session configuration. Active sessions won't be disturbed even if the configured max-session limit is lesser than the current active sessions. Default value for max-session value is 40 in line mode. There is no default value for the telnet-server-limit and ssh-server-limit.

After configuring max-session parameter if user tries to configure SSH/Telnet sessions then the total value of Telnet and SSH session limit should be lesser than the max-session value otherwise error will be thrown.

If already Telnet and SSH session-limits configured, now if user is configuring max-session then there won't be any error but maximum number of sessions will be limited to max-session value.

Topology

The procedures in this section use the topology as mentioned below. Setup consists of one node acting as Telnet server.



Figure 16-30: Telnet topology

Configuration of Telnet Session Limit Lesser than Max-Session

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable Feature Telnet in VRF Managementv
`(config)#telnet server session-limit 12 vrf management`	Configure the Session limit as 12 which is less than Max-Sesssion parameter in line VTY
`(config)#commit`	Perform commit to submit the changes done
`(config)#feature telnet vrf management`	Enable telnet feature in VRF management
`(config)#commit`	Perform commit to submit the changes done
`(config)#exit`	Exit configure mode

Validation

Check that the maximum telnet session possible are 12 which is lesser than Max-Session limit parameter value in line VTY.

```
#show running-config telnet server
telnet server session-limit 12 vrf management
feature telnet vrf management
no feature telnet
```

Configuration of SSH Server Session Limit Lesser than Max-Session

Configure SSH Server Session limit to be lesser than Max-Session.

Topology

Setup consists of one node acting as SSH server.



Figure 16-31: SSH Server topology

Configuration of SSH Server Session Limit Lesser than Max-Session

`#configure terminal`	Enter configure mode
`(config)#no feature ssh vrf management`	Disable feature SSH
`(config)#ssh server session-limit 12 vrf management`	Configure SSH server session-limit to be lesser than Max-Session limit
`(config)#commit`	Perform Commit to submit changes done
`(config)#feature ssh vrf management`	Enable feature SSH
`(config)#commit`	Perform commit to submit changes
`(config)#exit`	Exit configure mode

Validation

Check that the maximum SSH session possible are 12 which is lesser than Max-Session limit parameter value in line VTY.

```
#show running-config ssh server
feature ssh vrf management
ssh server session-limit 12 vrf management
```


© 2021 IP Infusion Inc. Proprietary

```
no feature ssh
```

Configuration of Telnet Session Limit Greater than Max-Session

In the below section, configure Telnet Session limit to be greater than Max-Session limit.

Topology

Setup consists of one node acting as Telnet server.



Figure 16-32: Telnet Session Topology

Configuration of Telnet server Session-Limit to be greater than line-VTY max-session

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable feature telnet
`(config)#telnet server session-limit 12 vrf management`	Configure Session-limit as 12 for telnet server
`(config)#commit`	Perform commit to submit changes
`(config)#feature telnet vrf management`	Enable Telnet server
`(config)#commit`	Perform commit to submit changes
`(config)#line vty`	Enter line VTY mode
`(config-line)#max-session 10`	Configure max-session as 10
`(config-line)#commit`	Perform commit to submit changes
`(config)#exit`	Exit configure mode

Validation

Check that the total telnet sessions possible is 10 even though telnet server session limit is configured as 12.

```
#show running-config telnet server
telnet server session-limit 12 vrf management
feature telnet vrf management
no feature telnet

#show running-config | grep max-session
 max-session 10
```

Configuration of SSH Session Limit Greater than Max-Session

In the below section, configure SSH Session limit to be greater than Max-Session limit.

Topology

Setup consists of one node acting as SSH server.



Configuration of SSH server Session-Limit to be greater than line-vty max-session

`#configure terminal`	Enter configure mode
`(config)#no feature ssh vrf management`	Disable feature SSH
`(config)#ssh server session-limit 12 vrf management`	Configure Session-limit as 12 for SSH server
`(config)#commit`	Perform commit to submit changes
`(config)#feature ssh vrf management`	Enable SSH server
`(config)#commit`	Perform commit to submit changes
`(config)#line vty`	Enter line VTY mode
`(config-line)#max-session 10`	Configure max-session as 10
`(config-line)#commit`	Perform commit to submit changes
`(config)#exit`	Exit configure mode

Validation

Check that the total SSH sessions possible is 10 even though SSH server session limit is configured as 12.

```
#show running-config ssh server
feature ssh vrf management
ssh server session-limit 12 vrf management
no feature ssh

#show running-config | grep max-session
 max-session 10
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 17 NTP Client Configuration

Overview

NTP modes differ based on how NTP allows communication between systems. NTP communication consists of time requests and control queries. Time requests provide the standard client/server relationship in which a client requests time synchronization from an NTP server. Control queries provide ways for remote systems to get configuration information and reconfigure NTP servers.

SNTP is a simplified form of NTP that does not reach the level of accuracy compared to a full implementation of NTP. SNTP can be used for simple applications where the requirements for accuracy and reliability are not too demanding. OcNOS supports SNTP version 4, defined in RFC 2030.

Note: OcNOS uses `ntp` for the SNTP command names instead of `sntp`.

Support for Default VRF via In-band Management

OcNOS supports NTP over the default and management VRFs via in-band management interface and OOB management interface, respectively.

By default, NTP runs on the management VRF.

NTP Modes

The following describes the various NTP node types.

Client

An NTP client is configured to let its clock be set and synchronized by an external NTP timeserver. NTP clients can be configured to use multiple servers to set their local time and are able to give preference to the most accurate time sources. They do not, however, provide synchronization services to any other devices.

Server

An NTP server is configured to synchronize NTP clients. Servers can be configured to synchronize any client or only specific clients. NTP servers, however, will accept no synchronization information from their clients and therefore will not let clients update or affect the server's time settings.

Peer

With NTP peers, one NTP-enabled device does not have authority over the other. With the peering model, each device shares its time information with the others, and each device can also provide time synchronization to the others.

Authentication

For additional security, you can configure your NTP servers and clients to use authentication. Routers support MD5 authentication for NTP. To enable a router to do NTP authentication:

1. Enable NTP authentication with the `ntp authenticate` command.
2. Define an NTP authentication key with the ntp authentication-key vrf management command. A unique number identifies each NTP key. This number is the first argument to the ntp authentication-key vrf management command.
3. Use the ntp trusted-key vrf management command to tell the router which keys are valid for authentication. If a key is trusted, the system will be ready to synchronize to a system that uses this key in its NTP packets. The trusted key should already be configured and authenticated.

NTP Configuration

NTP client, user can configure an association with a remote server. In this mode the client clock can synchronize to the remote server

After configuring the NTP servers, wait a few minutes before you verify that clock synchronization is successful. When clock synchronization has actually happened, there will be an asterisk “*” symbol along with the interface when you give the `show ntp peers` command.

Topology

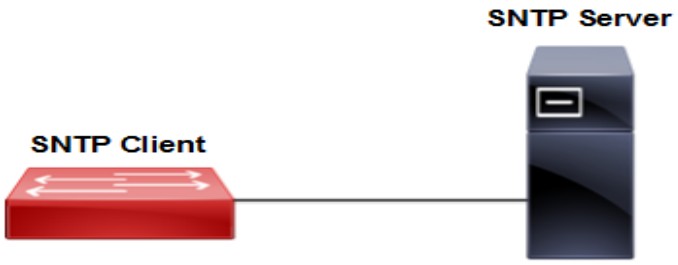


Figure 17-33: SNTP Client and Server

NTP Client

`#configure terminal`	Enter configure mode.
`(config)#feature ntp vrf management`	Configure feature on default or management VRF. By default this feature runs on management VRF.
`(config)# ntp enable vrf management`	This feature enables ntp. This will be enabled in default.
`(config)#ntp server 10.1.1.1 vrf management`	Configure ntp server ip address.
`(config)#exit`	Exit from the Configure Mode.

Validation Commands

```
#show ntp peers
    ------------------------------------------------------------
    Peer IP Address Serv/Peer
    ------------------------------------------------------------
    10.1.1.1 Server (configured)

    #show ntp peer-status
```


© 2021 IP Infusion Inc. Proprietary

```
    Total peers : 1
    * - selected for sync, + -  peer mode(active),
    - - peer mode(passive), = - polled in client mode
         remote           refid      st t when poll reach   delay   offset  jitter
    ==============================================================================
    *10.1.1.1        LOCAL(0)         7 u   14   32   37    0.194   -4.870   3.314
```

Maxpoll and Minpoll Configuration

The maximum poll interval are specified in defaults to 6 (64 seconds), but can be increased by the `maxpoll` option to an upper limit of 16 (18.2 hours). The minimum poll interval defaults to 4 (16 seconds), and this is also the minimum value of the `minpoll` option.

The client will retry between `minpoll` and `maxpoll` range configured for synchronization with the server.

Client

`#configure terminal`	Enter configure mode.
`(config)#feature ntp vrf management`	Configure feature on default or management VRF. By default this feature runs on management VRF.
`(config)#ntp server 10.1.1.1 maxpoll 7 minpoll 5 vrf management`	Configure `minpoll` and `maxpoll` range for ntp server.
`(config)#exit`	Exit from the Configure Mode.

Validation Commands

```
#show ntp peers
    ------------------------------------------------------------
    Peer IP Address Serv/Peer
    ------------------------------------------------------------
    10.1.1.1 Server (configured)

#show ntp peer-status
    Total peers : 1
    * - selected for sync, + -  peer mode(active),
    - - peer mode(passive), = - polled in client mode
         remote           refid      st t when poll reach   delay   offset  jitter
    ==============================================================================
    *10.1.1.1        LOCAL(0)         7 u   14   32   37    0.194   -4.870   3.314
```

NTP Authentication

When you enable NTP authentication, the device synchronizes to a time source only if the source carries the authentication keys specified with the source by key identifier. The device drops any packets that fail the authentication check, and prevents them from updating the local clock.

Client

`#configure terminal`	Enter configure mode.
`(config)#feature ntp vrf management`	Enable feature on default or management VRF. By default this feature runs on management VRF..
`(config)#ntp server 10.1.1.1 vrf management`	Configure ntp server ip address.
`(config)#ntp authenticate vrf management`	Enable NTP Authenticate. NTP authentication is disabled by default.
`(config)#ntp authentication-key 1234 md5 text vrf management`	Configure ntp authentication key along with md5 value.
`(config)#ntp trusted-key 1234 vrf management`	Configure trusted key <1-65535>
`(config)#exit`	Exit from the Configure Mode.

Validation Commands

```
#show ntp authentication-status
    Authentication enabled

#show ntp authentication-keys
    --------------------------
     Auth Key       MD5 String
    --------------------------
    1234              SWWX

#show ntp trusted-keys
    Trusted Keys:
    1234
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 18 Port Breakout Configuration

This chapter contains an overview of splitting single 40G port to 4x10G ports.

Overview

Port Breakout system enables numerous 40GbE/100GbE ports to be broken out into 4x10GbE, 4x25GbE, 2x50GbE ports through a secure, highly reliable breakout cabling solution. Today's large-scale virtualized datacenter networks require a mix of 10Gb, 25Gb, 40Gb and 100Gb Ethernet interface speeds able to utilize the widest range of flexible connectivity options. These same networks require a variety of cost-effective cabling options for both addressing connectivity and allowing for simple migrations as network speeds and density requirements evolve. As data centers scale and bandwidth demands increase, the networking infrastructure must be capable of scaling with it. Port Breakout feature provides flexibility in splitting 40G to 4x10G and 100G to 4x10G, 4x25G, 2x50G cabling and vice-versa whenever requires, and hence provide Administrator a great flexibility in choosing the port speed as per their requirement. A Port Breakout group consists of 4 ports, first port will be control port and the rest 3 are subsidiary ports. Naming of Control port and its subsidiary port is as below

xe50/1, xe50/2, xe50/3, xe50/4

In xe50, numeral 50 indicates the slot of the port on a board and numerals after "/" indicates port numbers on that slot. First port (interface 50/1 in above example) is always control port whereas the rest 3 ports (ports 50/2, 50/3 and 50/4) are subsidiary ports. Only Control port can become 40G or 100G port. For Transceiver types mentioned in fec command will be enabled by default for both control port and the rest 3 subsidiary ports. If Peer is not supporting FEC, fec off needs to be configured on the ports manually.

Currently below breakout options are available

- 40G ports
  - 40G to 4x10G breakout ports
- 100G ports
  - 100G to 4x10G breakout ports
  - 100G to 4x25G breakout ports (due to HW limitation Autoneg isn't supported)
  - 100G to 2x50G breakout ports (due to HW limitation Autoneg isn't supported).

Note: There are some configuration restrictions for Subsidiary ports such as:

1. Port breakout enable/disable is not allowed on Subsidiary ports.
2. Speed, Duplex configurations are not allowed on InActive Subsidiary ports.
3. One control port and subsidiary ports will be supported in 100g to 2x50G breakout
   For Example: Port XE1/1(control port) and XE1/3(subsidiary port) will be active out of 4 ports.

Terminology

Following is a brief description of terms and concepts used to describe port breakout.

Ctl: Control port

A 40G or 100G split-able port is called Control port.

Brk: Port Breakout

A control port which is split into 4x10G 4x25G or 2x50 ports.

Subsidiary ports

Ports which are members of Control Port, A subsidiary port can be Active or InActive

IA: InActive Ports

Subsidiary ports whose control port is not configured for “Port Breakout”

Configuring Port Breakout 40G to 4x10G

Configuring Port Breakout (40G to 4x10G) is provided in below section.

`#configure terminal`	Enter configure mode.
`(config)#interface xe50/1`	Specify the interface `(xe5/1)` to be configured for port Breakout.
`(config-if)# port breakout enable`	Configure port breakout on interface
`(config-if)#exit`	Exit interface mode.

Removing Port Breakout

Removing Port Breakout is provided in below section.

Note: Interface xe50/1 is back to back connected and interfaces are up.

`#configure terminal`	Enter configure mode.
`(config)#interface xe50/1`	Specify the interface `(xe5/1)` to be configured for port Breakout.
`(config-if)#no port breakout`	Unconfigure port breakout on interface
`(config-if)#exit`	Exit interface mode.

Validation

```
#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min-links) - Protocol Down Min-links
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
```


© 2021 IP Infusion Inc. Proprietary

```
-------------------------------------------------------------------------------
--
Interface     Type             Status  Reason  Speed
Interface
-------------------------------------------------------------------------------
--
eth0          METH             up      --      1g


-------------------------------------------------------------------------------
--
Interface    Status      Description
-------------------------------------------------------------------------------
--
lo           up          --
lo.management  up          --


-------------------------------------------------------------------------------
--
Ethernet   Type  PVID  Mode              Status  Reason  Speed Port    Ctl Br/
Bu
Interface                                                    Ch #
-------------------------------------------------------------------------------
--
xe1        ETH   --    routed            up      none    1g    --       Bu  No
xe2        ETH   --    routed            down    PD      10g   --       No  No
xe3        ETH   --    routed            down    PD      10g   --       No  No
xe4        ETH   --    routed            down    PD      10g   --       No  No
xe5        ETH   --    routed            down    PD      10g   --       Bu  No
xe6        ETH   --    routed            down    PD      10g   --       No  No
xe7        ETH   --    routed            down    PD      10g   --       No  No
xe8        ETH   --    routed            down    PD      10g   --       No  No
xe9        ETH   --    routed            down    PD      10g   --       Bu  No
xe10       ETH   --    routed            down    PD      10g   --       No  No
xe11       ETH   --    routed            down    PD      10g   --       No  No
xe12       ETH   --    routed            down    PD      10g   --       No  No
xe13       ETH   --    routed            down    PD      10g   --       Bu  No
xe14       ETH   --    routed            down    PD      10g   --       No  No
xe15       ETH   --    routed            down    PD      10g   --       No  No
xe16       ETH   --    routed            down    PD      10g   --       No  No
xe17       ETH   --    routed            down    PD      10g   --       Bu  No
xe18       ETH   --    routed            down    PD      10g   --       No  No
xe19       ETH   --    routed            down    PD      10g   --       No  No
xe20       ETH   --    routed            down    PD      10g   --       No  No
xe21       ETH   --    routed            down    PD      10g   --       Bu  No
xe22       ETH   --    routed            down    PD      10g   --       No  No
xe23       ETH   --    routed            down    PD      10g   --       No  No
xe24       ETH   --    routed            down    PD      10g   --       No  No
xe25       ETH   --    routed            up      none    10g   --       Bu  No
xe26       ETH   --    routed            down    PD      10g   --       No  No
xe27       ETH   --    routed            up      none    10g   --       No  No
xe28       ETH   --    routed            down    PD      10g   --       No  No
xe29       ETH   --    routed            down    PD      10g   --       Bu  No
xe30       ETH   --    routed            down    PD      10g   --       No  No
xe31       ETH   --    routed            down    PD      10g   --       No  No
```

```
xe32       ETH   --    routed            down    PD      10g   --       No  No
xe33       ETH   --    routed            down    PD      10g   --       Bu  No
xe34       ETH   --    routed            down    PD      10g   --       No  No
xe35       ETH   --    routed            down    PD      10g   --       No  No
xe36       ETH   --    routed            down    PD      10g   --       No  No
xe37       ETH   --    routed            down    PD      10g   --       Bu  No
xe38       ETH   --    routed            down    PD      10g   --       No  No
xe39       ETH   --    routed            down    PD      10g   --       No  No
xe40       ETH   --    routed            down    PD      10g   --       No  No
xe41       ETH   --    routed            down    PD      10g   --       Bu  No
xe42       ETH   --    routed            down    PD      10g   --       No  No
xe43       ETH   --    routed            down    PD      10g   --       No  No
xe44       ETH   --    routed            down    PD      10g   --       No  No
xe45       ETH   --    routed            down    PD      10g   --       Bu  No
xe46       ETH   --    routed            down    PD      10g   --       No  No
xe47       ETH   --    routed            down    PD      10g   --       No  No
xe48       ETH   --    routed            down    PD      10g   --       No  No
xe49/1     ETH   --    routed            down    PD      40g   --       Br  No
xe49/2     ETH   --    routed            down    IA      --    --       No  No
xe49/3     ETH   --    routed            down    IA      --    --       No  No
xe49/4     ETH   --    routed            down    IA      --    --       No  No
xe50/1     ETH   --    routed            up      none    40g   --       Br  No
xe50/2     ETH   --    routed            down    IA      --    --       No  No
xe50/3     ETH   --    routed            down    IA      --    --       No  No
xe50/4     ETH   --    routed            down    IA      --    --       No

#show interface xe50/1
Interface xe50/1
  Flexport: Breakout Control Port (Active): Break Out disabled
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba4  Logical:(not set)
  Port Mode is Router
  Interface index: 10053
  Metric 1 mtu 1500 duplex-full link-speed 40g
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:03:20 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 20 bits/sec, 0 packets/sec
  5 minute output rate 20 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 7 bytes 766
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 7 broadcast packets 0
    output packets 7 bytes 766
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```


© 2021 IP Infusion Inc. Proprietary

```
#show interface xe50/2
Interface xe50/2
  Flexport: Non Control Port (InActive)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba5  Logical:(not set)
  Port Mode is Router
  Interface index: 10054
  Metric 1 mtu 1500
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:03:46 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 0 broadcast packets 0
    output packets 0 bytes 0
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show interface xe50/3
Interface xe50/3
  Flexport: Non Control Port (InActive)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba6  Logical:(not set)
  Port Mode is Router
  Interface index: 10055
  Metric 1 mtu 1500
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:07:30 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
```

```
    Rx pause 0
  TX
    unicast packets 0 multicast packets 0 broadcast packets 0
    output packets 0 bytes 0
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show interface xe50/4
Interface xe50/4
  Flexport: Non Control Port (InActive)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba7  Logical:(not set)
  Port Mode is Router
  Interface index: 10056
  Metric 1 mtu 1500
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:07:36 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 0 broadcast packets 0
    output packets 0 bytes 0
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```

Here xe50/1 is a control Port whereas xe50/2, xe50/3 and xe50/4 are their subsidiary ports. The out-put shows only xe50/1 is active (interface up and running) whereas other ports are inactive (interface up but not running).

Below Outputs after applying port-breakout configured on xe50/1:

```
#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min-links) - Protocol Down Min-links
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
```


© 2021 IP Infusion Inc. Proprietary

```
       Ctl - Control Port (Br-Breakout/Bu-Bundle)


-------------------------------------------------------------------------------
--
Interface     Type             Status  Reason  Speed
Interface
-------------------------------------------------------------------------------
--
eth0          METH             up      --      1g


-------------------------------------------------------------------------------
--
Interface    Status      Description
-------------------------------------------------------------------------------
--
lo           up          --
lo.management  up          --


-------------------------------------------------------------------------------
--
Ethernet   Type  PVID  Mode              Status  Reason  Speed Port    Ctl Br/
Bu
Interface                                                    Ch #
-------------------------------------------------------------------------------
--
xe1        ETH   --    routed            up      none    1g    --       Bu  No
xe2        ETH   --    routed            down    PD      10g   --       No  No
xe3        ETH   --    routed            down    PD      10g   --       No  No
xe4        ETH   --    routed            down    PD      10g   --       No  No
xe5        ETH   --    routed            down    PD      10g   --       Bu  No
xe6        ETH   --    routed            down    PD      10g   --       No  No
xe7        ETH   --    routed            down    PD      10g   --       No  No
xe8        ETH   --    routed            down    PD      10g   --       No  No
xe9        ETH   --    routed            down    PD      10g   --       Bu  No
xe10       ETH   --    routed            down    PD      10g   --       No  No
xe11       ETH   --    routed            down    PD      10g   --       No  No
xe12       ETH   --    routed            down    PD      10g   --       No  No
xe13       ETH   --    routed            down    PD      10g   --       Bu  No
xe14       ETH   --    routed            down    PD      10g   --       No  No
xe15       ETH   --    routed            down    PD      10g   --       No  No
xe16       ETH   --    routed            down    PD      10g   --       No  No
xe17       ETH   --    routed            down    PD      10g   --       Bu  No
xe18       ETH   --    routed            down    PD      10g   --       No  No
xe19       ETH   --    routed            down    PD      10g   --       No  No
xe20       ETH   --    routed            down    PD      10g   --       No  No
xe21       ETH   --    routed            down    PD      10g   --       Bu  No
xe22       ETH   --    routed            down    PD      10g   --       No  No
xe23       ETH   --    routed            down    PD      10g   --       No  No
xe24       ETH   --    routed            down    PD      10g   --       No  No
xe25       ETH   --    routed            up      none    10g   --       Bu  No
xe26       ETH   --    routed            down    PD      10g   --       No  No
xe27       ETH   --    routed            up      none    10g   --       No  No
xe28       ETH   --    routed            down    PD      10g   --       No  No
xe29       ETH   --    routed            down    PD      10g   --       Bu  No
xe30       ETH   --    routed            down    PD      10g   --       No  No
```

```
xe31       ETH   --    routed            down    PD      10g   --       No  No
xe32       ETH   --    routed            down    PD      10g   --       No  No
xe33       ETH   --    routed            down    PD      10g   --       Bu  No
xe34       ETH   --    routed            down    PD      10g   --       No  No
xe35       ETH   --    routed            down    PD      10g   --       No  No
xe36       ETH   --    routed            down    PD      10g   --       No  No
xe37       ETH   --    routed            down    PD      10g   --       Bu  No
xe38       ETH   --    routed            down    PD      10g   --       No  No
xe39       ETH   --    routed            down    PD      10g   --       No  No
xe40       ETH   --    routed            down    PD      10g   --       No  No
xe41       ETH   --    routed            down    PD      10g   --       Bu  No
xe42       ETH   --    routed            down    PD      10g   --       No  No
xe43       ETH   --    routed            down    PD      10g   --       No  No
xe44       ETH   --    routed            down    PD      10g   --       No  No
xe45       ETH   --    routed            down    PD      10g   --       Bu  No
xe46       ETH   --    routed            down    PD      10g   --       No  No
xe47       ETH   --    routed            down    PD      10g   --       No  No
xe48       ETH   --    routed            down    PD      10g   --       No  No
xe49/1     ETH   --    routed            down    PD      40g   --       Br  No
xe49/2     ETH   --    routed            down    IA      --    --       No  No
xe49/3     ETH   --    routed            down    IA      --    --       No  No
xe49/4     ETH   --    routed            down    IA      --    --       No  No
xe50/1     ETH   --    routed            up      none    10g   --       Br  Yes
xe50/2     ETH   --    routed            up      none    10g   --       No  No
xe50/3     ETH   --    routed            up      none    10g   --       No  No
xe50/4     ETH   --    routed            up      none    10g   --       No

#show interface xe50/1
Interface xe50/1
  Flexport: Breakout Control Port (Active): Break Out Enabled
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba4  Logical:(not set)
  Port Mode is Router
  Interface index: 10053
  Metric 1 mtu 1500 duplex-full link-speed 10g
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:54:58 (00:32:03 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 23 bytes 801
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 16
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 14 broadcast packets 0
    output packets 14 bytes 1532
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
```


© 2021 IP Infusion Inc. Proprietary

```
    Tx pause 0

#show interface xe50/2
Interface xe50/2
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba5  Logical:(not set)
  Port Mode is Router
  Interface index: 10054
  Metric 1 mtu 1500 duplex-full link-speed 10g
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:45:16 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 23 bytes 790
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 16
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 7 broadcast packets 0
    output packets 7 bytes 766
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show interface xe50/3
Interface xe50/3
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba6  Logical:(not set)
  Port Mode is Router
  Interface index: 10055
  Metric 1 mtu 1500 duplex-full link-speed 10g
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:42:15 (00:45:31 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 26 bytes 801
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 19
```

```
      input with dribble 0 input discard 0
      Rx pause 0
    TX
      unicast packets 0 multicast packets 7 broadcast packets 0
      output packets 7 bytes 766
      jumbo packets 0
      output errors 0 collision 0 deferred 0 late collision 0
      output discard 0
      Tx pause 0

#show interface xe50/4
Interface xe50/4
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: a82b.b5ad.db6f
  Physical:a82b.b5ad.dba7  Logical:(not set)
  Port Mode is Router
  Interface index: 10056
  Metric 1 mtu 1500 duplex-full link-speed 10g
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2001 Feb 13 18:54:58 (00:33:07 ago)
  Statistics last cleared: Never
  inet6 fe80::aa2b:b5ff:fead:db6f/64
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 22 bytes 792
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 15
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 14 broadcast packets 0
    output packets 14 bytes 1532
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```

Configuring Port Breakout (100G to 4x10G)

Configuring Port Breakout (100G to 4x10G) is provided in below section.

`#configure terminal`	Enter configure mode.
`(config)#interface ce1/1`	Specify the interface `(ce1/1)` to be configured for port Breakout.
`(config-if)# port breakout enable 4x10g`	Configure port breakout on interface
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

Note: Interface ce1/1 is back to back connected and interfaces are up.

Validation

```
#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min-links) - Protocol Down Min-links
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)


--------------------------------------------------------------------------------
--
Ethernet   Type  PVID  Mode              Status  Reason  Speed Port    Ctl Br/
Bu
Interface                                                      Ch #
--------------------------------------------------------------------------------
--
ce1/1      ETH   --    routed            up      none    10g   --       Br Yes
ce1/2      ETH   --    routed            up      none    10g   --       No  No
ce1/3      ETH   --    routed            up      none    10g   --       No  No
ce1/4      ETH   --    routed            up      none    10g   --       No  No
```

Configuring Port Breakout (100G to 4x25G)

Configuring Port Breakout (100G to 4x25G) is provided in below section.

`#configure terminal`	Enter configure mode.
`(config)#interface ce1/1`	Specify the interface `(ce1/1)` to be configured for port Breakout.
`(config-if)# port breakout enable 4x25g`	Configure port breakout on interface
`(config-if)#exit`	Exit interface mode.

Note: Interface ce1/1 is back to back connected and interfaces are up.

Validation

```
#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
```

```
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min-links) - Protocol Down Min-links
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)

-------------------------------------------------------------------------------
--
Ethernet   Type  PVID  Mode            Status  Reason  Speed Port    Ctl Br/Bu
Interface                                                    Ch #
-------------------------------------------------------------------------------
--
ce1/1      ETH   --    routed            up      none    25g   --       Br
Yes
ce1/2      ETH   --    routed            up      none    25g   --       No  No
ce1/3      ETH   --    routed            up      none    25g   --       No  No
ce1/4      ETH   --    routed            up      none    25g   --       No  No
```

Configuring Port Breakout (100G to 2x50G)

Configuring Port Breakout (100G to 2x50G) is provided in below section.

`#configure terminal`	Enter configure mode.
`(config)#interface ce1/1`	Specify the interface `(ce1/1)` to be configured for port Breakout.
`(config-if)# port breakout enable 2x50g`	Configure port breakout on interface
`(config-if)#exit`	Exit interface mode.

Note: Interface ce1/1 is back to back connected and interfaces are up.

Validation

```
#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min-links) - Protocol Down Min-links
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)


-------------------------------------------------------------------------------
--
Ethernet   Type  PVID  Mode              Status  Reason  Speed Port    Ctl Br/
Bu
Interface                                                      Ch #
```


© 2021 IP Infusion Inc. Proprietary

```
--------------------------------------------------------------------------------
--
ce1/1       ETH    --     routed             up       none     50g    --        Br
Yes
ce1/2       ETH    --     routed             down     IA       --     --        No   No
ce1/3       ETH    --     routed             up       none     50g    --        No   No
ce1/4       ETH    --     routed             down     IA       --     --        No   No
```

Configuring Port Breakout at Global Configuration Level

This port breakout command at global configuration level is applicable only for Trident III and Tomahawk II platforms. The interface level breakout and global hardware-profile CLI does not work for Trident III and Tomahawk II platforms.

Configuring Port Breakout (4X10g | 4X25g | 2X50g) at global configuration level is provided in below section.

`#configure terminal`	Enter configure mode.
`OcNOS(config)# port 49 breakout 4X10g`	Specify the port interface number (49) to breakout to (2X50g or 4X10g 4X25g) at global interface, where 49 refers to ce49 interface.
`OcNOS(config)#exit`	Exit interface mode.

Note: After the port breakout, the interface name is changed to xe49/1-xe49/4 globally.

Validation

```
#show running-config interface xe49/1
!
interface xe49/1
!

#show port-breakout details
----------------------------------------
Max Brkout Avail    Max Brkout Avail

0 x4X or 0 x2X



4 x4X or 4 x2X

----------------------------------------
Block1              Block2
----------------------------------------
Port  ||  Mode      Port  ||  Mode
----------------------------------------
1                   40
2                   41
3                   43
4                   44
5                   45
6                   46
7                   47
```

```
8                       48
9                       49          4X10G
10                      50          4X10G
11                      51          4X10G
12                      52          4X10G
13                      53
14                      54
15                      55
16                      56
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
42
OcNOS#
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 19 Proxy ARP and Local Proxy ARP

Overview

Proxy ARP (RFC 1027) is a technique by which a device on a given network answers the ARP queries for a network address that is not on that network. The Proxy ARP is aware of the location of the traffic's destination, and offers its own MAC address as destination. The captured traffic is then typically routed by the Proxy to the intended destination via another interface. Proxy ARP can help machines on a subnet reach remote subnets without the need to configure routing or a default gateway.

Use `no ip proxy-arp` to disable Proxy ARP, Proxy ARP is disabled by default.

Topology

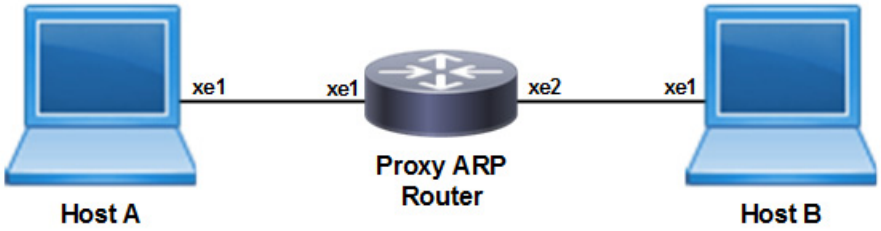


Figure 19-34: Sample topology

Configuration

Host A

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#ip address 20.20.0.2/24`	Assign an IPv4 address to the interface
`(config)#end`	Exit interface and configure mode

Host B

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#ip address 20.20.1.2/24`	Assign an IPv4 address to the interface
`(config)#end`	Exit interface and configure mode

Proxy ARP Server

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#ip address 20.20.0.1/24`	Assign an IPv4 address to the interface

`(config-if)#ip proxy-arp`	Enable proxy ARP
`(config-if)#exit`	Exit interface mode
`(config-if)#interface xe2`	Enter interface mode
`(config-if)#ip address 20.20.1.1/24`	Assign an IPv4 address to the interface
`(config)#end`	Exit interface and configure mode

Validation

```
#show running-config arp
!
interface xe1
ip proxy-arp
!
```

The `show arp` command on the hosts shows the ARP table entries to reach different subnets. Ping Host B from Host A. The ARP table should have router's xe1 interface MAC address to reach Host B. Execute the command at Host A.

```
#show arp

Address                  HWaddress              Interface      Type
20.20.0.2                52:54:00:24:43:23       eth1          Dynamic
192.168.52.1             fe:54:00:0d:1e:dc       eth0          Dynamic
```

Local Proxy ARP Overview

The local proxy ARP feature enables local proxy support for ARP requests at the interface level. The router answers all ARP requests on the configured subnet, even for clients that should not normally need routing. Local proxy ARP means that the traffic comes in and goes out the same interface.

Local proxy ARP allows responding to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly.

© 2021 IP Infusion Inc. Proprietary

Topology

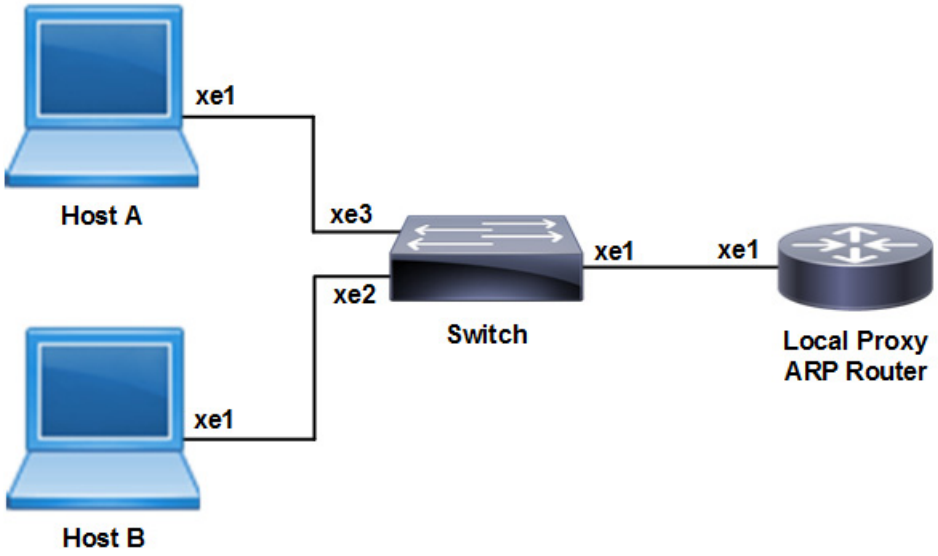


Figure 19-35: Sample topology

Configuration

Host A

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#ip address 20.20.0.2/24`	Assign an IPv4 address to the interface
`(config)#end`	Exit interface and configure mode

Host B

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#ip address 20.20.0.3/24`	Assign an IPv4 address to the interface
`(config)#end`	Exit interface and configure mode

Switch Private VLAN

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create ieee vlan-bridge on switch for pvlan configuration
`(config)#vlan database`	Enter VLAN database mode
`(config-vlan)#vlan 100-101 bridge 1 state enable`	Create VLANs 100 and 101 as part of bridge 1
`(config-vlan)#private-vlan 100 primary bridge 1`	Configure VLAN 100 as primary VLAN
`(config-vlan)#private-vlan 101 isolated bridge 1`	Configure VLAN 101 as isolated VLAN

© 2021 IP Infusion Inc. Proprietary

(config-vlan)#private-vlan 100 association add 101 bridge 1	Associate secondary VLAN 101 to primary VLAN 100
(config-vlan)#exit	Exit VLAN database mode
(config)#interface xe1	Enter interface mode
(config-if)#switchport	Configure xe1 as a Layer 2 interface
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary VLAN to the interface
(config-if)#switchport mode private-vlan promiscuous	Make the interface a promiscuous port
(config-if)#switchport private-vlan mapping 100 add 101	Associate primary VLAN 100 and secondary VLAN 101 to a promiscuous port
(config-if)#exit	Exit interface mode
(config)#interface xe2	Enter interface mode
(config-if)#switchport	Make the interface a Layer 2 interface
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary VLAN to the interface
(config-if)#switchport mode private-vlan promiscuous	Make the interface a promiscuous port
(config-if)#switchport private-vlan mapping 100 add 101	Associate primary VLAN 100 and secondary VLAN 101 to a promiscuous port
(config-if)#exit	Exit interface mode
(config)#interface xe3	Enter interface mode
(config-if)#switchport	Make the interface a Layer 2 interface
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary VLAN to the interface
(config-if)#switchport mode private-vlan promiscuous	Make the interface a promiscuous port
(config-if)#switchport private-vlan mapping 100 add 101	Associate primary VLAN 100 and secondary VLAN 101 to a promiscuous port
(config-if)#exit	Exit interface mode

Router Local Proxy ARP

#configure terminal	Enter configure mode
(config)#interface xe1	Enter interface mode
(config-if)#ip address 20.20.0.3/24	Assign an IPv4 address to the interface
(config-if)#ip local-proxy-arp	Enable local proxy ARP
(config)#end	Exit interface and configure mode

Validation

The show arp command on hosts shows the arp table entries to reach different subnets. Ping Host B from Host A. The ARP table should have Router's xe1 interface MAC address to reach Host B. Execute the below command at Host A.

```
#show arp
```


© 2021 IP Infusion Inc. Proprietary

```
Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 2
Address          Age          MAC Address     Interface    State
20.20.0.3      00:02:39      ecf4.bbc0.3d71      xe1       STALE.
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 20 RADIUS Client Configuration

Overview

Remote Authentication Dial In User Service (RADIUS) is a remote authentication protocol that is used to communicate with an authentication server.

A RADIUS server is responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

The key points for RADIUS authentication are:

- Transactions between client and server are authenticated through the use of a shared key and this key is never sent over the network.
- The password is encrypted before sending it over the network.

RADIUS Server Authentication



Figure 20-36: RADIUS Server Host Configuration

Host

`#configure terminal`	Enter configure mode.
`(config)# radius-server login key testing101 vrf management`	Specify the global key for radius servers that are not configured with their respective keys for management vrf. This key should match the one present in the config file of tacacs server.
`(config)# radius-server login key testing101`	Specify the global key for radius servers that are not configured with their respective keys for default vrf. This key should match the one present in the config file of tacacs server
`(config)# radius-server login host 10.16.19.2 vrf management key testing123`	Specify the radius server ipv4 address to be configured with shared local key for management vrf. The same key should be present on the server config file.
`(config)# radius-server login host 10.16.19.2 key testing123`	Specify the radius server ipv4 address to be configured with shared local key for default vrf. The same key should be present on the server config file.
`(config)# radius-server login host 10.12.30.86 vrf management auth-port 1045`	Specify the radius server ipv4 address to be configured with port number for management vrf. The radius server should be started with same port number.

`(config)# radius-server login host 10.12.30.86 auth-port 1045`	Specify the radius server ipv4 address to be configured with port number for default vrf.The radius server should be started with same port number
`(config)#radius-server login host 10.12.17.11 vrf management key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for management vrf. The radius server should be started with same port number.
`(config)#radius-server login host 10.12.17.11 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for default vrf. The radius server should be started with same port number. The radius server should be started with same port number
`(config)#radius-server login host Radius-Server-1 vrf management key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 2`	Specify the radius server configured with hostname, key authentication port number, accounting port number, for management VRF. The radius server should be started with same port number
`radius-server login host Radius-Server-1 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 2`	Specify the radius server configured with hostname sequence number, key and port number for default VRF. The radius server should be started with same port number.
`(config)#aaa authentication login default vrf management group radius`	Enable authentication for radius server configured for management VRF. Authorization is also enabled by default
`(config)#aaa authentication login default group radius`	Enable authentication for radius server configured for default vrf. Authorization is also enabled by default.
`(config)#aaa authentication login default vrf management group radius local`	Enable authentication for radius server and fallback to local configured for management VRF. Authorization is also enabled by default
`(config)#aaa authentication login default group radius local`	Enable authentication for radius server and fallback to local configured for default vrf. Authorization is also enabled by default
`(config)#aaa authentication login default vrf management group radius local none`	Enable authentication for radius server, fallback to local followed by fallback to none, configured for management VRF. Authorization is also enabled by default
`(config)#aaa authentication login default radius local none`	Enable authentication for radius server, fallback to local followed by fallback to none, configured for default vrf. Authorization is also enabled by default
`(config)#aaa authentication login default vrf management group radius none`	Enable authentication for radius, fallback to none, configured for management VRF. Authorization is also enabled by default
`(config)#aaa authentication login default group radius none`	Enable authentication for radius, fallback to none, configured for default VRF. Authorization is also enabled by default
`(config)#aaa group server radius G1 vrf management`	Create aaa radius group G1 for management vrf
`(config)#aaa group server radius G1`	Create AAA radius group G1 for default VRF
`(config-radius)#server 10.12.30.86`	Make the radius server 10.12.30.86 a part of this group G1 for default VRF
`(config-radius)#server Radius-Server-1`	Make Radius-Server-1 a part of this group G1
`(config-radius)#exit`	Exit radius mode
`(config)#aaa group server radius G1`	Enter radius mode
`(config-radius)#server 10.12.30.86`	Make the radius server 10.12.30.86 a part of this group G1 for default vrf
`(config-radius)#server Radius-Server-1`	Make Radius-Server-1 a part of this group G1
`(config)#exit`	Exit radius mode.

© 2021 IP Infusion Inc. Proprietary

`(config)#aaa authentication login default vrf management group G1`	Authenticate the tacacs+ group G1 with aaa authentication for management vrf
`(config)#aaa authentication login default group G1`	Authenticate the tacacs+ group G1 with aaa authentication for default vrf

Validation

To verify the RADIUS authentication process, use SSH or Telnet from the host machine to Host IP with the authenticating user created, and provide a RADIUS server password and check whether the client validates the user with the corresponding username and password.

```
OcNOS#show radius-server vrf management
        VRF: management
Global RADIUS shared secret: ********
timeout value: 5

Total number of servers:3

Following RADIUS servers are configured:

                10.12.17.11:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  timeout:6
                  RADIUS shared secret:********

                10.12.30.86:
                  available for authentication on port:1045
                  available for accounting on port:1813

                10.16.19.2:
                  available for authentication on port:1812
                  available for accounting on port:1813
                  RADIUS shared secret:********

#show radius-server vrf all
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
```

```
                  RADIUS shared secret:********
        VRF: default
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

#show radius-server
        VRF: default
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

#show radius-server vrf management sorted
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********
```


© 2021 IP Infusion Inc. Proprietary

```
                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

#show radius-server vrf all sorted
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********


                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

        VRF: default
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********


                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

#show radius-server sorted
        VRF: default
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:
```

```
                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********


                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

#show radius-server vrf management groups
        VRF: management

        group radius:
                server: all configured radius servers

        group rad1:
                server Radius-Server-1:
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1:
                auth_port is 60000
                acct_port is 60000
                key is ********

#show radius-server vrf all groups
        VRF: management

        group radius:
                server: all configured radius servers

        group rad1:
                server Radius-Server-1:
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1:
                auth_port is 60000
                acct_port is 60000
                key is ********

        VRF: default

        group radius:
                server: all configured radius servers
```


© 2021 IP Infusion Inc. Proprietary

```
        group rad1:
                server Radius-Server-1:
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1:
                auth_port is 60000
                acct_port is 60000
                key is ********

#show radius-server groups
        VRF: default

        group radius:
                server: all configured radius servers

        group rad1:
                server Radius-Server-1:
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1:
                auth_port is 60000
                acct_port is 60000
                key is ********

#show radius-server vrf management groups rad1
        VRF: management

        group rad1:
                server Radius-Server-1
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1
                auth_port is 60000
                acct_port is 60000
                key is ********

#show radius-server vrf all groups rad1
        VRF: management

        group rad1:
                server Radius-Server-1
                auth_port is 60000
                acct_port is 60000
                key is ********
```

```
                server 100.0.0.1
                auth_port is 60000
                acct_port is 60000
                key is ********


        VRF: default

        group rad1:
                server Radius-Server-1
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1
                auth_port is 60000
                acct_port is 60000
                key is ********

#show radius-server groups rad1
        VRF: default

        group rad1:
                server Radius-Server-1
                auth_port is 60000
                acct_port is 60000
                key is ********

                server 100.0.0.1
                auth_port is 60000
                acct_port is 60000
                key is ********

#show radius vrf management
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
```


© 2021 IP Infusion Inc. Proprietary

```
                  RADIUS shared secret:********

#show radius vrf all
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********
        VRF: default
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                100.0.0.1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

#show radius
        VRF: default
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

                100.0.0.1:
```

```
                  available for authentication on port:60000
                  available for accounting on port:60000
                  RADIUS shared secret:********

#show aaa authentication vrf management
                VRF: management
  default: group radius
  console: local

#show aaa authentication vrf all
                VRF: management
  default: group radius
  console: local

                VRF: default
  default: group radius
  console: local

#show aaa authentication
                VRF: default
  default: group radius
  console: local

#show aaa groups vrf management
                VRF: management
radius
rad1

rad1

#show aaa groups vrf all
                VRF: management
radius
rad1

                VRF: default
radius
rad1

#show aaa groups
                VRF: default
radius
rad1


#show running-config radius
radius-server login host 100.0.0.1 vrf management key 7 wawyanb123 auth-port 600
00 acct-port 60000
radius-server login host Radius-Server-1 vrf management key 7 wawyanb123 auth-po
rt 60000 acct-port 60000
```

 © 2021 IP Infusion Inc. Proprietary

```
radius-server login host Radius-Server-1  key 7 wawyanb123 auth-port 60000 acct-
port 60000
radius-server login host 100.0.0.1 key 7 wawyanb123 auth-port 60000 acct-port 6
000

#show running-config aaa
aaa authentication login default vrf management group radius
aaa group server radius rad1 vrf management
    server Radius-Server-1 vrf management
    server 100.0.0.1 vrf management

aaa authentication login default group radius
aaa group server radius rad1
    server Radius-Server-1
    server 100.0.0.1

#show running-config aaa all
aaa authentication login default vrf management group radius
aaa authentication login console local
aaa accounting default vrf management local
no aaa authentication login default fallback error local vrf management
no aaa authentication login console fallback error local
no aaa authentication login error-enable vrf management
aaa local authentication attempts max-fail 3
aaa local authentication unlock-timeout 1200
aaa group server radius rad1 vrf management
    server Radius-Server-1 vrf management
    server 100.0.0.1 vrf management

aaa authentication login default group radius
aaa authentication login console local
aaa accounting default local
no aaa authentication login default fallback error local
no aaa authentication login console fallback error local
no aaa authentication login error-enable
aaa local authentication attempts max-fail 3
aaa local authentication unlock-timeout 1200
aaa group server radius rad1
    server Radius-Server-1
    server 100.0.0.1
```

RADIUS Server Accounting

You can configure accounting to measure the resources that another user consumes during access.

User

`#configure terminal`	Enter configure mode.
`(config)#radius-server login host 10.12.17.11 vrf management key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for management vrf. The radius server should be started with same port number.
`(config)#radius-server login host 10.12.17.11 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with port number for default vrf.The radius server should be started with same port number
`(config)#aaa accounting default vrf management group radius`	Enable accounting for radius server configured for vrf management
`(config)#aaa accounting default group radius`	Enable accounting for radius server configured for default vrf

Validation

```
#show aaa accounting vrf management
                VRF: management
  default: group radius

#show aaa accounting vrf all
                VRF: management
  default: group radius

                VRF: default
  default: group radius

#show aaa accounting
                VRF: default
  default: group radius
#
#show running-config aaa
aaa authentication login default vrf management group radius
aaa accounting default vrf management group radius
aaa group server radius rad1 vrf management
    server Radius-Server-1 vrf management
    server 100.0.0.1 vrf management

aaa authentication login default  group radius
aaa accounting default  group radius
aaa group server radius rad1
    server Radius-Server-1
    server 100.0.0.1
```

Sample Radius Clients.conf File

```
client 10.12.58.20 {
  secret    = testing123
  shortname = localhost
}
```


© 2021 IP Infusion Inc. Proprietary

```
client 192.168.1.2 {
  secret    = testing123
  shortname = localhost
}
client 10.12.37.196 {
  secret    = testing123
}
client 100.0.0.2 {
  secret    = testing123
  shortname = localhost
}

# IPv6 Client
#client ::1 {
#       secret          = testing123
#       shortname       = localhost
#}
#
# All IPv6 Site-local clients
#client fe80::/16 {
#       secret          = testing123
#       shortname       = localhost
```

Sample Radius Users Configuration File

```
#
#DEFAULT
#       Service-Type = Login-User,
#       Login-Service = Rlogin,
#       Login-IP-Host = shellbox.ispdomain.com

# #
# # Last default: shell on the local terminal server.
# #
# DEFAULT
#       Service-Type = Administrative-User

# On no match, the user is denied access.

selftest Cleartext-Password := "password"
testuser1 Cleartext-Password := "user1@101"
testuser2 Cleartext-Password := "user2@202"
testuser3 Cleartext-Password := "user3@303"
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 21 sFlow Configuration

Overview

This chapter provides the steps for configuring Sampled Flow (sFlow).

sFlow is the standard for monitoring high-speed switched and routed networks. The sFlow monitoring system consists of an sFlow Agent which is embedded in a switch or router and an sFlow Collector.

The sFlow agent samples packets as well as polling traffic statistics for the device it is monitoring. The packet sampling is performed by the switching/routing device at wire speed. The sFlow agent forwards the sampled traffic statistics in sFlow PDUs as well as sampled packets to an sFlow collector for analysis.

Note: sFlow egress sampling for multicast, broadcast, or unknown unicast packets is not supported.

The sFlow agent uses the following forms of sampling:

- Sampling packets: samples one packet out of a defined sampling rate. This sampling is done by hardware at wire speed.
- Sampling counters: polls interface statistics such as generic and Ethernet counters at a defined interval.

You must enable the sFlow feature and collector before enabling sFlow sampling on an interface.

You cannot globally enable sFlow sampling monitoring on all interfaces with a single command. Instead you must enable sFlow sampling on the required interfaces individually.

sFlow feature is supported on physical interface as well as LAG interface. Configuring sampling on a LAG interface will enable the same on all member ports part of that LAG interface.

Topology

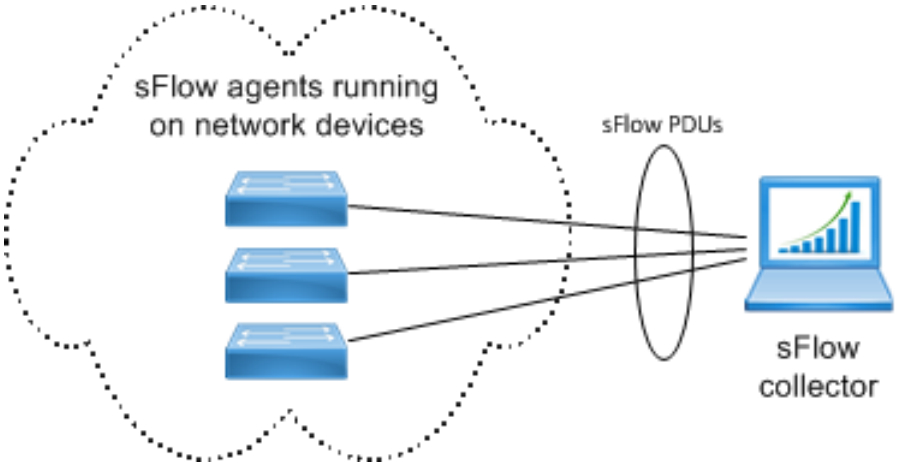


Figure 21-37: Basic sFlow topology

Configuration

sFlow Agent

`#configure terminal`	Enter configure mode.
`(config)#feature sflow`	Enable the sFlow feature.
`(config)#sflow collector 2.2.2.2 port 6343 receiver-time-out 0 max-datagram-size 200`	Configure the sFlow collector
`(config)#interface xe1`	Enter interface mode
`(config-if)#sflow poll-interval 5`	Set the counter poll Interval on the interface.
`(config-if)#sflow sampling-rate 1024 direction ingress max-header-size 200`	Set the sFlow sampling interval on the interface in ingress directions.
`(config-if)#sflow sampling-rate 1024 direction egress max-header-size 200`	Set the sFlow sampling interval on the interface in egress directions.
`(config-if)#sflow enable`	Start packet sampling on the interface
`(config-if)#end`	Exit interface and configure mode.

Validation

```
OcNOS#show sflow detail
sFlow Feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 10.10.26.132
Collector IP: 10.156.159.29    Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface  Packet-Sampling           Packet-Sampling            Counter-
Polling         Maximum Header
                  Rate                    Count                Interval
Count        Size(bytes)
         Ingress     Egress      Ingress     Egress      (sec)
Ingress     Egress
---------  ----------------------   ----------------------  ----------------
-------   --------------------
xe1/1           1024        1024       464564        414532          5
131     200          20
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 22 Show Tech Support Configurations

Overview

OcNOS maintains a collection of consolidated information about system configurations and statistics. This information is for debugging and diagnosing system issues, and can be uploaded to a remote server. You generate a file with this information via the `show techsupport` command.

Note: Output is not displayed on the terminal.

The default directory (`/var/log/`) is where the stored information is saved. The filename has the form: `tech_support_YYYY_MMM_DD_HH_MM_SS.tar.gz`. If a file name is specified, the information will be saved to `filename_YYYY_MMM_DD_HH_MM_SS_.tar.gz`. Date stamps are in the `YYYY_MM_DD` form, and time stamps are in the form `HH_MM_SS`.

The collected system data contains the following logs:

- Saved start-up configuration of the system.
- The `running-config`, and statistics for a specified module or all modules.
- The last 100 commands.
- Memory and CPU usage of the process.
- Process Id and process name.
- The user account running the process.

Tech Support Samples

`#show techsupport all`	Collects system configurations and statistics for all modules, and saves it in `tech_support_date_timestamp.tar.gz` in the `/var/log/` directory.
`#show techsupport all log-path /home/filename`	Collects system configurations and statistics for all modules, and saves it in `filename_date_timestamp.tar.gz` in the `/home/directory`.
`#show techsupport nsm`	Collects `nsm` protocol configurations and statistics, and saves it in `tech_support_date_timestamp.tar.gz` in the `/var/log/` directory.
`#show techsupport nsm log-path /home/filename`	Collects `nsm` protocol configurations and statistics, and saves it at `filename_date_timestamp.tar.gz` in the `/home/directory`.
`#show techsupport hostpd authd imi`	Collects `hostp`, `authd`, and `imi` protocol configurations and statistics and saves it at `tech_support_date_timestamp.tar.gz` in the `/var/log/` directory.
`#show techsupport hostpd authd imi log-path /home/filename`	Collects `hostp`, `authd`, `imi` protocol configurations and statistics, saves it as `filename_date_timestamp.tar.gz` in the `/home/` directory.

Validation Commands

You can display the status of a `show techsupport` command given earlier which indicates the protocol modules that have completed, are in progress, or have not executed. If the command has completed, it lists the last five generated tech support files with their path.

```
#show techsupport status

Tech Support Command Execution Is Complete
##Generated Tech Support File-list
/var/log/tech_support_18_Dec_2017_20_39_02.tar.gz
#
```

Note: the running `show techsupport` operation has not completed, reentering the `show techsupport` command is ignored.

© 2021 IP Infusion Inc. Proprietary

CHAPTER 23 Simple Network Management Protocol

Overview

SNMP provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- An SNMP manager: The system used to control and monitor the activities of network devices. This is sometimes called a Network Management System (NMS).
- An SNMP agent: The component within a managed device that maintains the data for the device and reports these data SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables which describe the system configuration. These variables can be queried (and sometimes set) by SNMP managers.

In SNMP, administration groups are known as communities. SNMP communities consist of one agent and one or more SNMP managers. You can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The security levels are:

- noAuthNoPriv: No authentication or encryption
- authNoPriv: Authentication but no encryption
- authPriv: Both authentication and encryption

SNMP is defined in RFCs 3411-3418.

Topology

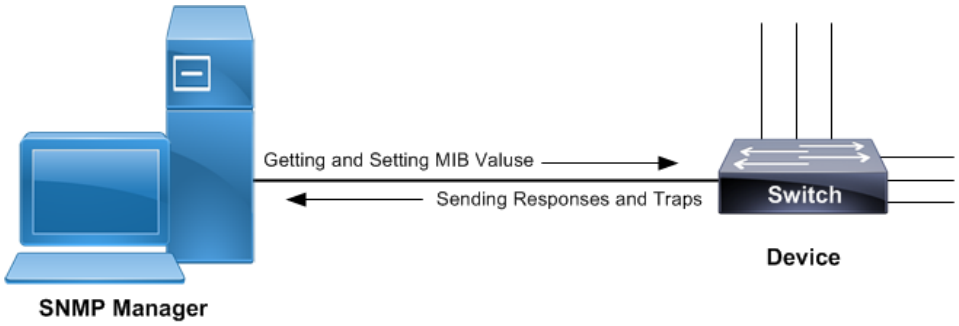


Figure 23-38: SNMP sample topology

Standard SNMP Configurations

`#configure terminal`	Enter configure mode.
`(config)#snmp-server view all .1 included vrf management`	Creates SNMP view labeled as “all” for OID-Tree as “.1” for vrf management.
`(config)#snmp-server community test group network-operator vrf management`	Set community string as “test” for group of users having “network-operator” privilege.
`(config)#snmp-server host 10.12.6.63 traps version 2c test udp-port 162 vrf management`	Specify host “10.12.6.63” to receive SNMP version 2 notifications at udp port number 162 with community string as “test”.
`(config)#snmp-server enable snmp vrf management`	Use this command to start the SNMP agent.
`(config)#exit`	Exit configure mode.

Validation

Use the below commands to verify the SNMP configuration:

```
#show running-config snmp
snmp-server view all .1 included vrf management
snmp-server community test group network-operator vrf management
snmp-server host 10.12.6.63 traps version 2c test udp-port 162 vrf management

#show snmp group
-------------------------------------------------------------------------------
community/user    group         version   Read-View   Write-view   Notify-view
-------------------------------------------------------------------------------
test          network-operator    2c/1       all        none           all

#show snmp host
-------------------------------------------------------------------------------
Host                Port   Version   Level          Type           SecName
-------------------------------------------------------------------------------
10.12.6.63          162    2c        noauth         trap           test
```

SNMP GET Command

```
# snmpget -v2c -c test 10.12.45.238
.1.3.6.1.2.1.6.13.1.2.10.12.45.238.22.10.12.6.63.52214

TCP-MIB::tcpConnLocalAddress.10.12.45.238.22.10.12.6.63.52214 = IpAddress:
10.12.45.238
```

SNMP WALK Command

SNMP WALK for particular OID

```
#snmpwalk -v2c -c test 10.12.45.238 .1.3.6.1.2.1.25.3.8.1.8
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.1 = STRING: 0-1-1,0:0:0.0
```


© 2021 IP Infusion Inc. Proprietary

```
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.4 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.5 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.6 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.10 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.12 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.13 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.14 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.15 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.16 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.17 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.18 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.19 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.20 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.21 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.22 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.23 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.24 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.25 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.26 = STRING: 0-1-1,0:0:0.0
```

Complete SNMP WALK

```
#snmpwalk -v2c -c test 10.12.45.238 .1
```

SNMP WALK Command

```
#snmpset -v2c -c test 10.12.45.102 1.3.6.1.2.1.10.246.1.2.1.30.1 u 123
iso.3.6.1.2.1.10.246.1.2.1.30.1 = Gauge32: 123
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 24 Software Monitoring and Reporting

Overview

OcNOS provides a mechanism (called “watchdogging”) to monitor all OcNOS modules and provides the following functions.

1. Periodic heart beat check.
2. Automatic restarts of a module upon a hung state or crash detection.
3. Upon hanging or crashing of a module, a crash report (including system states) is logged.
4. A proprietary SNMP trap is sent to the trap manager, if configured, after a fault is detected in a protocol module. Similarly a trap is sent when the module recovers.

By default, the software watchdog is enabled and the keep-alive time interval is 30 seconds. All OcNOS processes periodically send keep-alive messages to a monitoring module at the configured keep-alive time interval.

This functionality can be disabled for a particular module or all OcNOS modules by using CLI commands. In order to permanently disable software monitoring functionality, the user has to disable the watchdog feature. If, however, software watchdogging is disabled the monitoring module doesn’t take any action upon a hang or crash of any OcNOS module.

Configuration

`#configure terminal`	Enter configure mode.
`(config)#feature software-watchdog`	Enable software watchdog for all OcNOS modules — This is the default.
`(config)#no software-watchdog imi`	To disable software watchdog for only imi modules.
`(config)#software-watchdog keep-alive-time 100`	The keep-alive time interval in seconds. Default is 60 seconds and applies to all OcNOS modules.
`#show software-watchdog status`	Display the keep-alive time interval and list of OcNOS process names with watchdog status for each OcNOS modules.

Validation

```
#show software-watchdog status
Software Watchdog timeout in seconds : 100
Process name         Watchdog status
============         ===============
nsm                  Enabled
ripd                 Enabled
ospfd                Enabled
isisd                Enabled
hostpd               Enabled
```

```
ldpd                    Enabled
rsvpd                   Enabled
mribd                   Enabled
pimd                    Enabled
authd                   Enabled
mstpd                   Enabled
imi                     Disabled
onmd                    Enabled
HSL                     Enabled
oam                     Enabled
vlogd                   Enabled
vrrpd                   Enabled
ndd                     Enabled
ribd                    Enabled
bgpd                    Enabled
l2mribd                 Enabled
lagd                    Enabled
sflow                   Enabled
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 25 SSH Client Server Configuration

Overview

SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plain text, rendering them shusceptible to packet analysis.[2] The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet.SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user.

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols. SSH uses the client-server model

TCP port 22 is assigned for contacting SSH servers. This document covers the SSH server configuration to enable SSH service and key generation and SSH client configuration for remote login to server.

In-band Management over Default VRF

OcNOS supports SSH over the default and management VRFs via the in-band management interface and out-of-band management interfaces, respectively.

SSH can run on the default and management VRFs simultaneously. By default, it runs on the management VRF.

Topology



Figure 25-39: SSH sample topology

Basic Configuration

`#configure terminal`	Enter configure mode
`(config)#ssh login-attempts 2 vrf management`	Set the number of login attempts to 2
`(config)#exit`	Exit configuration mode

Validation

```
#show ssh server
ssh server enabled port: 22
authentication-retries 2
```

```
#show running-config ssh server
feature ssh vrf management
ssh login-attempts 2 vrf management
```

SSH Client Session

When the device acts as an SSH client, it supports both SSH IPv4 sessions to log into the remote machine.

`#ssh root@10.10.10.1 vrf management`	Log into remote machine using an IPv4 address

SSH Keys

Use the ssh key command to generate new RSA/DSA keys for the SSH server. By default, the system has RSA/DSA public/private key pair placed in /etc/ssh/. If you want to regenerate RSA keys, you must specify the force option.

Configuration

`#configure terminal`	Enter configure mode.
`(config)#ssh key rsa force vrf management`	Specify the `force` option to regenerate SSH RSA keys
`(config)#exit`	Exit configuration mode

Validation

```
#sh ssh key
****************RSA KEY*******************
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDMuVc0jpNgMyNzaqzIELX6LlsaK/
1q7pBixmwHAGDsZm/
dClTLb18AIB27W68YD8k0+Yw0LR0rHuPtNeSFMEsMaQxsaLkSi7yg86xSJaqgLQTyOUTS/
OC9hreXkJ73ay
n0yXa8+bre0oyJq1NWxAI9B1jEhfSSAipoDSp/
dmc93VJyV+3hgy1FMTAheyebQaUVeLBEMH7siRlSfyo7OHsBYSF6GzAmSuCm6PAelpHm/
3L4gChcnPL+0outQOifCSLdUOXEZhTFXrzC61l+14LGt8pR6YN+2uEnU6kq1i
aDLEffIWK4dWCp67JUIef1BTOvxRurpssuRdslhJQXDFaj
bitcount: 2048 fingerprint: a4:23:5d:8a:5a:54:8b:3e:0b:38:06:79:82:e9:83:48
************************************
****************DSA KEY*******************
ssh-dsa AAAAB3NzaC1kc3MAAACBALpY6MFhFPYI+VcAHzHppnwVnNXv9oR/
EGHUM50BBqdQE1Qi1mlt1rft4oa4tYR46P4gazKnnNfVE/
97FwEbCZaXaz9Wzfcfa3ALtsvGdyNQQk2BebYiRnmeWnS3wGV0M/D64bAiV0
2p/
LyF6D0ygMnZ3up3ttTN5QfHeyYQtwyzAAAAFQD+k6wQyr51IhXIQSsQD8by8qxjUwAAAIB0LxP3ljn
fzxEXyEkNNzlxCcJ7ZZkFYUmtDJxRZlDceuSf4QipMrQVrdrgdqZNhrUiDWM/
HaCMO9LdEQxfPh5TaIwPyccngn
VUS83Tx577ofBW6hellTey3B3/3I+FfiGKUXS/
mZSyf5FW3swwyZwMkF0mV0SRCYTprnFt5qx8awAAAIEAjDNqMkyxUvB6JBqfo7zbGqXjBQmJ+dE8fG
jI2znlgq4lhYcMZJVNwTiydDIgMVNFfKc1dAT3zr6qMZfGv56EbK
1qUu103K5CF44XfVkYNcHJV+/
fcfAJasGU8W6oSbU5Q08abyMsIGRYTurOMkRhvif6sxvieEpVnVK2/nPVVXA=
bitcount: 1024 fingerprint: d9:7a:80:e0:76:48:20:72:a6:5b:1c:67:da:91:9f:52
************************************
```


© 2021 IP Infusion Inc. Proprietary

Note: The newly created rsa/dsa key can be verified by logging into the device from a remote machine and checking whether the newly created key's fingerprint matches with the logging session fingerprint.

SSH Encryption Cipher

Specify an SSH cipher to encrypt an SSH session. By default, all the ciphers are supported for a new SSH client to connect to the SSH server.

SSH supports these encryption algorithms:

- Advanced Encryption Standard Counter:
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - aes128-cbc
- Advanced Encryption Standard Cipher Block Chaining:
  - aes192-cbc
  - aes256-cbc
- Triple Data Encryption Standard Cipher Block Chaining:
  - 3des-cbc

Configuration

`#configure terminal`	Enter configuration mode
`(config)#ssh server algorithm encryption aes128-ctr vrf management`	Set the SSH server encryption algorithm to AES 128 bit counter
`(config)#ssh server algorithm encryption aes128-cbc vrf management`	Set the SSH server encryption algorithm to AES 128 cipher block chaining
`(config)#exit`	Exit configuration mode

Validation

The new cipher encryption algorithm takes effect for a new incoming ssh client connection.

```
#show running-config ssh server
feature ssh vrf management
ssh server algorithm encryption aes128-ctr aes128-cbc vrf management
```

SSH Client Session

`#ssh cipher aes128-ctr root@1.1.1.1 vrf management`	Specify AES 128-bit counter encryption to establish an SSH connection to a remote machine using an IPv4 address

SSH Key Based Authentication

Enable OcNOS device SSH server to perform public key based SSH authentication, to enable machine to machine communication possible without requiring password. Public key based authentication increases the trust between two Linux servers for easy file synchronization or transfer. Public-key authentication with SSH is more secure than password authentication, as it provides much stronger identity checking through keys.

Topology



Figure 25-40: SSH Key based Authentication sample topology

Public Key Authentication Method

The server has the public key of the user stored; using this the server creates a random value, encrypts it with the public key and sends it to the user. If the user is who is supposed to be, he can decrypt the challenge using the private key and send it back to the server, server uses the public key again to decrypt received message to confirm the identity of the user. SSH is supported in In-band (default VRF) and Out of band (management VRF). Installed keys are stored at ~/.ssh/authorized_keys file.

SSH key based authentication steps:

1. Login to remote machine linux desktop (ssh client) and generate the key pair using the command “ssh-keygen”.
2. Create username in OCNOS switch device (ssh server).
3. Install the public key of remote Linux ssh client in OCNOS device.
4. Display the installed key in OCNOS device using “show running-config”.
5. Login from remote Linux ssh client to OCNOS device without providing password.

Useful commands on Remote Desktop Client

`# ssh-keygen`	To generate key pair on remote Linux machine (ssh client)
`# cd /bob/.ssh/`	To go to the location of saved key pair
`# cat id_rsa.pub`	Command to display the generated public key in remote Linux client

© 2021 IP Infusion Inc. Proprietary

Configuration commands in OCNOS

#configure terminal	Enter configure mode.
#feature ssh vrf management	Enable the SSH feature on vrf management. To enable in default vrf give the command “feature ssh”
# username fred	To create username with default role as network-user. To create user with different role specify role using command “username <username> role <role_name>
# username fred sshkey ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/VHVgU2Y0/ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV bob@localhost.localdomain	Install the public key of remote Linux client in ocnos device.
#exit	Exit configuration mode

Validation

The new cipher encryption algorithm takes effect for a new incoming ssh client connection.

```
#show running-config

<skipped other content>
feature ssh vrf management
username fred role network-user
username fred sshkey
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml
+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
<skipped other content>
OCNOS#show running-config ssh server
feature ssh vrf management
```

SSH Key based Client Session

#ssh fred@10.10.26.186	Specify user name and ip address to access the device. Supports IPv4 and IPv6.User should be able to access without password and through key based authentication

Restrictions

1. Key generation or installation are not supported for “root” user account in OcNOS device.
2. Third party SSH utilities cannot be used for key installation, rather OcNOS CLI interface is the only way to install public keys.

Sample Use case:

Step 1 :

```
Login to remote machine linux desktop (ssh client) and generate the key pair
using the command “ssh-keygen”
[bob@localhost ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/bob/.ssh/id_rsa):
/bob/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /bob/.ssh/id_rsa.
Your public key has been saved in /bob/.ssh/id_rsa.pub.
The key fingerprint is:
b2:d0:cc:d2:dd:db:3d:05:c1:33:fc:4a:df:8e:85:af bob@localhost.localdomain
The key's randomart image is:
+--[ RSA 2048]----+
|             o.  |
|              =. |
|              .+ |
|     = . .    ...|
|    o * S .  . +o|
|     o o   o .o.+|
|      .   . . o= |
|              ..o|
|              E. |
+-----------------+
[bob@localhost ~]# cd /bob/.ssh/
[bob@localhost .ssh]# cat id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0Sb
cU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlv
e3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml
+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
[bob@localhost .ssh]#
```

Step 2 :

```
Create username in OCNOS switch device (ssh server)
OCNOS(config)#username fred
Note : By default user role will be network-user
```

Step 3 :

```
Install the public key of remote Linux ssh client in OCNOS device.
OCNOS(config)#username fred sshkey
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0Sb
cU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlv
```


© 2021 IP Infusion Inc. Proprietary

```
e3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml
+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
```

Step 4 :

```
Display the installed key in OCNOS device using "show running-config"
OCNOS#show running-config
<skipped other content>
username fred role network-user
username fred sshkey
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0Sb
cU15axI/VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlv
e3lGbB1UUxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml
+QcJ9NER5O8rMS5D5NnTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV
bob@localhost.localdomain
<skipped other content>
```

Step 5 :

```
Login from remote Linux ssh client to OCNOS device without providing password
[bob@localhost .ssh]# ssh fred@10.10.26.186

OCNOS >en
OCNOS #
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 26 Syslog Configuration

Syslog is a standard for logging system messages. Logging helps for fault notification, network forensics, and security auditing.

OcNOS supports logging messages to a syslog server in addition to logging to a file or on the VTY terminal (ssh/telnet connection) and on the TTY serial console device. OcNOS messages can be logged to a local syslog server (the system on which OcNOS executes) into /var/log/messages by default as well as to one or multiple remote syslog servers (maximum of 8 remote syslog server is supported). Remote syslog servers can either be configured with IPv4 addresses or host names.

Support for In-band management over default VRF

OcNOS shall stream logs to remote syslog server through the interfaces associated with management VRF by default. Also OcNOS provides configurable option to stream the logs through interfaces associated with default VRF. At any point of time OcNOS shall stream logs through only one VRF.

Topology



Figure 26-41: Syslog sample topology

Enabling rsyslog

`#configure terminal`	Enter configure mode.
`config)#feature rsyslog vrf management`	Enable syslog feature on default or management VRF. By default this feature runs on the management VRF.
`config)#exit`	Exit configuration mode

Logging to a File

The below configurations enable debug logs for a particular protocol. In this case, OSPF is shown.

`#debug ospf all`	This enables the debugging on OSPF.
`#configure terminal`	Enter configure mode
`(config)#router ospf 1`	Enable OSPF process 1
`(config-router)#exit`	Exit router mode
`(config)#feature rsyslog`	Enable syslog feature on default or management VRF. By default this feature runs on the management VRF.
`(config)#logging level ospf 7`	This enable debug messages for OSPF module. This is configurable either if default of management VRF.

(config)#logging logfile ospf1 7	This creates the log file where the logs will be saved. The path of the file will be in the directory /log/ospf1. Log File size 4096-4194304 bytes.
(config)#exit	Exit configure mode

To verify this, do some OSPF configuration and view the messages in the log file or with the show logging logfile command.

Validation Commands

```
    #show logging logfile

    File logging : enabled  File Name : /log/ospf1  Size : 419430400  Severity :
    (7)
    2019 Jan 05 20:10:52.202 : OcNOS : OSPF : INFO : NSM Message Header
    2019 Jan 05 20:10:52.202 : OcNOS : OSPF : INFO :  VR ID: 0
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  VRF ID: 0
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  Message type:
    NSM_MSG_LINK_ADD
     (5)
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  Message length: 232
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  Message ID: 0x00000000
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO : NSM Interface
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  Interface index: 100001
    2019 Jan 05 20:10:52.203 : OcNOS : OSPF : INFO :  Name: po1
    2019 Jan 05 20:10:52.204 : OcNOS : OSPF : INFO :  Flags: 536875010
    2019 Jan 05 20:10:52.204 : OcNOS : OSPF : INFO :  Status: 0x00000804
    2019 Jan 05 20:10:52.204 : OcNOS : OSPF : INFO :  Metric: 1
    2019 Jan 05 20:10:52.207 : OcNOS : OSPF : INFO :  MTU: 1500
    2019 Jan 05 20:10:52.207 : OcNOS : OSPF : INFO :  Type: L3
    2019 Jan 05 20:10:52.207 : OcNOS : OSPF : INFO :  HW type: 9
    2019 Jan 05 20:10:52.208 : OcNOS : OSPF : INFO :  HW len: 6
    2019 Jan 05 20:10:52.209 : OcNOS : OSPF : INFO :  HW address: ecf4.bb5c.a2b0
    2019 Jan 05 20:10:52.210 : OcNOS : OSPF : INFO :  Bandwidth: 0.000000
    2019 Jan 05 20:10:52.211 : OcNOS : OSPF : INFO :  Interface lacp key flag 0
    2019 Jan 05 20:10:52.212 : OcNOS : OSPF : INFO :  Interface lacp aggregator
    upda
    te flag 0

#show logging level

    Facility        Default Severity        Current Session Severity
    nsm                     3                       3
    ripd                    3                       3
    ospfd                   3                       7
    ospf6d                  3                       3
    isisd                   3                       3
    hostpd                  3                       3
    ldpd                    2                       2
    rsvpd                   2                       2
    mribd                   2                       2
    pimd                    2                       2
    authd                   2                       2
    mstpd                   2                       2
    imi                     2                       2
    onmd                    2                       2
```


© 2021 IP Infusion Inc. Proprietary

```
    oamd                    2                       2
    vlogd                   2                       2
    vrrpd                   2                       2
    ribd                    2                       2
    bgpd                    3                       3
    l2mribd                 2                       2
    lagd                    2                       2
    sflow                   2                       2
    pservd                  2                       2
```

Logging to the Console

`#configure terminal`	Enter configure mode.
`(config)#logging level ospf 7`	This enable debug messages for OSFP module.
`(config)#logging console 7`	This enables the console logs.
`(config)#debug ospf`	This enables the debugging on OSPF configurations.
`(config)#router ospf`	Enabling ospf for process 1.
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit configure mode.

To verify this, do some OSPF configuration and view the messages in the console.

Validation Commands

```
#show logging console
    Console logging     : enabled Severity: (debugging)

#show logging level

    Facility        Default Severity        Current Session Severity
    nsm                     3                       3
    ripd                    3                       3
    ospfd                   3                       7
    ospf6d                  3                       3
    isisd                   3                       3
    hostpd                  3                       3
    ldpd                    2                       2
    rsvpd                   2                       2
    mribd                   2                       2
    pimd                    2                       2
    authd                   2                       2
    mstpd                   2                       2
    imi                     2                       2
    onmd                    2                       2
    oamd                    2                       2
    vlogd                   2                       2
    vrrpd                   2                       2
    ribd                    2                       2
    bgpd                    3                       3
    l2mribd                 2                       2
    lagd                    2                       2
```

```
    sflow                   2                           2
    pservd                  2                           2
```

Logging to Remote Server

`#configure terminal`	Enter configure mode.
`(config)#logging level bgp 7`	This enable debug messages for BGP module.
`(config)#logging remote server 10.16.2.1 vrf management`	Redirects the log messages to the remote server configured.
`(config)#debug bgp`	This enables the debugging on BGP configurations.
`(config)#router bgp 1`	Enabling BGP process 1.
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit configure mode.

Validation Commands

```
#show logging server
      Remote Servers:
                  10.16.2.1
                  severity: (debugging)
                  facility: local7
                  VRF: management

    #show logging level

    Facility        Default Severity        Current Session Severity
    nsm                     3                           3
    ripd                    3                           3
    ospfd                   3                           3
    ospf6d                  3                           3
    isisd                   3                           3
    hostpd                  3                           3
    ldpd                    2                           2
    rsvpd                   2                           2
    mribd                   2                           2
    pimd                    2                           2
    authd                   2                           2
    mstpd                   2                           2
    imi                     2                           2
    onmd                    2                           2
    oamd                    2                           2
    vlogd                   2                           2
    vrrpd                   2                           2
    ribd                    2                           2
    bgpd                    3                           7
    l2mribd                 2                           2
    lagd                    2                           2
    sflow                   2                           2
    pservd                  2                           2
```


© 2021 IP Infusion Inc. Proprietary

Configuration

Note: The configuration to support multiple logging servers is listed below. Maximum 4 remote syslog server is supported.

`#configure terminal`	Enter Configure mode.
`(config)#hostname OcNOS`	Configuring the hostname of the device
`(config)#feature rsyslog vrf management`	Enable feature on default or management VRF. By default this feature runs on the management VRF.
`(config)#logging level all 7`	Enables debug messages for all modules.
`(config)# logging remote server 10.12.17.10 5 vrf management`	Redirects the log messages to the server configured. (Configuring 1 logging server).Configuring with log severity level as 5.By default severity level 7 is considered if no specific levels configured.
`(config)# logging remote server 10.12.17.16 5 vrf management`	Redirects the log messages to the server configured. (Configuring 2 logging server). Configuring with log severity level as 5. By default severity level 7 is considered if no specific levels configured.
`(config)# logging remote server 10.12.17.11 7 vrf management`	Redirects the log messages to the server configured. (Configuring 3 logging server). Configuring with log severity level as 7. By default severity level 7 is considered if no specific levels configured.
`(config)# logging remote server 10.12.28.22 7 vrf management`	Redirects the log messages to the server configured. (Configuring 4 logging server). Configuring with log severity level as 7. By default severity level 7 is considered if no specific levels configured.
`(config)#exit`	Exit configure mode.

Validation Commands

```
OcNOS # show running-config logging
<snippet of show running-config logging output ...>
feature rsyslog vrf management
logging remote server 10.12.17.10 5 vrf management
logging remote server 10.12.17.16 5 vrf management
logging remote server 10.12.17.11 7 vrf management
logging remote server 10.12.28.22 7 vrf management

OcNOS # show logging server
  Remote Servers:
               10.12.17.10
               severity: Operator (informational)
               facility: local7
               VRF : management
               10.12.17.16
               severity: Operator (informational)
               facility: local7
               VRF : management
               10.12.17.11
               severity: Operator (debug-detailed)
```

```
facility: local7
VRF : management
10.12.28.22
severity: Operator (debug-detailed)
facility: local7
VRF : management
```

Remote machine Syslog Configuration:

Provided below are the changes required for rsyslog configuration on a debian system. Please refer to respective operating system official sites for more information

```
cat /etc/rsyslog.conf
$ModLoad imuxsock.so    # provides support for local system logging (e.g. via
logger command)
$ModLoad imklog.so      # provides kernel logging support (previously done by
rklogd)
$ModLoad immark.so    # provides --MARK-- message capability
$ModLoad imudp.so
$UDPServerRun 514
$ModLoad imtcp.so
$InputTCPServerRun 514
# Logs will be  placed in  separate folders based on hostnames and process
modules  in the provided path
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~

$template precise,"%msg%\n"
*.* /var/log/messages
auth,authpriv.*                 /var/log/auth.log
```

Save the changes and restart the rsyslog services to bring the changes in effect.

Monitoring Logging Server:

```
Provided below are the sample outputs collected from one of the remote logging
server.
root@localhost:~# cd /var/log/
```

Different folders I get created based on hostnames inthe defined location in rsyslog.conf

```
root@localhost:/var/log# ls -lt
drwx------ 2 root        root     4096 Nov 18 03:02 Leaf1
drwx------ 2 root        root     4096 Nov 15 07:24 10.12.56.112-leaf5
drwx------ 2 root        root     4096 Nov 15 05:40 10.12.56.109-leaf2
drwx------ 2 root        root     4096 Nov 15 01:26 Bingo1
drwx------ 2 root        root     4096 Nov 14 06:07 Leaf2
drwx------ 2 root        root     4096 Nov 11 04:57 R1-LEAF1
drwx------ 2 root        root     4096 Nov  8 06:46 leaf2
drwx------ 2 root        root     4096 Nov  8 03:38 R7-LEAF4
drwx------ 2 root        root     4096 Nov  8 01:30 LEAF1
drwx------ 2 root        root     4096 Nov  8 01:18 leaf3
drwx------ 2 root        root     4096 Nov  7 07:56 OcNOS
drwx------ 2 root        root     4096 Nov  6 23:58 mgmt-sw-3k
drwx------ 2 root        root     4096 Nov  4 21:51 R5-LEAF3
```


© 2021 IP Infusion Inc. Proprietary

```
Check under OcNOS folder
root@localhost:/var/log/OcNOS# ls –ltr
```

Different log files get created based on process name under folder based on hostname.

```
-rw-r--r-- 1 root root      444 Oct 25 02:20 PSERV.log
-rw-r--r-- 1 root root      328 Oct 30 05:05 ONMD.log
-rw-r--r-- 1 root root      174 Oct 30 05:37 usermod.log
-rw-r--r-- 1 root root      498 Oct 30 07:55 SFLOW.log
-rw-r--r-- 1 root root      486 Oct 30 07:55 RIP.log
-rw-r--r-- 1 root root      486 Oct 30 07:55 LAG.log
-rw-r--r-- 1 root root      492 Oct 30 07:55 VRRP.log
-rw-r--r-- 1 root root      486 Oct 30 07:55 PIM.log
-rw-r--r-- 1 root root      504 Oct 30 07:55 OSPFv3.log
-rw-r--r-- 1 root root      492 Oct 30 07:55 OSPF.log
-rw-r--r-- 1 root root      498 Oct 30 07:55 IS-IS.log
-rw-r--r-- 1 root root      504 Oct 30 07:55 802.1X.log
-rw-r--r-- 1 root root      492 Oct 30 07:56 MSTP.log
-rw-r--r-- 1 root root      483 Oct 30 07:56 HSL.log
-rw-r--r-- 1 root root      486 Oct 30 07:56 RIB.log
-rw-r--r-- 1 root root      492 Oct 30 07:56 MRIB.log
-rw-r--r-- 1 root root     8709 Nov  2 11:22 OAM.log
-rw-r--r-- 1 root root    17959 Nov  2 11:23 NSM.log
-rw-r--r-- 1 root root    12178 Nov  2 11:23 BGP.log
-rw-r--r-- 1 root root    74488 Nov  3 07:41 CMM.log
-rw-r--r-- 1 root root     4128 Nov  3 08:17 login.log
-rw-r--r-- 1 root root     5265 Nov  3 08:17 HOSTP.log
-rw-r--r-- 1 root root    21982 Nov  3 08:17 CML.log
-rw-r--r-- 1 root root 28094411 Nov  3 08:17 CMLSH.log
-rw-r--r-- 1 root root   278619 Nov  3 08:19 sshd.log
-rw-r--r-- 1 root root   695277 Nov  3 08:20 CRON.log
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 27 Telnet Configuration

Overview

Telnet is a TCP/IP protocol used on the Internet and local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection. The Telnet program runs, connects it to a server on the network. A user can then enter commands through the Telnet program and they will be executed as if the user were entering them directly on the server console.Telnet enables users to control the server and communicate with other servers on the network. The default port number for Telnet protocol is 23.Telnet offers users the capability of running programs remotely and facilitates remote administration.

Support for In-band Management Over Default VRF

OcNOS supports Telnet over the default and management VRFs via in-band management interface and OOB management interface, respectively.

By default, Telnet runs on the management VRF.

Topology



Figure 27-42: Telnet topology

Enable and Disable the Telnet Server

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable Telnet feature
`(config)#feature telnet vrf management`	Enable Telnet feature
`(config)#exit`	Exit configure mode

Configure the Telnet Server Port

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable Telnet feature
`(config)#telnet server port 6112 vrf management`	Set Telnet port to 61112

(config)#feature telnet vrf management	Enable Telnet feature
(config)#exit	Exit configure mode

Telnet Client Session

#telnet 10.10.10.1 vrf management	Log into remote machine using IPv4 address

Validation Commands

```
#show telnet server
telnet server enabled port: 6112

#show running-config telnet server
feature telnet
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 28 TACACS Client Configuration

Overview

Terminal Access Controller Access Control System (TACACS) is a remote authentication protocol that is used to communicate with an authentication server. With TACACS, a network device communicates to an authentication server to determine whether a particular user should be allowed access to the device. TACACS+ listens at port 49.

TACACS Server Authentication

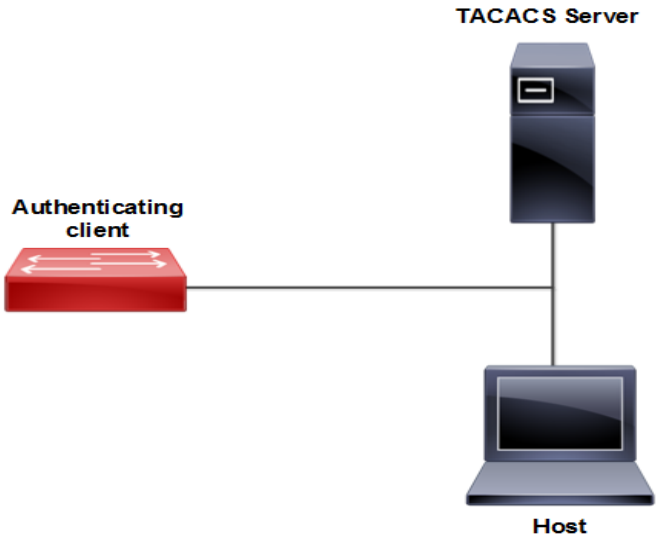


Figure 28-43: TACACS Server Host Configuration

Authenticating Device

`#configure terminal`	Enter configure mode.
`(config)#feature tacacs+ vrf management`	Enable the feature TACACS+ for management vrf
`(config)#feature tacacs+`	Enable the feature TACACS+. for default vrf
`(config)#(config)#tacacs-server login key 0 testing101 vrf management`	Specify the global key for tacacs servers that are not configured with their respective keys for management vrf This key should match the one present in the config file of tacacs server
`(config)#tacacs-server login key 0 testing101`	Specify the global key for tacacs servers that are not configured with their respective keys for default vrf This key should match the one present in the config file of tacacs server
`(config)#tacacs-server login host 10.16.19.2 vrf management seq-num 1 key 0 testing123`	Specify the tacacs server ipv4 address to be configured with shared key. The same key should be present on the server config file
`(config)#tacacs-server login host 10.16.19.2 seq-num 2 key 0 testing123`	Specify the tacacs server ipv4 address to be configured with shared local key for default vrf The same key should be present on the server config file.

© 2021 IP Infusion Inc. Proprietary

(config)#tacacs-server login host 10.12.30.86 vrf management seq-num 4 port 1045	Specify the tacacs server ipv4 address to be configured with the sequence and port number.The tacacs server should be started with same port number
config)#tacacs-server login host 10.12.30.86 seq-num 2 port 1045	Specify the tacacs server ipv4 address to be configured with the sequence and port number for default vrf. The tacacs server should be started with same port number
(config)#tacacs-server login host 10.12.17.11 vrf management seq-num 8 key 7 65535 port 65535	Specify the tacacs server ipv4 address to be configured with the sequence, key and port number for management vrf. The tacacs server should be started with same port number.
(config)#tacacs-server login host 10.12.17.11 seq-num 8 key 7 65535 port 65535	Specify the tacacs server ipv4 address to be configured with the sequence, key and port number for default vrf. The tacacs server should be started with same port number.
(config)#tacacs-server login host Tacacs-Server-1 vrf management seq-num 7 key 7 65535 port 65535	Specify the tacacs server configured with host-name sequence number key and port number for management vrf. The tacacs server should be started with same port number
(config)#tacacs-server login host Tacacs-Server-1 seq-num 7 key 7 65535 port 65535	Specify the tacacs server configured with host-name sequence number key and port number for default vrf. The tacacs server should be started with same port number
(config)#aaa authentication login default vrf management group tacacs+	Enable authentication for TACACS+ server configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group tacacs+	Enable authentication for TACACS+ server configured for default vrf. Authorization is also enabled by default.
(config)#aaa authentication login default vrf management group tacacs+ local	Enable authentication for TACACS+ and fall-back to local configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group tacacs+ local none	Enable authentication for TACACS+ fall-back to local followed by fall-back to none configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group tacacs+ none	Enable authentication for TACACS+ fall-back to none configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group tacacs+ none	Enable authentication for TACACS+ fall-back to none , configured for default vrf. Authorization is also enabled by default
(config)#aaa group server tacacs+ G1 vrf management	Create aaa group G1 for management vrf
(config-tacacs)#server 10.12.30.86 vrf management	Make the tacacs-server 10.12.30.86 a part of this group G1 for default vrf
(config-tacacs)#server Tacacs-Server-1	Make the tacacs-server Tacacs-Server-1 a part of this group G1 for management vrf
(config-tacas)#exit	Exit the tacacs-config
(config)#aaa group server tacacs+ G1	Create aaa group G1 for default vrf
(config-tacacs)server 10.12.30.86	Make the tacacs-server 10.12.30.86 a part of this group G1 for default vrf
(config-tacacs)#server Tacacs-Server-1	Make the tacacs-server Tacacs-Server-1 a part of this group G1 for management vrf
(config-tacacs)#exit	Exit the tacacs-config mode
(config)#aaa authentication login default vrf management group G1	Authenticate the tacacs+ group G1 with aaa authentication for management vrf
(config)#aaa authentication login default group G1	Authenticate the tacacs+ group G1 with aaa authentication for default vrf

© 2021 IP Infusion Inc. Proprietary

Users are mapped as shown as shown in Table 28-1:

Table 28-1: Role/privilege level mapping

Role	Privilege level
Network administrator	15
Network engineer	14
Network operator	1 to 13
Network user	0 or any other values (>15 or negative values or any character)

Validation

```
Leaf1#show tacacs-server vrf management
        VRF: management
total number of servers:4

Tacacs+ Server                  : 10.16.19.2/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 10.12.30.86/1045
           Sequence Number      : 2
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : Tacacs-Server-1/65535
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 10.12.17.11/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Leaf1#show tacacs-server
        VRF: default
total number of servers:4

Tacacs+ Server                  : 10.16.19.2/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
```

```
     Last Successful authentication:

    Tacacs+ Server                  : 10.12.30.86/1045
               Sequence Number      : 2
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    Tacacs+ Server                  : Tacacs-Server-1/65535
               Sequence Number      : 7
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    Tacacs+ Server                  : 10.12.17.11/65535
               Sequence Number      : 8
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    (*) indicates last active.

#show tacacs-server vrf all
             VRF: management
    total number of servers:2
    Tacacs+ Server                  : Tacacs-Server-1/65535(*)
               Sequence Number      : 7
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 1
       Failed Connect Attempts      : 0
     Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                  : 10.12.17.11/65535
               Sequence Number      : 8
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:


             VRF: default
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/2222
               Sequence Number      : 7
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    Tacacs+ Server                  : 100.0.0.1/2222
               Sequence Number      : 8
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
```


© 2021 IP Infusion Inc. Proprietary

```
       Failed Connect Attempts     : 0
     Last Successful authentication:


    (*) indicates last active.
#


    #
#show tacacs-server
            VRF: default
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/2222
               Sequence Number      : 7
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    Tacacs+ Server                  : 100.0.0.1/2222
               Sequence Number      : 8
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    (*) indicates last active.

#show tacacs-server vrf management groups G1
            VRF: management

            group G1:
                    server Tacacs-Server-1:
                    seq-num 7
                    port is 65535
                    key is ********

                    server 10.12.17.11:
                    seq-num 8
                    port is 65535
                    key is ********

#show tacacs-server vrf all groups G1
            VRF: management

            group G1:
                    server Tacacs-Server-1:
                    seq-num 7
                    port is 65535
                    key is ********

                    server 10.12.17.11:
                    seq-num 8
                    port is 65535
                    key is ********
```

```
            VRF: default

            group G1:
                    server Tacacs-Server-1:
                    seq-num 7
                    port is 2222
                    key is ********

                    server 100.0.0.1:
                    seq-num 8
                    port is 2222
                    key is ********



#
#show tacacs-server groups G1
            VRF: default
    group G1:
                    server Tacacs-Server-1:
                    seq-num 7
                    port is 2222
                    key is ********

                    server 100.0.0.1:
                    seq-num 8
                    port is 2222
                    key is ********
    #show tacacs vrf management
            VRF: management
    total number of servers:2

    Tacacs+ Server                 : Tacacs-Server-1/65535(*)
               Sequence Number     : 7
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 1
       Failed Connect Attempts     : 0
     Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                 : 10.12.17.11/65535
               Sequence Number     : 8
          Failed Auth Attempts     : 0
         Success Auth Attempts     : 0
       Failed Connect Attempts     : 0
     Last Successful authentication:

    (*) indicates last active.



    #show tacacs vrf all
            VRF: management
    total number of servers:2
```


© 2021 IP Infusion Inc. Proprietary

```
Tacacs+ Server                  : Tacacs-Server-1/65535(*)
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 1
   Failed Connect Attempts      : 0
 Last Successful authentication: 2018 October 30, 10:10:22

Tacacs+ Server                  : 10.12.17.11/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:


        VRF: default
total number of servers:2

Tacacs+ Server                  : Tacacs-Server-1/2222(*)
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 1
   Failed Connect Attempts      : 0
 Last Successful authentication: 2018 October 30, 10:32:52

Tacacs+ Server                  : 100.0.0.1/2222
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:


(*) indicates last active.
#

#show tacacs
        VRF: default
total number of servers:2

Tacacs+ Server                  : Tacacs-Server-1/2222(*)
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 1
   Failed Connect Attempts      : 0
 Last Successful authentication: 2018 October 30, 10:32:52

Tacacs+ Server                  : 100.0.0.1/2222
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

(*) indicates last active.

#show tacacs vrf management
```

```
            VRF: management
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/65535(*)
               Sequence Number      : 7
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 1
       Failed Connect Attempts      : 0
     Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                  : 10.12.17.11/65535
               Sequence Number      : 8
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    (*) indicates last active.

#show tacacs vrf all
            VRF: management
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/65535(*)
               Sequence Number      : 7
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 1
       Failed Connect Attempts      : 0
     Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                  : 10.12.17.11/65535
               Sequence Number      : 8
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:


            VRF: default
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/2222(*)
               Sequence Number      : 7
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 1
       Failed Connect Attempts      : 0
     Last Successful authentication: 2018 October 30, 10:32:52

    Tacacs+ Server                  : 100.0.0.1/2222
               Sequence Number      : 8
          Failed Auth Attempts      : 0
         Success Auth Attempts      : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:


    (*) indicates last active.
```


© 2021 IP Infusion Inc. Proprietary

```
#

#show tacacs
            VRF: default
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/2222(*)
               Sequence Number      : 7
            Failed Auth Attempts    : 0
           Success Auth Attempts    : 1
       Failed Connect Attempts      : 0
     Last Successful authentication: 2018 October 30, 10:32:52

    Tacacs+ Server                  : 100.0.0.1/2222
               Sequence Number      : 8
            Failed Auth Attempts    : 0
           Success Auth Attempts    : 0
       Failed Connect Attempts      : 0
     Last Successful authentication:

    (*) indicates last active.

#show aaa authentication vrf management
                     VRF: management
      default: group G1
      console: local

#show aaa authentication vrf all
                     VRF: management
      default: group G1
      console: local

                     VRF: default
      default: group tacacs+
      console: local

#show aaa authentication
                     VRF: default
      default: group tacacs+
      console: local
#

# show aaa groups vrf management
                     VRF: management
    radius
    tacacs+
    G1

#
    # show aaa groups vrf all
                     VRF: management
    radius
    tacacs+
    G1
```

```
                    VRF: default
    radius
    tacacs+
    G1


#show aaa groups
                    VRF: default
    radius
    tacacs+
    G1

#show running-config tacacs+
    feature tacacs+ vrf management
    tacacs-server login host Tacacs-Server-1 vrf management seq-num 7 key 7 65535
    po
    rt 65535
    tacacs-server login host 10.12.17.11 vrf management seq-num 8 key 7 65535 port
    6
    5535

    feature tacacs+
    tacacs-server login host Tacacs-Server-1 seq-num 7 key 7 65535 port 2222
    tacacs-server login host 100.0.0.1 seq-num 8 key 7 65535 port 2222

#show running-config aaa
    aaa authentication login default vrf management group G1
    aaa group server tacacs+ G1 vrf management
        server Tacacs-Server-1 vrf management
        server 10.12.17.11 vrf management

    aaa authentication login default group tacacs+
    aaa group server tacacs+ G1
        server Tacacs-Server-1
        server 100.0.0.1

#show running-config aaa all
    aaa authentication login default vrf management group G1
    aaa authentication login console local
    aaa accounting default vrf management local
    no aaa authentication login default fallback error local vrf management
    no aaa authentication login console fallback error local
    no aaa authentication login error-enable vrf management
    aaa local authentication attempts max-fail 3
    aaa local authentication unlock-timeout 1200
    aaa group server tacacs+ G1 vrf management
        server Tacacs-Server-1 vrf management
        server 10.12.17.11 vrf management

    aaa authentication login default group tacacs+
    aaa authentication login console local
    aaa accounting default local
    no aaa authentication login default fallback error local
    no aaa authentication login console fallback error local
    no aaa authentication login error-enable
    aaa local authentication attempts max-fail 3
```


© 2021 IP Infusion Inc. Proprietary

```
aaa local authentication unlock-timeout 1200
aaa group server tacacs+ G1
    server Tacacs-Server-1
    server 100.0.0.1
```

TACACS Server Accounting

After authentication, the user can configure accounting to measure the resources that the user consumes during access.

Authenticating Device

`#configure terminal`	Enter configure mode.
`(config)#feature tacacs+ vrf management`	Enable the feature TACACS+ for vrf management
`(config)#feature tacacs+`	Enable the feature TACACS+ for default vrf
`(config)#tacacs-server login host 10.16.19.2 vrf management seq-num 1 key 0 testing123`	Specify the TACACS server IPv4 address to be configured with shared key for vrf management. The same key should be present in the server configuration file.
`(config)#tacacs-server login host 10.16.19.2 key testing123`	Specify the TACACS server IPv4 address to be configured with shared key default vrf. The same key should be present in the server configuration file.
`(config)#aaa accounting default vrf management group tacacs+`	Enable accounting for TACACS server configured for vrf management.
`(config)#aaa accounting default group tacacs+`	Enable accounting for TACACS server configured for default vrf
`(config)#exit`	Exit configure mode
`#clear tacacs-server counters vrf management`	Clear tacacs server counters for management vrf
`#clear tacacs-server counters vrf all`	Clear tacacs server counters for management and default vrf
`#clear tacacs-server counters`	Clear tacacs server counters for default vrf

To verify the TACACS accounting process, connect using SSH or Telnet from the host to the client with the user created and provided TACACS server password, and check whether the client validates the user with corresponding username and password.

Validation Commands

show tacacs-server, show aaa accounting, show aaa accounting

```
#show aaa accounting vrf management
                    VRF: management
          default: group tacacs+
#

#show aaa accounting vrf all
                    VRF: management
          default: group tacacs+
```

```
                    VRF: default
          default: group tacacs+

#show aaa accounting
                    VRF: default
          default: group tacacs+
          #

#show running-config aaa
    aaa authentication login default vrf management group G1
    aaa accounting default vrf management group tacacs+
    aaa group server tacacs+ G1 vrf management
        server Tacacs-Server-1 vrf management
        server 10.12.17.11 vrf management

    aaa authentication login default group tacacs+
    aaa accounting default group tacacs+
    aaa group server tacacs+ G1
        server Tacacs-Server-1
        server 100.0.0.1
```

Sample TACACS Config File Contents

```
#tacacs configuration file
#set the key

    key = "testing123"
    accounting file = /var/log/tac_acc.log

    user = test1 {
            default service = permit
            login = cleartext "12345"
    }

    group = netadmin {
            service = ppp protocol = ip {
            priv-lvl = 1
            }
    }

    user = test2 {
            default service = permit
            login = cleartext "12345"
            member = netadmin
    }

    user = test3 {
            default service = permit
            login = cleartext "12345"
            service = ppp protocol = ip {
            priv-lvl = 15
    }
    }
```


© 2021 IP Infusion Inc. Proprietary

TACACS Server Authorization

Authorization is realized by mapping the authenticated users to one of the existing predefined roles as shown in Table 28-1.

The privilege information from the TACACS+ server is retrieved for the authenticated users and is mapped onto one of the roles as shown in Table 28-1.

Each authenticated user is mapped to one of the pre-defined privilege level.

Users with priv-level <=0 and priv-level > 15 are treated as read-only user mapped onto the pre-defined network-user role.

There is no command to enable authorization. Authorization functionality is enabled by default when remote authentication is enabled with TACACS+.

Authorization is “auto-enabled”. After successful authentication, a user can enter into privilege exec mode, irrespective of its privilege level and such user is not prompted with enable mode password, if configured. However based on their role, commands are rejected if not allowed to perform certain operations.

Example

A network-user has read-only access and can only execute show commands. A network-user cannot enter configuration mode. An error message is displayed upon executing any command which is not allowed.

```
#write
% Access restricted for user %
#configure terminal
% Access restricted for user %
```

The following attribute value pair in TACACS+ server is used to fetch user privilege information.

```
service = ppp protocol = ip {
        priv-lvl = <0…15>
}
```

Sample TACACS+ Configuration File

```
#tacacs configuration file from “tac_plus version F4.0.3.alpha “
#set the key

key = "testing123"
accounting file = /var/log/tac_acc.log

#Read only user “test1”, without any priv-lvl, mapped to role “network-user”
user = test1 {
default service = permit
login = cleartext "12345"
}

#We can create a group of users mapped to a privilege
group = netadmin {
service = ppp protocol = ip {
priv-lvl = 15
}
```

```
}

#User “test2” with highest priv-lvl=15, mapped to role “network-admin”
user = test2 {
default service = permit
login = cleartext "12345"
member = netadmin
}

#User “test3” with priv-lvl= 1…13, mapped to role “network-operator”
user = test3 {
default service = permit
login = cleartext "12345"
service = ppp protocol = ip {
priv-lvl = 10
}
}
#User “test4” with priv-lvl=14, mapped to role “network-engineer” user = test4 {
default service = permit
login = cleartext "12345"
service = ppp protocol = ip {
priv-lvl = 14
}
}
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 29 Traffic Mirroring Configuration

This chapter contains a sample local and remote switched port analyzer feature configuration.

SPAN Overview

Switched Port Analyzer (SPAN) refers to selecting network traffic for analysis by a network analyzer. SPAN feature is introduced on switches as the switch forwards traffic that is destined for a MAC address directly to the corresponding port leaving no scope to analyze the traffic.

SPAN monitors the traffic on source port and sends a copy of the traffic to a destination port. The network analyzer, which is attached to the destination port, analyzes the received traffic. Source port can be a single port or multiple ports. A replication of the packets is sent to the destination port for analysis

SPAN is originally referred to port mirroring or port monitoring where all the network traffic on the source port is mirrored to destination port. Port mirroring has three subdivisions.

- Ingress mirroring: Traffic received on the source port will be monitored
- Egress mirroring: Traffic transmitted from the source port will be monitored
- Ingress and egress mirroring: Both received and transmitted traffic on the source port will be monitored.

With enhancements to SPAN, mirroring can be classified into three categories.

Port Mirroring

In port mirroring, source will be a port which could be a physical interface or a port channel. All the traffic on the source port will be mirrored to destination port. Either traffic received on the source port or traffic transmitted from the source port or both can be monitored.

Note: If monitor session configured with two or more source interfaces in the Egress direction (tx) then the destination mirror port will receive only one copy of the non-unicast packet.

Also, the mirrored packet would be having default TPID of the mirror destination port i.e. 0x8100.

VLAN Mirroring

In VLAN mirroring, the source is a VLAN identifier and the traffic received on all ports with the VLAN identifier matching source VLAN identifier are mirrored to destination port.

Rule Based Mirroring

In rule based mirroring, there is a set of matching criteria for the ingress traffic such as matching destination MAC address, matching frame type, and so on. The traffic matching the rules is mirrored to the destination port

Topology

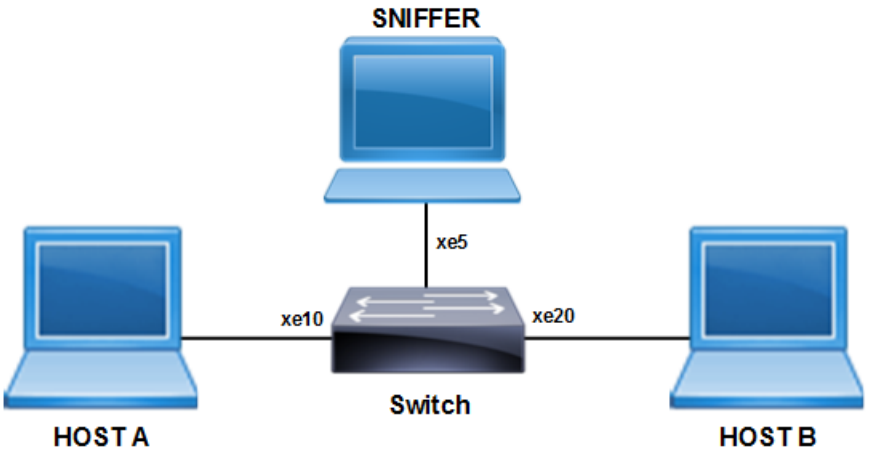


Figure 29-44: SPAN Topology

Port Mirroring Configuration

This example shows detailed configuration of port mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe5`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)#exit`	Exit interface mode.
`(config)# monitor session 1`	Enter monitor session configuration mode

© 2021 IP Infusion Inc. Proprietary

(config-monitor)# destination interface xe5	Configure the interface as destination port
(config-monitor)# source interface xe10 both	Configure the source interface to mirror ingress as well as egress direction traffic
(config-monitor)# no shut	Activate monitor session
(config-monitor)#end	Exit monitor session configuration mode

Validation

Enter the below commands to confirm the configurations.

```
#show running-config monitor
!
monitor session 1
 source interface xe10 both
 destination interface xe5
 no shut

#show monitor session all
   session 1
---------------
type              : local
state             : up
source intf       :
    tx            : xe10
    rx            : xe10
    both          : xe10
source VLANs      :
    rx            :
destination ports : xe5
filter count      :

Legend: f = forwarding enabled, l = learning enabled
```

If monitor session configured with two source interface as egress direction (tx) then the destination port will receive only one copy of the egressed packet.

#configure terminal	Enter configure mode.
(config)# bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)# vlan 101-110 bridge 1 state enable	Configure VLANs.
(config)#interface xe10	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe20	Enter interface mode.

(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe30	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1	Enter monitor session configuration mode
(config-monitor)# destination interface xe5	Configure the interface as destination port
(config-monitor)# source interface xe10 tx	Configure the source interface to mirror egress direction traffic
(config-monitor)# source interface xe30 tx	Configure the source interface to mirror egress direction traffic
(config-monitor)# no shut	Activate monitor session
(config-monitor)#end	Exit monitor session configuration mode

Validation

```
#show running-config monitor
!
monitor session 1
source interface xe10 tx
source interface xe30 tx
destination interface xe5
no shut

#show monitor session all
       session 1
    ---------------
Type                : local
State               : up
source intf         :
        tx          : xe10  xe30
        rx          :
        both        :
source VLANs        :
        rx          :
```


© 2021 IP Infusion Inc. Proprietary

```
destination ports   : xe5
filter count        :
Legend: f = forwarding enabled, l = learning enable
```

If you send 10 frames from xe20 packets egress via xe10 and xe30, then on mirror destination port only 10 packets are received.

VLAN and Rule Based Mirroring

This example shows detailed configuration of VLAN with rule based mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe5`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)#exit`	Exit interface mode.
`(config)# monitor session 1`	Enter monitor session configuration mode
`(config-monitor)# destination interface xe5`	Configure the interface as destination port
`(config-monitor)# source vlan 101`	Configure source VLAN to be mirrored
`(config-monitor)# filter src-mac host 0000.0000.0005`	Configure the rule to match the source MAC
`(config-monitor)# no shut`	Activate monitor session
`(config-monitor)#end`	Exit monitor session configuration mode

Validation

Enter the below commands to confirm the configurations.

```
#show running-config monitor
!
monitor session 1
 source vlan 101
 destination interface xe5
```


© 2021 IP Infusion Inc. Proprietary

```
 filter src-mac host 0000.0000.0005
 no shut


#show monitor session all
   session 1
---------------
type               : local
state              : up
source intf        :
    tx             :
    rx             :
    both           :
source VLANs       :
    rx             : 101
destination ports  : xe5
filter count       : 1

Legend: f = forwarding enabled, l = learning enabled


#show monitor session 1 filter
   session 1
---------------
filter count       : 1

  ---------------
  match set 1
  ---------------
  source mac address : 0000.0000.0005 (host)
```

RSPAN Overview

When several switches need to be analyzed with a single centralized sniffer, remote switched port analyzer (RSPAN) is used. In RSPAN, all the mirrored traffic will be tagged with a RSPAN VLAN ID and forwarded to remote destination via a port called reflector port. Reflector port will have the same characteristics of a local destination port. RSPAN VLAN ID will be a dedicated VLAN for the monitoring purpose and will not participate in bridging. RSPAN destination switch will strip the RSPAN VLAN tag and send it the sniffer for analysis. RSPAN will have the same sub-categories as SPAN except that the mirrored traffic will be tagged with RSPAN VLAN header and forwarded to destination switch for analysis.

Topology

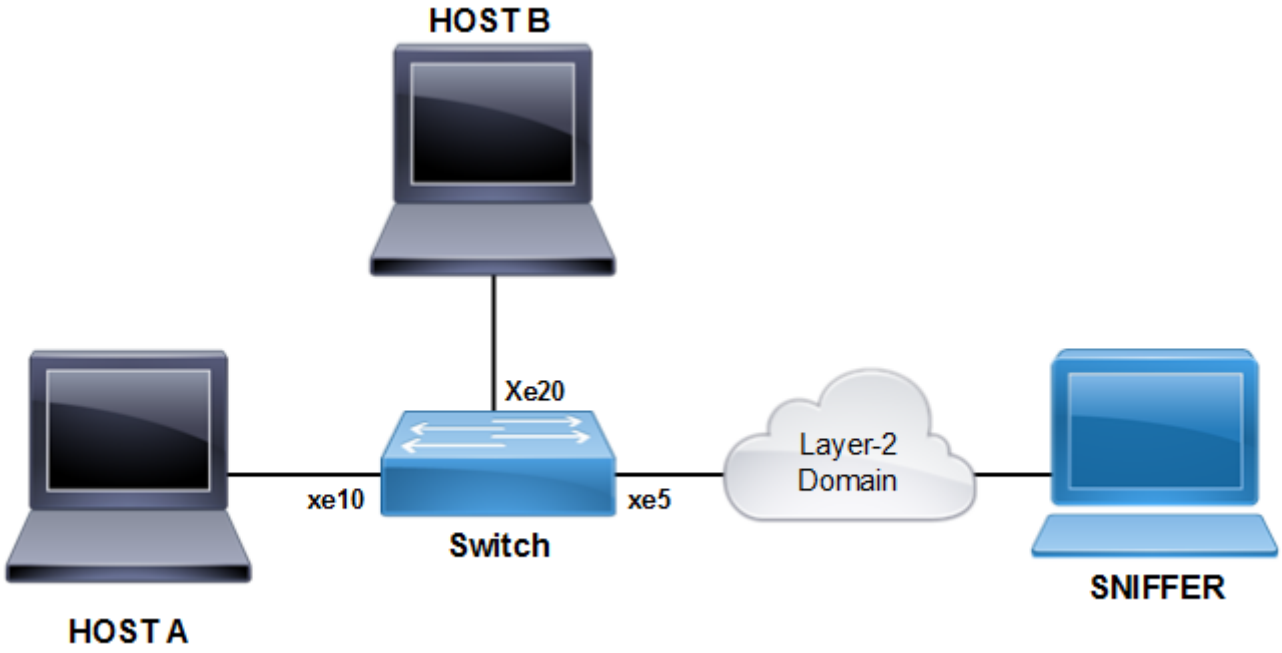


Figure 29-45: RSPAN Topology

Port Mirroring Configuration

This example shows detailed configuration of port mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.

© 2021 IP Infusion Inc. Proprietary

(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe20	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1 type remote	Enter monitor session configuration mode.
(config-monitor)# destination remote vlan 100 reflector-port xe5	Configure the interface as remote destination port
(config-monitor)# source interface xe10 both	Configure the source interface to mirror ingress as well as egress direction traffic.
(config-monitor)# no shut	Activate monitor session.
(config-monitor)#end	Exit monitor session configuration mode.

Validation

Enter the commands below to confirm the configurations

```
#show running-config monitor
!
monitor session 1 type remote
 source interface xe10 both
 destination remote vlan 100 reflector-port xe5
 no shut


#show monitor session all
   session 1
---------------
type               : remote
state              : up
source intf        :
    tx             : xe10
    rx             : xe10
    both           : xe10
source VLANs       :
    rx             :
rspan VLAN         : 100
```

```
reflector ports   : xe5
filter count      :

Legend: f = forwarding enabled, l = learning enabled
```


© 2021 IP Infusion Inc. Proprietary

VLAN and Rule Based Mirroring Configuration

This example shows detailed configuration of VLAN with rule based mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe5`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)#exit`	Exit interface mode.
`(config)# monitor session 1 type remote`	Enter monitor session configuration mode.
`(config-monitor)# destination remote vlan 100 reflector-port xe5`	Configure the interface as remote destination port.
`(config-monitor)# source vlan 101`	Configure source VLAN to be mirrored.
`(config-monitor)# filter src-mac host 0000.0000.0005`	Configure the rule to match the source MAC.
`(config-monitor)# no shut`	Activate monitor session.
`(config-monitor)#end`	Exit monitor session configuration mode.

Validation

Enter the commands below to confirm the configuration.

```
#show running-config monitor
!
monitor session 1 type remote
 source vlan 101
```

```
 destination remote vlan 100 reflector-port xe5
 filter src-mac host 0000.0000.0005
 no shut


#show monitor session all
   session 1
---------------
type               : remote
state              : up
source intf        :
    tx             :
    rx             :
    both           :
source VLANs       :
    rx             : 101
rspan VLAN         : 100
reflector ports    : xe5
filter count       : 1

Legend: f = forwarding enabled, l = learning enabled


#show monitor session 1 filter
   session 1
---------------
filter count       : 1

  ---------------
  match set 1
  ---------------
  source mac address : 0000.0000.0005 (host)
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 30 Trigger Failover Configuration

Overview

This chapter contains Trigger Failover (TFO) configuration examples.

This example shows the complete configuration to enable TFO in a simple network topology. TFO complements NIC teaming functionality supported on blade servers. TFO allows a switch module to monitor specific uplink ports to detect link failures. When the switch module detects a link failure, it disables the corresponding downlink ports automatically.

TFO uses these components:

- A Fail Over Group (FOG) contains a Monitor Port Group (MPG) and a Control Port Group (CPG).
- An MPG contains only uplink ports.
- A CPG contains only downlink ports.

Note:

- TFO is supported in STP or RSTP bridge mode.
- TFO can be configured on a LAG interface.

Basic Configuration



Figure 30-46: Basic topology

Switch

`#configure terminal`	Enter configure mode.
`(config)#tfo enable`	Enable TFO globally.
`(config)#fog 1 enable`	Create a Fail over group (FOG) and enable it.
`(config)#interface xe35`	Enter interface mode
`(config-if)#link-type uplink`	Specify the link-type as Uplink.
`(config-if)#fog 1 type mpg`	Specify the MPG member for FOG 1.
`(config-if)#exit`	Exit interface mode
`(config)#interface xe34`	Enter interface mode
`(config-if)#link-type downlink`	Specify the link-type as Downlink.
`(config-if)#fog 1 type cpg`	Specify the CPG member for FOG 1.
`(config-if)#end`	Exit interface and configure mode

© 2021 IP Infusion Inc. Proprietary

Validation

```
#show tfo

TFO : Enable

Failover Group 1 : Enable
Failover Status : MPG Link Failure
No. of links to trigger failover : 0
MPG Port(s) :
xe35   Status : DOWN
CPG Port :
xe34   Status : DOWN
No. of times MPG link failure : 1
No. of times MPG link recovered : 0
No. of times CPG got auto disabled : 1
No. of times CPG got auto enable : 0
```

Port-Channel Configuration

Topology



Figure 30-47: TFO with port-channel

Switch 1

`#configure terminal`	Enter configure mode.
`(config)#tfo enable`	Enable TFO globally.
`(config)#fog 1 enable`	Create a Fail over group (FOG) and enable it.
`(config)#interface po1`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer2.
`(config-if)#exit`	Exit interface mode
`(config)#interface xe32`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer2.
`(config-if)#link-type uplink`	Specify the link-type as Uplink.
`(config-if)#channel-group 1 mode active`	Specify the channel group in interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe33`	Enter interface mode
`(config-if)#switchport`	Make the interface as Layer2.

© 2021 IP Infusion Inc. Proprietary

(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#interface xe34	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#interface xe20	Enter interface mode
(config-if)#link-type downlink	Specify the link-type as Downlink.
(config-if)#fog 1 type cpg	Specify the CPG member for FOG 1
(config-if)#exit	Exit interface mode
(config)#interface po1	Enter port-channel mode
(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#fog 1 type mpg	Specify the MPG member for FOG 1.
(config-if)#exit	Exit interface and configure mode

Switch 2

(config)#interface po1	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#exit	Exit interface mode
(config)#interface xe32	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#interface xe33	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#interface xe34	Enter interface mode
(config-if)#switchport	Make the interface as Layer2
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode

Validation

```
#show interface brief | include up
xe20      ETH   --    routed           up      none    1g    --       Br  Yes
xe32      ETH   --    routed           up      none    10g   --       Br  Yes
xe33      ETH   --    routed           up      none    10g   --       No  No
xe34      ETH   --    routed           up      none    10g   --       No  No
```

```
eth0      METH                          up       --      1g
lo                                      up       --
lo.management                           up       --

#show tfo

TFO : Enable

Failover Group 1 : Enable
Failover Status : MPG Link Failure
No. of links to trigger failover : 0
MPG Port(s) :
po1   Status : DOWN
CPG Port :
xe20   Status : DOWN
No. of times MPG link failure : 0
No. of times MPG link recovered : 0
No. of times CPG got auto disabled : 0
No. of times CPG got auto enable : 0
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 31 User Configuration

Overview

User management is an authentication feature that provides administrators with the ability to identify and control the users who log into the network.

OcNOS provides 4 different roles for users.

- Network Administrator: can make permanent changes to switch configuration. Changes are persistent across reset/reboot of switch.
- Network Engineer: can make permanent changes to switch configuration. Changes are persistent across reset/reboot of switch.
- Network Operator: can make permanent changes to switch configuration. Changes are not persistent across reset/reboot of switch.
- Network User: displays information; cannot modify configuration.

User Configuration

`#configure terminal`	Enter configure mode.
`(config)#username user1 password user12345`	Create “user1” with password user12345 which will have default role as network-user.
`(config)#username user1 role network-operator password user12345`	Change the role for user1 to network-operator.
`(config)#username user2 role network-operator password user12345`	Create “user2” with role as network-operator.
`(config)#username user3 role network-admin password user12345`	Create “user3” with role as network-admin.
`(config)#username user4 role network-engineer password user12345`	Create “user4” with role as network-engineer.
`(config)#exit`	Exit configure mode.

Validation Commands

`show user-account, show user-account <username>, show role`

```
    #show user-account
    User:user1
                    roles: network-operator
    User:user2
                    roles: network-operator
    User:user3
                    roles: network-admin
    User:user4
                    roles: network-engineer
```

```
#show role
Role Name                              Info
-------------------------------------------------------------------------
network-admin          Network Administrator - Have all permissions
network-engineer       Network Engineer - Can save configuration
network-operator       Network Operator - Can not save configuration
network-user           Network User - Can not change configuration
rbac-customized-role   RBAC User - Can change only  permitted configuration


#show user-account user1
User:user1
                roles: network-operator
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 32 Using the Management Interface

Overview

OcNOS provides support for different types of Management Interfaces. The management interface can be the standard out of band (OOB) port, or any in-band port.

To provide segregation between management traffic and data traffic, OcNOS provides a Management VRF. The Management VRF is created by default when OcNOS boots. This VRF cannot be deleted. All ports used as Management Interface needs to be in Management VRF. The management VRF is used for all types of Management applications listed below

- Remote access to router (SSH/Telnet)
- File transfer applications (SFTP/SCP)
- Login Authentication via Radius/Tacacs
- Network management protocols (SNMP, Netconf)

Apart from this, DHCP, DNS, NTP, Syslog, License/Software upgrade also uses ports mapped to management VRF for their operations. Also LLDP protocol can be run on any ports mapped to this Management VRF.

Note: If the management interface flaps, the device becomes unreachable.

Management Port

The Out of Band (OOB) Management Port in OcNOS is identified as “eth0.” This port is automatically mapped to the Management VRF when OcNOS boots, and will remain in same VRF throughout. It cannot be moved out of this VRF.

The IP address of the management port can be configured statically or via DHCP.

Static IP Configuration

A static IP can be configured on the management port during ONIE installation itself, or after installation using the OcNOS CLIs commands. To configure a static IP during ONIE installation, do the following

```
#onie-discovery-stop
#ifconfig eth0 <ip address> netmask <subnet mask> up
```

Please check the *Install Guide* for details.

The IP address configured during ONIE installation will be applied to the management port and the same will be retained when OcNOS boot up, and the port becomes part of Management VRF.

```
#show running-config interface eth0
!
interface eth0
 ip vrf forwarding management
 ip address 10.12.44.109/24
```

After getting the OcNOS prompt, this IP address can be changed from the CLI.

`#configure terminal`	Enter configure mode
`(config)#interface eth0`	Enter interface mode
`(config-if)#ip address 10.12.44.120/24`	Assign an IPv4 address to the interface
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit configuration mode

If a static IP is not configured during ONIE installation the same can be configured via CLI by following the above steps. Using the OcNOS CLI, DHCP can also be enabled on the Management port.

`#configure terminal`	Enter configure mode
`(config)#interface eth0`	Enter interface mode
`(config-if)#ip address dhcp`	Enable DHCP on interface
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit configuration mode

Obtaining IP Address via DHCP

During onie installation, the management port attempts to acquire IP address via DHCP automatically unless stopped explicitly using “onie-discovery-stop”. So, if management port is getting IP via DHCP, after OcNOS boots, the management port will continue to use DHCP, even when it is part of the Management VRF.

```
#show running-config interface eth0
!
interface eth0
 ip vrf forwarding management
 ip address dhcp
```

After OcNOS boots, the IP address can be changed to any static IP from the command line as shown earlier.

In-Band Ports

Any front-end ports of the device (in-band ports) can be made part of the management VRF. Once they are part of the management VRF they can also support all management applications such as SSH/Telnet and others as listed in Overview.

Once the ports are part of the management VRF, they should not be used for data traffic and routing or switching purposes. In-band ports can be added or removed from Management VRF as and when required.

`#configure terminal`	Enter configure mode
`(config)#interface xe1/1`	Enter interface mode
`(config-if)#ip vrf forwarding management`	Add in-band port to Management VRF
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit configuration mode

`#configure terminal`	Enter configure mode
`(config)#interface xe1/1`	Enter interface mode

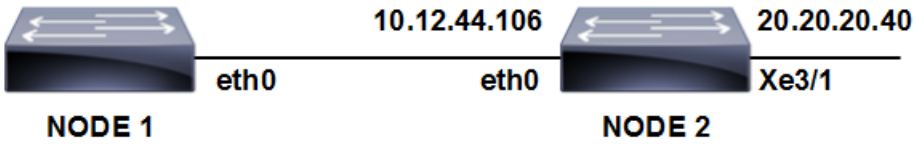
© 2021 IP Infusion Inc. Proprietary

`(config-if)# no ip vrf forwarding management`	Remove in-band port from Management VRF
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit configuration mode

Using Ping in Management VRF

To check reachability to any node in the management network, you need to explicitly mention the VRF name as “management.”

In the following example, Node-1 has management interface eth0 and Node-2 has management interfaces eth0 and xe3/1. In order to reach the network 20.20.20.40/24 from Node-1 a static route needs to added.



`#configure terminal`	Enter configure mode
`(config)# ip route vrf management 20.20.20.0/24 10.12.44.106 eth0`	Add static route in management VRF to reach 20.20.20.0/24 network
`(config)#exit`	Exit configuration mode

```
Node-1#show ip route vrf management
Codes: K - kernel, C - connected, S - static, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "management"
C       10.12.44.0/24 is directly connected, eth0
S       20.20.20.0/24 [1/0] via 10.12.44.106, eth0

Gateway of last resort is not set

Node-1#ping 20.20.20.40 vrf management
PING 20.20.20.40 (20.20.20.40) 56(84) bytes of data.
64 bytes from 20.20.20.40: icmp_seq=1 ttl=64 time=0.494 ms
64 bytes from 20.20.20.40: icmp_seq=2 ttl=64 time=0.476 ms
```

© 2021 IP Infusion Inc. Proprietary

System Management Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Access Control List Commands (Standard)*
- Chapter 2, *Access Control List Commands (XGS)*
- Chapter 3, *Authentication, Authorization and Accounting*
- Chapter 4, *Basic Commands*
- Chapter 5, *Chassis Management Module Commands*
- Chapter 6, *Configuration Management*
- Chapter 7, *Common Management Layer Commands*
- Chapter 8, *DHCP Snooping Commands*
- Chapter 9, *DHCPv6 Prefix delegation Commands*
- Chapter 10, *Digital Diagnostic Monitoring Commands*
- Chapter 11, *Dynamic Host Configuration Protocol Client*
- Chapter 12, *Dynamic Host Configuration Protocol Relay*
- Chapter 13, *Domain Name System*
- Chapter 14, *Interface Commands*
- Chapter 15, *IP Service Level Agreements Commands*
- Chapter 16, *Linux Shell Commands*
- Chapter 17, *Network Time Protocol*
- Chapter 18, *RADIUS*
- Chapter 19, *Secure Shell*
- Chapter 20, *sFlow Commands*
- Chapter 21, *Simple Network Management Protocol*
- Chapter 22, *Software Monitoring and Reporting*
- Chapter 23, *Syslog*
- Chapter 24, *System Configure Mode Commands*
- Chapter 25, *TACACS+*
- Chapter 26, *Telnet*
- Chapter 27, *Time Range Commands*
- Chapter 28, *Traffic Mirroring Commands*
- Chapter 29, *Trigger Failover Commands*
- Chapter 30, *User Management*
- Chapter 31, *VLOG Commands*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Access Control List Commands (Standard)

This chapter is a reference for the standard Access Control List (ACL) commands. Standard access-lists are not allowed to be attached to interfaces and are used for protocol-level filtering.

- ip access-list standard
- ip access-list standard filter
- Ipv6 access-list standard
- ipv6 access-list standard filter

ip access-list standard

Use this command to define a standard IP access control list (ACL) in which multiple specifications can be configured. A specification determines whether to accept or drop an incoming IP packet based on the source IP address, either an exact match or a range of prefixes.

A standard ACL can be used by Layer 3 and SNMP protocols to permit or deny IP packets from a host or a range of prefixes.

Use the `no` form of this command to remove an ACL.

Note: Standard access-lists are not allowed to be attached to interfaces and are used for protocol-level filtering purposes.

Command Syntax

```
ip access-list standard NAME
no ip access-list standard NAME
```

Parameters

`NAME`	Standard IP access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#configure terminal
(config)#ip access-list standard ip-acl-01
(config-ip-acl-std)#exit
(config)#no ip access-list standard ip-acl-01
```


© 2021 IP Infusion Inc. Proprietary

ip access-list standard filter

Use this command to configure an access control entry in an access control list (ACL). This command determines whether to accept or drop a packet based on the configured source IP address.

Use the `no` form of this command to remove an ACL specification.

Command Syntax

```
(deny|permit) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
no (deny|permit) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
```

Parameters

`deny`	Drop the packet.
`permit`	Accept the packet.
`A.B.C.D/M`	Source IP prefix and length.
`A.B.C.D A.B.C.D`	Source IP address and mask.
`host A.B.C.D`	A single source host IP address.
`any`	Match any source IP address.

Default

No default value is specified

Command Mode

Standard IP access-list mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl-std)#permit 30.30.30.0/24
(config-ip-acl-std)#no permit 30.30.30.0/24
```

Ipv6 access-list standard

Use this command to define a standard IPv6 access control list (ACL) in which multiple specifications can be configured. A specification determines whether to accept or drop an incoming IPv6 packet based on the source IPv6 address, either an exact match or a range of prefixes.

a standard IPv6 ACL can be used by Layer 3 protocols to permit or deny IPv6 packets from a host or a range of prefixes.

Use the `no` form of this command to remove an ACL.

Note: Standard access-lists are not allowed to be attached to interfaces and are used for protocol-level filtering purposes.

Command Syntax

```
ipv6 access-list standard NAME
no ipv6 access-list standard NAME
```

Parameters

`NAME`	Standard IPv6 access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#configure terminal
(config)#ipv6 access-list standard ipv6-acl-01
(config-ipv6-acl-std)#exit
(config)#no ipv6 access-list standard ipv6-acl-01
```


© 2021 IP Infusion Inc. Proprietary

ipv6 access-list standard filter

Use this command to configure an access control entry in an access control list (ACL).This commands determines whether to accept or drop a packet based on the configured IPv6 prefix.

Use the `no` form of this command to remove an ACL specification.

Command Syntax

```
(deny|permit)(X:X::X:X/M|X:X::X:X X:X::X:X|any)
no(deny|permit)(X:X::X:X/M|X:X::X:X X:X::X:X|any)
```

Parameters

`deny`	Drop the packet.
`permit`	Accept the packet.
`X:X::X:X/M`	Source address with network mask length.
`X:X::X:X X:X::X:X`	Source address with wild card mask.
`any`	Any source address.

Default

No default value is specified

Command Mode

Standard IPv6 access-list mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#configure terminal
(config)#ipv6 access-list standard ipv6-acl-01
(config-ipv6-acl-std)#permit 2000::0/64
(config-ipv6-acl-std)#no permit 2000::0/64
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Access Control List Commands (XGS)

This chapter is a reference for the Access Control List (ACL) commands for XGS devices (Trident II, Trident II+, and Tomahawk):

- access-list logging cache-size
- access-list logging rate-limit
- arp access-group
- arp access-list
- arp access-list filter
- arp access-list remark
- arp access-list resequence
- arp access-list response
- clear access-list
- clear access-list log-cache
- clear arp access-list
- clear ip access-list
- clear ipv6 access-list
- clear mac access-list
- ip access-group
- ip access-list
- ip access-list default
- ip access-list filter
- ip access-list fragments
- ip access-list icmp
- ip access-list remark
- ip access-list resequence
- ip access-list tcp|udp
- ipv6 access-group
- ipv6 access-list
- ipv6 access-list default
- ipv6 access-list filter
- ipv6 access-list fragments
- ipv6 access-list icmpv6
- ipv6 access-list remark
- ipv6 access-list resequence
- ipv6 access-list sctp
- ipv6 access-list tcp|udp
- line vty
- mac access-group

© 2021 IP Infusion Inc. Proprietary

- mac access-list
- mac access-list default
- mac access-list filter
- mac access-list remark
- mac access-list resequence
- show access-lists
- show access-list log-cache
- show arp access-lists
- show ip access-lists
- show ipv6 access-lists
- show mac access-lists
- show running-config aclmgr
- show running-config access-list
- show running-config ipv6 access-list

© 2021 IP Infusion Inc. Proprietary

access-list logging cache-size

Use this command to set the ACL logging table size.

Use the `no` form of this command to set the table size to its default (1000).

Command Syntax

```
access-list logging cache-size <1000-10000>
no access-list logging cache-size
```

Parameters

`<1000-10000>`	Maximum number of cache entries

Default

By default, the logging table size is 1000.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#access-list logging cache-size 2000
(config)#end
```

access-list logging rate-limit

Use this command to set the rate limit for logging ACL denied packets.

Use the `no` form of this command to reset the rate to its default (200).

Command Syntax

```
access-list logging rate-limit <0-1000>
no access-list logging rate-limit
```

Parameters

`<0-1000>`	Packets per second

Default

By default, the rate is 200 packets per second.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#access-list logging rate-limit 500
(config)#end
```


© 2021 IP Infusion Inc. Proprietary

arp access-group

Use this command to attach ARP access list to an interface to filter incoming ARP packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

Use the `no` form of this command to detach an ARP access group.

Note: To attach an ARP access-group to an interface, the ingress-arp TCAM group should be enabled. See the hardware-profile filter (XGS) command for more details.

Command Syntax

```
arp access-group NAME in
no arp access-group NAME in
```

Parameters

`NAME`	ARP Access list name

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#exit
(config)#interface xe1
(config-if)#arp access-group ARP_ACL1 in
(config-if)#no arp access-group ARP_ACL1 in
```

arp access-list

Use this command to define a named ARP access control list (ACL) that determines whether to accept or drop an incoming ARP packet based on the sender or target IP address, sender or target MAC address, ARP type.

An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are sequenced. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. The implied specification can be updated to permit if the use-case is to deny a certain set of ARP traffic.

Use the no form of this command to remove an ACL specification

Command Syntax

```
arp access-list NAME
no arp access-list NAME
```

Parameters

NAME	ARP Access list name

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#exit
(config)#no arp access-list ARP_ACL1
```


© 2021 IP Infusion Inc. Proprietary

arp access-list filter

Use this command to configure access control entry in ARP access control list (ACL).

This determines whether to accept or drop an ARP packet based on the configured match criteria. Use the no form of this command to remove an ACL specification.

Note: Configuring the same filter again with a change of sequence number or change of action results in an update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (request |) ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) mac (any | (XX-XX-XX-XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-
  XX-XX-XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (vlan <1-4094>|) (inner-vlan <1-4094>|)
  (log|) (sample|)
no (<1-268435453>|)(deny|permit) (request |) ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) mac (any | (XX-XX-XX-XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-
  XX-XX-XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (vlan <1-4094>|) (inner-vlan <1-4094>|)
  (log|) (sample|)
```

Parameters

`deny`	Drop the packet.
`permit`	Accept the packet.
`<1-268435453>`	ARP ACL sequence number.
`request`	RP request type
`A.B.C.D/M`	Source IP prefix and length.
`A.B.C.D A.B.C.D`	Source IP address and mask.
`host A.B.C.D`	Single source host IP address.
`any`	Match any source IP address.
`any`	Any source/destination.
`XX-XX-XX-XX-XX-XX`	Source MAC address (Option 1).
`XX:XX:XX:XX:XX:XX`	Source MAC address (Option 2).
`XXXX.XXXX.XXXX`	Source MAC address (Option 3).
`XX-XX-XX-XX-XX-XX`	Source wildcard (Option 1).

`XX:XX:XX:XX:XX:XX`	Source wildcard (Option 2).
`XXXX.XXXX.XXXX`	Source wildcard (Option 3).
`vlan <1-4094>`	VLAN identifier.
`inner-vlan<1-4094>`	Inner VLAN identifier.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#15 permit ip host 2.2.2.1 mac any inner-vlan 3
(config-arp-acl)#no 15
```


© 2021 IP Infusion Inc. Proprietary

arp access-list remark

Use this command to add a description to a named ARP access control list (ACL).

Use the no form of this command to remove an ACL description.

Command Syntax

```
remark LINE
no remark
```

Parameters

LINE	ACL description up to 100 characters.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#arp access-list arplist
(config-arp-acl)#remark permit the selected arp entries
(config-arp-acl)#exit
(config)#arp access-list arplist
(config-arp-acl)#no remark
(config-arp-acl)#exit
```

arp access-list resequence

Use this command to modify the sequence numbers of an ARP access list.

Note: IP Infusion Inc. recommends to use a non-overlapping sequence space for a new sequence number set to avoid unexpected rule matches during transition.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting sequence number.
`INCREMENT`	Sequence number increment steps.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#ip access-list arplist
(config-arp-acl)#resequence 5 5
(config-arp-acl)#end
```


© 2021 IP Infusion Inc. Proprietary

arp access-list response

Use this command to configure an ARP access control entry in an ARP access control list (ACL). This determines whether to accept or drop an ARP response packet based on the configured match criteria.

Use the `no` form of this command to remove an ACL specification.

Command Syntax

```
(<1-268435453>|)(deny|permit) response ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) mac (any | (XX-XX-XX-
  XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (vlan <1-4094>|) (inner-vlan <1-4094>|)
  (log|) (sample|)
no (<1-268435453>|)(deny|permit) response ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) mac (any | (XX-XX-XX-
  XX-XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-
  XXXX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (vlan <1-4094>|) (inner-vlan <1-4094>|)
  (log|) (sample|)
```

Parameters

`deny`	Drop the packet.
`permit`	Accept the packet.
`<1-268435453>`	ARP ACL sequence number.
`response`	ARP reply type
`A.B.C.D/M`	Source/Destination IP prefix and length.
`A.B.C.D A.B.C.D`	Source/Destination IP address and mask.
`host A.B.C.D`	A single source/destination host IP address.
`any`	Match any source/destination IP address.

`any`	Source/Destination any.
`XX-XX-XX-XX-XX-XX`	Source/Destination MAC address (Option 1).
`XX:XX:XX:XX:XX:XX`	Source/Destination MAC address (Option 2).
`XXXX.XXXX.XXXX`	Source/Destination MAC address (Option 3).
`XX-XX-XX-XX-XX-XX`	Source/Destination wildcard (Option 1).
`XX:XX:XX:XX:XX:XX`	Source/Destination wildcard (Option 2).
`XXXX.XXXX.XXXX`	Source/Destination wildcard (Option 3).
`vlan <1-4094>`	VLAN identifier.
`inner-vlan <1-4094>`	Inner VLAN identifier.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#arp access-list ARP_ACL1
(config-arp-acl)#50 permit response ip host 2.2.2.1 any mac any any vlan 2
(config-arp-acl)#no 50 permit response ip host 2.2.2.1 any mac any any vlan 2
```


© 2021 IP Infusion Inc. Proprietary

clear access-list

Use this command to clear the access-list counters.

Command Syntax

```
clear access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode and Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear access-list counters
```

clear access-list log-cache

Use this command to clear the access-list logging table.

Command Syntax

```
clear access-list log-cache
```

Parameters

None

Command Mode

Exec mode and Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear access-list log-cache
```


© 2021 IP Infusion Inc. Proprietary

clear arp access-list

Use this command to clear the ARP access-list counters.

Command Syntax

```
clear arp access-list (NAME|) counters
```

Parameters

NAME	ARP access list name

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#clear arp access-list counters
```

clear ip access-list

Use this command to clear the IP access-list counters.

Command Syntax

```
clear ip access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode and Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip access-list counters
```


© 2021 IP Infusion Inc. Proprietary

clear ipv6 access-list

Use this command to clear the IPv6 access-list counters.

Command Syntax

```
clear ipv6 access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ipv6 access-list counters
```

clear mac access-list

Use this command to clear the MAC access-list counters.

Command Syntax

```
clear mac access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear mac access-list counters
```


© 2021 IP Infusion Inc. Proprietary

ip access-group

Use this command to attach an IP access list to an interface or terminal line to filter incoming or outgoing IP packets.

The `time-range` parameter is optional. If used, the access-group is tied to the timer specified.

After the access-group has been configured with the time-range, to detach the access-group from the time-range, use the `no` form of this command with a time-range parameter as shown in the syntax and examples below.

To delete the access-group, use the `no` form of this command without a time-range.

Note: An egress IP ACL is supported on physical and lag interfaces only. An egress IP ACL will match only routed traffic and not switched traffic. VLAN and inner-VLAN options in ACL rules will match incoming packet VLANs even when ACL attached at egress.

Command Syntax

```
ip access-group NAME (in|out) (time-range TR_NAME|)
no ip access-group NAME (in|out) (time-range TR_NAME|)
```

Parameters

`NAME`	Access list name.
`in`	Filter incoming packets
`out`	Filter outgoing packets.
`TR_NAME`	Time range name set with the time-range command.

Command Mode

Line mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3. The `time-range` parameter was added in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#permit ip any any
(config-ip-acl)#exit

(config)#hardware-profile filter ingress-ipv4-ext enable

(config)#interface xe3
(config-if)#ip access-group mylist in
(config-if)#exit

(config)#interface xe3
(config-if)#no ip access-group mylist in time-range TIMER1
(config-if)#exit
```

```
(config)#line vty
(config-all-line)#no ip access-group mylist in
```

Usage: VLANs and LAGs

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

Usage: TCAM Groups

An access-group in the egress direction uses the TCAM group used by the QoS output service policy. Therefore, actions are unpredictable when conflicting matches are configured on same interface. IP Infusion Inc. recommends to avoid such a configuration. Otherwise, you need to configure the priority (in QoS) or the sequence number (in ACL) carefully to handle such cases.

To attach an IP ACL in the ingress direction, ensure the `ingress-ipv4` TCAM group is enabled. See the hardware-profile filter (XGS) commands for details.

Usage: Loopback and VTY Interfaces

You can create ACLs for loopback (inband) and VTY interfaces to protect management applications such as SSH, Telnet, NTP, SNMP, and SNMP traps. Filtering TCP, UDP, and ICMP are supported.

Note: Loopback and VTY ACLs are mutually exclusive. If you set up one, you cannot set up the other.

For an ACL for a loopback interface, you create the ACL, configure it with rules, and associate the ACL with a loopback interface:

```
...
(config)#interface lo
(config-if)#ip access-group loopback in
```

For an ACL for VTY, you create the ACL, configure it with rules, and associate the ACL to the terminal line in line mode:

```
...
(config)#line vty
(config-all-line)#ip access-group vty in
```

Loopback and VTY ACLs do not support the following:

- The default rule `deny all`. You must explicitly set up a `deny all` rule based on your requirements.
- VLAN-specific rules.
- Rules with TCP flags.
- Rules with `dscp`, `fragments`, `log`, `precedence`, and `sample` parameters.

Usage: Timed ACL on interfaces

You create a timer range that is identified by a name and configured with a start time, end time, and frequency. Once you create the time range, you can tie the ACL configuration to the time-range object. This allows you to create an

 © 2021 IP Infusion Inc. Proprietary

access group that is enabled when the timer has started and disabled when the timer ends. You can also disassociate an access group from the timer if needed.

ip access-list

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming IP packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Use the `no` form of this command to remove an ACL

Command Syntax

```
ip access-list NAME
no ip access-list NAME
```

Parameters

`NAME`	Access-list name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
```


© 2021 IP Infusion Inc. Proprietary

ip access-list default

Use this command to modify the default rule action of access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the IP packets not matching any of the user defined rules match default rule.

Command Syntax

```
default (deny-all|permit-all) (log|) (sample|)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl)#default permit-all sample
```

ip access-list filter

Use this command to configure access control entry in an access control list (ACL).

This determines whether to accept or drop an IP packet based on the configured match criteria.

Use the `no` form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) (deny|permit) (<0-255>|ahp|any|eigrp|esp|gre|ipip|ipcomp|ipv6ip
  |ospf|pim|rsvp|vrrp) (A.B.C.D/ M|A.B.C.D A.B.C.D|host A.B.C.D|any) (A.B.C.D/
  M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63>|af11| af12| af13| af21| af22|
  af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
  default| ef )|) (fragments|) (vlan <1-4094>|)(inner-vlan <1-4094>|) (log|)
  (sample|)((redirect-to-port IFNAME)|)
no (<1-268435453>|)(deny|permit)(<0-255> |ahp | any | eigrp | esp | gre | ipip |
  ipcomp | ipv6ip | ospf | pim | rsvp| vrrp) (A.B.C.D/ M|A.B.C.D A.B.C.D | host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63> |af11|
  af12| af13| af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3|
  cs4| cs5|cs6| cs7| default| ef )|) (fragments|) (vlan <1-4094>|)(inner-vlan <1-
  4094>|) (log|) (sample|)|)((redirect-to-port IFNAME)|)
no (<1-268435453>)
```

Parameters

`<1-268435453>`	IPv4 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`<0-255>`	IANA assigned protocol number.
`any`	Any protocol packet.
`ahp`	Authentication Header packet.
`eigrp`	Enhanced Interior Gateway Routing Protocol packet.
`esp`	Encapsulating Security Payload packet.
`gre`	Generic Routing Encapsulation packet.
`ipip`	IPv4 over IPv4 encapsulation packet.
`ipcomp`	IP Payload Compression Protocol packet.
`ipv6ip`	IPv6 over IPv4 encapsulation packet.
`ospf`	Open Shortest Path First packet.
`pim`	Protocol Independent Multicast packet
`rsvp`	Resource Reservation Protocol packet.
`vrrp`	Virtual Router Redundancy Protocol packet.
`A.B.C.D/M`	Source IP prefix and length.

© 2021 IP Infusion Inc. Proprietary

`A.B.C.D A.B.C.D`	
	Source IP address and mask.
`host A.B.C.D`	A single source host IP address.
`any`	Match any source IP address.
`A.B.C.D/M`	Destination IP prefix and length.
`A.B.C.D A.B.C.D`	
	Destination IP address and mask.
`host A.B.C.D`	A single destination host IP address.
`any`	Any destination address
`any`	Match any destination IP address.
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34
`af42`	AF42 DSCP (100100) decimal value 36.
`af43`	AF43 DSCP (100110) decimal value 38.
`cs1`	CS1 (precedence 1) DSCP (001000) decimal value 8.
`cs2`	CS2 (precedence 2) DSCP (010000) decimal value 16.
`cs3`	CS3 (precedence 3) DSCP (011000) decimal value 24.
`cs4`	CS4 (precedence 4) DSCP (100000) decimal value 32.
`cs5`	CS5 (precedence 5) DSCP (101000) decimal value 40.
`cs6`	CS6 (precedence 6) DSCP (110000) decimal value 48.
`cs7`	CS7 (precedence 7) DSCP (111000) decimal value 56.
`default`	Default DSCP (000000) decimal value 0.
`ef`	EF DSCP (101110) decimal value 46.
`precedence`	Match packets with given precedence value.
`<0-7>`	Enter precedence value 0-7.
`critical`	Match packets with critical precedence (5).
`flash`	Match packets with flash precedence (3).
`flashoverride`	
	Match packets with flash override precedence (4).

`immediate`	Match packets with immediate precedence (2).
`internet`	Match packets with internetwork control precedence (6).
`network`	Match packets with network control precedence (7).
`priority`	Match packets with priority precedence (1).
`routine`	Match packets with routine precedence (0).
`fragments`	Check non-initial fragments.
`vlan`	Match packets with given VLAN identifier.
`<1-4094>`	Enter VLAN identifier.
`inner-vlan`	Match packets with given inner VLAN identifier.
`<1-4094>`	Enter inner-VLAN identifier.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).
`redirect-to-port`	
	Redirect the packet (in-direction only)
`IFNAME`	Interface name to which packet to be redirected (switchport only)

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl)#11 permit any 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
(config-ip-acl)#no 11
```


© 2021 IP Infusion Inc. Proprietary

ip access-list fragments

Use this command to configure access list to deny or permit all the IP fragmented packets.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|)
no (<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|)
```

Parameters

`deny-all`	Drop the packet.
`permit-all`	Accept the packet.
`<1-268435453>`	IPv4 ACL sequence number.
`fragments`	Check non-initial.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#fragments deny-all
(config-ip-acl)#end
```

ip access-list icmp

Use this command to permit or deny ICMP packets based on the given source and destination IP address. Even DSCP, precedence, VLAN identifier, inner VLAN identifier, and fragment number can be configured to permit or deny with the given values.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (administratively-prohibited|
  alternate-address| conversion-error|dod-host-prohibited| dod-net-prohibited|
  echo| echo-reply|general-parameter-problem| host-isolated| host-precedence-
  unreachable|host-redirect| host-tos-redirect| host-tos-unreachable| host-
  unknown|host-unreachable| information-reply| information-request| mask-
  reply|mask-request| mobile-redirect| net-redirect| net-tos-redirect|net-tos-
  unreachable| net-unreachable| network-unknown| no-room-for-option|option-missing|
  packet-too-big| parameter-problem| port-unreachable|precedence-unreachable|
  protocol-unreachable| reassembly-timeout| redirect|router-advertisement| router-
  solicitation| source-quench|source-route-failed|time-exceeded| timestamp-reply|
  timestamp-request| traceroute|ttl-exceeded|unreachable|(<0-255> (<0-255>|))|)
  ((dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32| af33| af41| af42|
  af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef ))| (precedence (<0-7>|
  critical| flash | flashoverride|immediate| internet| network| priority|
  routine))|) (fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|) (log|) (sample|)
  ((redirect-to-port IFNAME)|)
no (<1-268435453>|)(deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (administratively-
  prohibited| alternate-address| conversion-error|dod-host-prohibited| dod-net-
  prohibited| echo| echo-reply|general-parameter-problem| host-isolated| host-
  precedence-unreachable|host-redirect| host-tos-redirect| host-tos-unreachable|
  host-unknown|host-unreachable| information-reply| information-request| mask-
  reply|mask-request| mobile-redirect| net-redirect| net-tos-redirect|net-tos-
  unreachable| net-unreachable| network-unknown| no-room-for-option|option-missing|
  packet-too-big| parameter-problem| port-unreachable|precedence-unreachable|
  protocol-unreachable| reassembly-timeout| redirect|router-advertisement| router-
  solicitation| source-quench|source-route-failed|time-exceeded| timestamp-reply|
  timestamp-request| traceroute|ttl-exceeded|unreachable|(<0-255> (<0-255>|))|)
  ("dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32| af33| af41| af42|
  af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef ))| (precedence (<0-7>|
  critical| flash | flashoverride|immediate| internet| network| priority|
  routine))|) (fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|)(log|)(sample|)
  ((redirect-to-port IFNAME)|)
```

Parameters

`<1-268435453>`	IPv4 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.

© 2021 IP Infusion Inc. Proprietary

`icmp` Internet Control Message Protocol packet.

`A.B.C.D/M` Source IP prefix and length.

`A.B.C.D A.B.C.D`
Source IP address and mask.

`host A.B.C.D` A single source host IP address.

`any` Match any source IP address.

`A.B.C.D/M` Destination IP prefix and length.

`A.B.C.D A.B.C.D`
Destination IP address and mask.

`host A.B.C.D` A single destination host IP address.

`any` Match any destination IP address.

`administratively-prohibited`
Administratively prohibited.

`alternate-address`
Alternate address.

`conversion-error`
Datagram conversion.

`dod-host-prohibited`
Host prohibited.

`dod-net-prohibited`
Net prohibited.

`echo` Echo (ping).

`echo-reply` Echo reply.

`general-parameter-problem`
Parameter problem.

`host-isolated` Host isolated.

`host-precedence-unreachable`
Host unreachable for precedence.

`host-redirect` Host redirect.

`host-tos-redirect`
Host redirect for ToS.

`host-tos-unreachable`
Host unreachable for ToS.

`host-unknown` Host unknown.

`host-unreachable`
Host unreachable.

`information-reply`
Information replies.

`information-request`

Information requests.

`mask-reply` Mask replies.

`mask-request` Mask requests.

`mobile-redirect`
Mobile host redirect.

`net-redirect` Network redirect.

`net-tos-redirect`
Net redirect for ToS.

`net-tos-unreachable`
Network unreachable for ToS.

`net-unreachable`
Net unreachable.

`network-unknown`
Network unknown.

`no-room-for-option`
Parameter required but no room.

`option-missing` Parameter required but not present.

`packet-too-big` Fragmentation needed and DF set.

`parameter-problem`
All parameter problems.

`port-unreachable`
Port unreachable.

`precedence-unreachable`
Precedence cutoff.

`protocol-unreachable`
Protocol unreachable.

`reassembly-timeout`
Reassembly timeout.

`redirect` All redirects.

`router-advertisement`
Router discovery advertisements.

`router-solicitation`
Router discovery solicitations.

`source-quench` Source quenches.

`source-route-failed`
Source route failed.

`time-exceeded` All time-exceeded messages.

`timestamp-reply`
Time-stamp replies.

© 2021 IP Infusion Inc. Proprietary

`timestamp-request`	
	Time-stamp requests.
`traceroute`	Traceroute.
`ttl-exceeded`	TTL exceeded.
`unreachable`	All unreachables.
`<0-255>`	ICMP type.
`<0-255>`	ICMP code.
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34
`af42`	AF42 DSCP (100100) decimal value 36.
`af43`	AF43 DSCP (100110) decimal value 38.
`cs1`	CS1 (precedence 1) DSCP (001000) decimal value 8.
`cs2`	CS2 (precedence 2) DSCP (010000) decimal value 16.
`cs3`	CS3 (precedence 3) DSCP (011000) decimal value 24.
`cs4`	CS4 (precedence 4) DSCP (100000) decimal value 32.
`cs5`	CS5 (precedence 5) DSCP (101000) decimal value 40.
`cs6`	CS6 (precedence 6) DSCP (110000) decimal value 48.
`cs7`	CS7 (precedence 7) DSCP (111000) decimal value 56.
`default`	Default DSCP (000000) decimal value 0.
`ef`	EF DSCP (101110) decimal value 46.
`precedence`	Match packets with given precedence value.
`<0-7>`	Enter precedence value 0-7.
`critical`	Match packets with critical precedence (5).
`flash`	Match packets with flash precedence (3).
`flashoverride`	
	Match packets with flash override precedence (4).
`immediate`	Match packets with immediate precedence (2).
`internet`	Match packets with internetwork control precedence (6).
`network`	Match packets with network control precedence (7).

`priority`	Match packets with priority precedence (1).
`routine`	Match packets with routine precedence (0).
`fragments`	Check non-initial fragments.
`vlan`	Match packets with given VLAN identifier.
`<1-4094>`	Enter VLAN identifier.
`inner-vlan`	Match packets with given inner VLAN identifier.
`<1-4094>`	Enter inner-VLAN identifier.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).
`redirect-to-port`	
	Redirect the packet (in-direction only)
`IFNAME`	Interface name to which packet to be redirected (switchport only)

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-icmp
(config-ip-acl)#200 permit icmp any any
```


© 2021 IP Infusion Inc. Proprietary

ip access-list remark

Use this command to add a description to a named IPv4 access control list (ACL).

Use the `no` form of this command to remove an ACL description.

Command Syntax

```
remark LINE
no remark
```

Parameters

`LINE`	ACL description up to 100 characters.

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#remark permit the inside admin address
(config-ip-acl)#exit

(config)#ip access-list mylist
(config-ip-acl)#no remark
(config-ip-acl)#exit
```

ip access-list resequence

Use this command to modify the sequence numbers of an IP access list specification.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting sequence number.
`INCREMENT`	Sequence number increment steps.

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#resequence 5 5
(config-ip-acl)#end
```


© 2021 IP Infusion Inc. Proprietary

ip access-list tcp|udp

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming packet based on the criteria specified match criteria.

This form of this command filters packets based on source and destination IP address along with protocol (TCP or UDP) and port.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|drip|echo
  |exec|finger|ftp |ftp- data|gopher|hostname|ident|irc|klogin|kshell|login
  |lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|
  uucp|whois|www)| range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|
  drip|echo|exec|finger|ftp|ftp-data|gopher|hostname|ident|irc|klogin|kshell|login
  |lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12|
  af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4|
  cs5| cs6| cs7| default| ef)) |(precedence (<0-7>| critical| flash |
  flashoverride| immediate| internet| network| priority| routine)) |)
  ({ack|established|fin|psh|rst|syn|urg}|) (fragments|)(vlan <1-4094>|)(inner-vlan
  <1-4094>|)(log|) (sample|)((redirect-to-port IFNAME)|)

(<1-268435453>|) (deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  ((eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard|dnsix|domain|
  echo|isakmp|mobile-ip |nameserver | netbios-dgm | netbios-ns| netbios-ss|non500-
  isakmp |ntp |pim-auto- rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp
  |time|who|xdmcp) | range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) ((eq|gt |lt|neq)(<0-65535> |biff |bootpc |bootps| discard| dnsix|
  domain| echo| isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
  ss|non500-isakmp |ntp|pim-auto- rp| snmp| snmptrap| sunrpc| syslog| tacacs| talk|
  tftp| time| who| xdmcp) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12|
  af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4|
  cs5| cs6| cs7| default| ef)) | (precedence (<0-7>| critical| flash |
  flashoverride| immediate| internet| network| priority| routine))|)
  (fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|) (log|) (sample|)

no (<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any)((eq|gt|lt|neq) (<0-65535>| bgp| chargen| cmd| daytime| discard|
  domain| drip| echo|exec|finger|ftp |ftp- data |gopher |hostname| ident| irc|
  klogin| kshell|login|lpd|nntp|pim-auto- rp |pop2 |pop3 |smtp| ssh| sunrpc| tacacs
  |talk|telnet|time|uucp|whois|www) | range <0-65535> <0-65535>|) (A.B.C.D/
  M|A.B.C.D A.B.C.D|host A.B.C.D|any)((eq|gt|lt|neq) (<0-65535> |bgp |chargen |cmd
  |daytime|discard|domain|drip|echo|exec|finger|ftp|ftp-data| gopher| hostname|
  ident| irc| klogin| kshell| login| lpd| nntp| pim-auto-rp | pop2| pop3| smtp |ssh
  |sunrpc|tacacs|talk|telnet|time|uucp|whois|www) | range <0-65535> <0-65535>|)
  ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42|
  af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>|
  critical| flash | flashoverride| immediate| internet| network| priority|
```

```
  routine)) |) ({ack|established|fin|psh|rst|syn|urg}|) (fragments|)(vlan <1-
  4094>|)(inner-vlan <1-4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|)
no (<1-268435453>|)(deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  ((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix| domain| echo|
  isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|
  ntp|pim-auto- rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xdmcp) |
  range <0-65535> <0-65535>|)(A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D| any)
  ((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix| domain|echo|
  isakmp|mobile- ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|
  ntp|pim-auto- rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xdmcp) |
  range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12| af13| af21| af22| af23|
  af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default|
  ef)) | (precedence (<0-7>| critical| flash | flashoverride| immediate| internet|
  network| priority| routine)) |) (fragments|)(vlan <1-4094>|)(inner-vlan <1-
  4094>|) (log|) (sample|)((redirect-to-port IFNAME)|)
```

Parameters

`<1-268435453>`	IPv4 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`tcp`	Transmission Control Protocol.
`udp`	User Datagram Protocol.
`A.B.C.D/M`	Source or destination IP prefix and length.
`A.B.C.D A.B.C.D`	Source or destination IP address and mask.
`host A.B.C.D`	Source or destination host IP address.
`any`	Any source or destination IP address.
`eq`	Source or destination port equal to.
`gt`	Source or destination port greater than.
`lt`	Source or destination port less than.
`neq`	Source or destination port not equal to.
`<0-65535>`	Source or destination port number.
`range`	Range of source or destination port numbers:
`<0-65535>`	Lowest value in the range.
`<0-65535>`	Highest value in the range.
`bgp`	Border Gateway Protocol.
`chargen`	Character generator.
`cmd`	Remote commands.
`daytime`	Daytime.
`discard`	Discard.
`domain`	Domain Name Service.
`drip`	Dynamic Routing Information Protocol.
`echo`	Echo.

© 2021 IP Infusion Inc. Proprietary

`exec`	EXEC.
`finger`	Finger.
`ftp`	File Transfer Protocol.
`ftp-data`	FTP data connections.
`gopher`	Gopher.
`hostname`	NIC hostname server.
`ident`	Ident Protocol.
`irc`	Internet Relay Chat.
`klogin`	Kerberos login.
`kshell`	Kerberos shell.
`login`	Login.
`lpd`	Printer service.
`nntp`	Network News Transport Protocol.
`pim-auto-rp`	PIM Auto-RP.
`pop2`	Post Office Protocol v2.
`pop3`	Post Office Protocol v3.
`smtp`	Simple Mail Transport Protocol.
`ssh`	Secure Shell.
`sunrpc`	Sun Remote Procedure Call.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`telnet`	Telnet.
`time`	Time.
`uucp`	UNIX-to-UNIX Copy Program.
`whois`	WHOIS/NICNAME
`www`	World Wide Web.
`nntp`	Range of source or destination port numbers:
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34

af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).
priority	Match packets with priority precedence (1).
routine	Match packets with routine precedence (0).
ack	Match on the Acknowledgment (ack) bit.
established	Matches only packets that belong to an established TCP connection.
fin	Match on the Finish (fin) bit.
psh	Match on the Push (psh) bit.
rst	Match on the Reset (rst) bit.
syn	Match on the Synchronize (syn) bit.
urg	Match on the Urgent (urg) bit.
biff	Biff.
bootpc	Bootstrap Protocol (BOOTP) client.
bootps	Bootstrap Protocol (BOOTP) server.
discard	Discard.
dnsix	DNSIX security protocol auditing.
domain	Domain Name Service.
echo	Echo.
isakmp	Internet Security Association and Key Management Protocol.
mobile-ip	Mobile IP registration.
nameserver	IEN116 name service.
netbios-dgm	Net BIOS datagram service.

© 2021 IP Infusion Inc. Proprietary

`netbios-ns`	Net BIOS name service.
`netbios-ss`	Net BIOS session service.
`non500-isakmp`	Non500-Internet Security Association and Key Management Protocol.
`ntp`	Network Time Protocol.
`pim-auto-rp`	PIM Auto-RP.
`snmp`	Simple Network Management Protocol.
`snmptrap`	SNMP Traps.
`sunrpc`	Sun Remote Procedure Call.
`syslog`	System Logger.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`tftp`	Trivial File Transfer Protocol.
`time`	Time.
`who`	Who service.
`xdmcp`	X Display Manager Control Protocol.
`fragments`	Check non-initial fragments.
`vlan`	Match packets with given VLAN identifier.
`<1-4094>`	Enter VLAN identifier.
`inner-vlan`	Match packets with given inner VLAN identifier.
`<1-4094>`	Enter inner-VLAN identifier.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).
`IFNAME`	Interface name to which packet to be redirected (switchport only)
`redirect-to-port`	Redirect the packet (in-direction only)

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-02
(config-ip-acl)#deny udp any any eq tftp
(config-ip-acl)#deny tcp any any eq ssh
(config-ip-acl)#end
```

ipv6 access-group

Use this command to attach an IPv6 access list to an interface to filter incoming or outgoing packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

Note: To attach an IPv6 access-group on interface, the IPv6 TCAM group should be enabled. To enable ingress-IPv6 /egress-IPv6, see the hardware-profile filter (XGS) command.

The `time-range` parameter is optional. If used, the access-group is tied to the timer specified.

After the access-group has been configured with the time-range, to detach the access-group from the time-range, use the `no` form of this command with a time-range parameter as shown in the syntax and examples below.

To delete the access-group, use the `no` form of this command without a time-range.

Note: To attach IPv6 ACL in the ingress direction ingress-ipv6 TCAM group needs to be enabled. See the hardware-profile filter (Qumran) command for details.

Command Syntax

```
ipv6 access-group NAME in (time-range TR_NAME|)
no ipv6 access-group NAME in (time-range TR_NAME|)
```

Parameters

`NAME`	Access list name.
`TR_NAME`	Time range name set with the time-range command.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3. The `time-range` parameter was added in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#permit ipv6 any any
(config-ipv6-acl)#exit
(config)#hardware-profile filter ingress-ipv6 enable

(config)#interface xe3
(config-if)#ipv6 access-group mylist in
```


© 2021 IP Infusion Inc. Proprietary

```
(config)#interface xe3
(config-if)#no ipv6 access-group mylist in

(config)#interface xe3
(config-if)#ipv6 access-group mylist in time-range TIMER1

(config)#interface xe3
(config-if)#no ipv6 access-group mylist in time-range TIMER1
```

ipv6 access-list

Use this command to define a IPv6 access control list (ACL) that determines whether to accept or drop an incoming IPv6 packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Use the `no` form of this command to remove an ACL.

Note: For IPv6 routing protocols need neighbor discovery for the session to establish. Applying Ipv6 acls implicitly drops all the icmpv6 packets, thereby affecting the protocol sessions. To overcome this problem, implicit icmpv6 permit rule is added in the IPv6 acls.

If required behavior is to deny the icmpv6, implicit rule can be deleted.

For example,

To create an ipv6 acl, execute the following:

```
(config)#ipv6 access-list ipv6-acl
#show ipv6 access-lists
IPv6 access list ip1
268435453 permit icmpv6 any any
```

To delete this rule, execute the following:

```
(config)#ipv6 access-list ipv6-acl
(config-ipv6-acl)# no 268435453 permit icmpv6 any any

#show ipv6 access-lists
IPv6 access list ip1
```

Command Syntax

```
ipv6 access-list NAME
no ipv6 access-list NAME
```

Parameters

`NAME`	Access-list name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Implicit rule is introduced in OcNOS version 2.0.

© 2021 IP Infusion Inc. Proprietary

Examples

```
#configure terminal
(config)#ipv6 access-list ipv6-acl-01
(config-ipv6-acl)#exit
```

ipv6 access-list default

Use this command to modify the default rule action of access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the IPv6 packets not matching any of the user defined rules match default rule.

Command Syntax

```
default (deny-all|permit-all) (log|) (sample|)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ipv6-acl-01
(config-ipv6-acl)#default permit-all sample
```


© 2021 IP Infusion Inc. Proprietary

ipv6 access-list filter

Use this command to define an access-control entry in an access control list (ACL) that determines whether to accept or drop an IPv6 packet based on the criteria specified. This form of this command filters packets based on:

- Protocol
- Source IP address
- Destination IP address

Use the `no` form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: For IPv6 source and destination address filters, only the network part from the address (upper 64 bits) is supported due to hardware restriction. If the address length is more than 64 bits, it cannot be applied on the interfaces but it can be used with distributed list in control plane protocols.

Command Syntax

```
(<1-268435453>|) (deny|permit)(<0-255>|ahp|any|eigrp|esp|gre|ipipv6|ipcomp
  |ipv6ipv6|ospf|pim|rsvp|vrrp) (X:X::X:X/ M|X:X::X:X X:X::X:X|host X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) (dscp (<0-63>|af11| af12| af13| af21| af22|
  af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
  default| ef )|) (flow-label<0-1048575>|) (fragments|) (vlan <1-4094>|)(inner-vlan
  <1-4094>|) (log|) (sample|)((redirect-to-port IFNAME)|)

no (<1-268435453>|)(deny|permit)(<0-255>|ahp|any|eigrp|esp|gre|ipipv6|ipcomp
  |ipv6ipv6|ospf|pim|rsvp|vrrp) (X:X::X:X/ M|X:X::X:X X:X::X:X|host X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) (dscp (<0-63>|af11| af12| af13| af21| af22|
  af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
  default| ef )|) (flow-label<0-1048575>|) (fragments|) (vlan <1-4094>|)(inner-vlan
  <1-4094>|) (log|) (sample|)((redirect-to-port IFNAME)|)

no (<1-268435453>)
```

Parameters

`<1-268435453>`	IPv4 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`<0-255>`	IANA assigned protocol number.
`any`	Any protocol packet.
`ahp`	Authentication Header packet.
`eigrp`	Enhanced Interior Gateway Routing Protocol packet.
`esp`	Encapsulating Security Payload packet.
`gre`	Generic Routing Encapsulation packet.
`ipipv6`	IPv4 over IPv6 Encapsulation packet.
`ipcomp`	IP Payload Compression Protocol packet.
`ipv6ipv6`	IPv6 over IPv6 Encapsulation packet.

`ospf`	Open Shortest Path First packet.
`pim`	Protocol Independent Multicast packet
`rsvp`	Resource Reservation Protocol packet. `v`
`rrp`	Virtual Router Redundancy Protocol packet.
`X:X::X:X/M`	Source Address with network mask length.
`X:X::X:X X:X::X:X`	Source Address with wild card mask.
`any`	Any source address.
`X:X::X:X/M`	Destination address with network mask length.
`X:X::X:X X:X::X:X`	Destination address with wild card mask.
`any`	Match any destination IP address.
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34
`af42`	AF42 DSCP (100100) decimal value 36.
`af43`	AF43 DSCP (100110) decimal value 38.
`cs1`	CS1 (precedence 1) DSCP (001000) decimal value 8.
`cs2`	CS2 (precedence 2) DSCP (010000) decimal value 16.
`cs3`	CS3 (precedence 3) DSCP (011000) decimal value 24.
`cs4`	CS4 (precedence 4) DSCP (100000) decimal value 32.
`cs5`	CS5 (precedence 5) DSCP (101000) decimal value 40.
`cs6`	CS6 (precedence 6) DSCP (110000) decimal value 48.
`cs7`	CS7 (precedence 7) DSCP (111000) decimal value 56.
`default`	Default DSCP (000000) decimal value 0.
`ef`	EF DSCP (101110) decimal value 46.
`vlan`	Match packets with given VLAN identifier.
`<1-4094>`	VLAN identifier.
`inner-vlan`	Match packets with given inner VLAN identifier.
`<1-4094>`	Inner-VLAN identifier.

© 2021 IP Infusion Inc. Proprietary

`redirect-to-port`	
	Redirect the packet (in-direction only)
`IFNAME`	Interface name to which packet to be redirected

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list ipv6-acl-01
(config-ip-acl)#permit ipipv6 any any
(config-ip-acl)#end
```

ipv6 access-list fragments

Use this command to permit or deny all the IPv6 fragments.

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|)
no (<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|)
```

Parameters

`<1-268435453>`	IPv6 ACL sequence number.
`fragments`	Check non-initial fragments.
`deny-all`	Specify packets to reject.
`permit-all`	Specify packets to forward.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#fragments deny-all
```


© 2021 IP Infusion Inc. Proprietary

ipv6 access-list icmpv6

Use this command to permit or deny IPv6 ICMP packets with the given source and destination IPv6 address, DSCP value, VLAN identifier, inner VLAN identifier, fragments, and flow label.

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (icmpv6) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/ M|X:X::X:X X:X::X:X|any) (beyond-scope| destination-unreachable| echo-reply|
  echo-request| header| hop-limit| mld-query| mld-reduction| mld-report| nd-na| nd-ns| next-
  header| no-admin| no-route| packet-too-big| parameter-option| parameter-problem| port-
  unreachable| reassembly-timeout| redirect| renum-command| renum-result| renum-seq-number|
  router-advertisement| router-renumbering| router-solicitation| time-exceeded| unreachable |
  (<0-255> (<0-255>|)|)) (dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32|
  af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef)|) (flow-
  label <0-1048575>|) (fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|) (log|)
  (sample|)((redirect-to-port IFNAME)|)

no (<1-268435453>|)(deny|permit) (icmpv6) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) (beyond-scope| destination-unreachable| echo-reply|
  echo-request| header| hop-limit| mld-query| mld-reduction| mld-report| nd-na| nd-ns| next-
  header| no-admin| no-route| packet-too-big| parameter-option| parameter-problem| port-
  unreachable| reassembly-timeout| redirect| renum-command| renum-result| renum-seq-number|
  router-advertisement| router-renumbering| router-solicitation| time-exceeded| unreachable |
  (<0-255> (<0-255>|)|)) (dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32|
  af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef )|) (flow-
  label <0-1048575>|) (fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|)(log|)
  (sample|)((redirect-to-port IFNAME)|)
```

Parameters

`<1-268435453>`	IPv6 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`icmpv6`	Internet Control Message Protocol packet.
`X:X::X:X/M`	Source Address with network mask length.
`X:X::X:X X:X::X:X`	Source Address with wild card mask.
`any`	Any source address.
`X:X::X:X/M`	Destination address with network mask length.
`X:X::X:X X:X::X:X`	Destination address with wild card mask.
`any`	Any destination address
`beyond-scope`	Destination beyond scope
`destination-unreachable`	

	Destination address is unreachable
`echo-reply`	Echo reply
`echo-request`	Echo request (ping)
`header`	Parameter header problems
`hop-limit`	Hop limit exceeded in transit
`mld-query`	Multicast Listener Discovery Query
`mld-reduction`	Multicast Listener Discovery Reduction
`mld-report`	Multicast Listener Discovery Report
`nd-na`	Neighbor discovery neighbor advertisements
`nd-ns`	Neighbor discovery neighbor solicitations
`next-header`	Parameter next header problems
`no-admin`	Administration prohibited destination
`no-route`	No route to destination
`packet-too-big`	Packet too big
`parameter-option`	
	Parameter option problems
`parameter-problem`	
	All parameter problems
`port-unreachable`	
	Port unreachable
`reassembly-timeout`	
	Reassembly timeout
`redirect`	Neighbor redirect
`renum-command`	Router renumbering command
`renum-result`	Router renumbering result
`renum-seq-number`	
	Router renumbering sequence number reset
`router-advertisement`	
	Neighbor discovery router advertisements
`router-renumbering`	
	All router renumbering
`router-solicitation`	
	Neighbor discovery router solicitations
`time-exceeded`	All time exceeded messages
`unreachable`	All unreachable
`<0-255>`	ICMPv6 message type
`<0-255>`	ICMPv6 message code
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.

© 2021 IP Infusion Inc. Proprietary

`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34
`af42`	AF42 DSCP (100100) decimal value 36.
`af43`	AF43 DSCP (100110) decimal value 38.
`cs1`	CS1 (precedence 1) DSCP (001000) decimal value 8.
`cs2`	CS2 (precedence 2) DSCP (010000) decimal value 16.
`cs3`	CS3 (precedence 3) DSCP (011000) decimal value 24.
`cs4`	CS4 (precedence 4) DSCP (100000) decimal value 32.
`cs5`	CS5 (precedence 5) DSCP (101000) decimal value 40.
`cs6`	CS6 (precedence 6) DSCP (110000) decimal value 48.
`cs7`	CS7 (precedence 7) DSCP (111000) decimal value 56.
`default`	Default DSCP (000000) decimal value 0.
`ef`	EF DSCP (101110) decimal value 46.
`flow-label`	IPv6 Flow-label.
`<0-1048575>`	IPv6 Flow-label value.
`fragments`	Check non-initial fragments.
`vlan`	Match packets with given VLAN identifier.
`<1-4094>`	Enter VLAN identifier.
`inner-vlan`	Match packets with given inner VLAN identifier.
`<1-4094>`	Enter inner-VLAN identifier.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).
`redirect-to-port`	Redirect the packet (in-direction only)
`IFNAME`	Interface name to which packet to be redirected (switchport only)

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#200 permit icmpv6 any any fragments
```


© 2021 IP Infusion Inc. Proprietary

ipv6 access-list remark

Use this command to add a description to an IPv6 access control list (ACL).

Use the `no` form of this command to remove an access control list description.

Command Syntax

```
remark LINE
no remark
```

Parameters

`LINE`	ACL description up to 100 characters.

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)# remark Permit the inside admin address
```

ipv6 access-list resequence

Use this command to modify the sequence numbers of an IPv6 access list specification.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting Sequence number.
`INCREMENT`	Sequence number increment steps.

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#resequence 15 15
```


© 2021 IP Infusion Inc. Proprietary

ipv6 access-list sctp

Use this command to allow ACL to permit or deny SCTP packets based on the given source and destination IPV6 address. Even DSCP, VLAN identifier, inner VLAN identifier, flow label, and fragment can be configured to permit or deny with the given values.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) (deny|permit) (sctp) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>) | (range <0-65535> <0-
  65535>)| (fragments)| } (dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31|
  af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)|)
  ((flow-label <0-1048575>)|)(fragments|)(vlan <1-4094>|)(inner-vlan <1-4094>|)
  (log|) (sample|)((redirect-to-port IFNAME)|)
no (<1-268435453>|) (deny|permit) (sctp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>) | (range <0-65535>
  <0-65535>)| (fragments)| } (dscp (<0-63>| af11| af12| af13| af21| af22| af23|
  af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default|
  ef)|) ((flow-label <0-1048575>)|) (fragments|)(vlan <1-4094>|)(inner-vlan <1-
  4094>|)(log|) (sample|)((redirect-to-port IFNAME)|)
```

Parameters

`<1-268435453>`	IPv6 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`sctp`	Stream Control Transmission Protocol packet.
`X:X::X:X/M`	Source address with network mask length.
`X:X::X:X`	Source address with wild card mask.
`X:X::X:X`	Source address's wild card mask (ignored bits).
`any`	Any source address.
`X:X::X:X/M`	Destination address with network mask length.
`X:X::X:X`	Destination address with wild card mask.
`X:X::X:X`	Destination address's wild card mask (ignored bits).
`any`	Any destination address.
`eq`	Source or destination port equal to.
`gt`	Source or destination port greater than.
`lt`	Source or destination port less than.
`neq`	Source or destination port not equal to.
`<0-65535>`	Source or destination port number.
`range`	Range of source or destination port numbers:
`<0-65535>`	Lowest value in the range.

<0-65535>	Highest value in the range.
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
flow-label	IPv6 Flow-label.
<0-1048575>	IPv6 Flow-label value.
fragments	Check non-initial fragments.
vlan	Match packets with given VLAN identifier.
<1-4094>	Enter VLAN identifier.
inner-vlan	Match packets with given inner VLAN identifier.
<1-4094>	Enter inner-VLAN identifier.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).
redirect-to-port	Redirect the packet (in-direction only)
IFNAME	Interface name to which packet to be redirected (switchport only)

© 2021 IP Infusion Inc. Proprietary

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#200 permit sctp any any fragments
```

ipv6 access-list tcp|udp

Use this command to define a IPv6 access control list (ACL) specification that determines whether to accept or drop an incoming IPv6 packet based on the criteria that you specify. This form of this command filters packets based on source and destination IPv6 address along with protocol (TCP or UDP) and port.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (tcp) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|
  discard|domain|drip|echo|exec|finger|ftp |ftp-
  data|gopher|hostname|ident|irc|klogin|kshell|login|lpd|nntp|pim-auto-
  rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|uucp|whois|www)| (range <0-
  65535> <0-65535>)| (fragments) |} (((dscp (<0-63>| af11| af12| af13| af21| af22|
  af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7|
  default| ef ))|) (flow-label <0-1048575>|)
  ({ack|established|fin|psh|rst|syn|urg}|)) (vlan <1-4094>|) (inner-vlan <1-
  4094>|) (log|) (sample|)

(<1-268435453>|)(deny|permit) (tcp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  {(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|drip|
  echo|exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|kshell
  |login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www) | (range <0-65535> <0-65535>)} (X:X::X:X/M|X:X::X:X
  X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|
  drip|echo|exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|kshell|
  login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|
  talk|telnet|time|uucp|whois|www) | (range <0-65535> <0-65535>)|} (((dscp (<0-
  63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1|
  cs2| cs3| cs4| cs5| cs6| cs7| default| ef ))|) (flow-label <0-1048575>|)
  ({ack|established|fin|psh|rst|syn|urg}|)) (vlan <1-4094>|) (inner-vlan <1-
  4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|)

(<1-268435453>|)(deny|permit) (udp) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard
  |dnsix|domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
  ss|non500-isakmp|ntp|pim-auto-rp|snmp|snmptrap|sunrpc|syslog|
  tacacs|talk|tftp|time|who|xdmcp) | (range <0-65535> <0-65535>) | (fragments) |}
  ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42|
  af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ))|) (flow-label <0-
  1048575>|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|) (sample|) ((redirect-
  to-port IFNAME)|)

(<1-268435453>|)(deny|permit) (udp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  {(eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard|dnsix
  |domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
  ss|non500-isakmp|ntp|pim-auto-rp|snmp|snmptrap|sunrpc|syslog|
  tacacs|talk|tftp|time|who|xdmcp) | (range <0-65535> <0-65535>) } (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard|
  dnsix|domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
  ss|non500-isakmp|ntp|pim-auto-rp|snmp|snmptrap|sunrpc|
```

 © 2021 IP Infusion Inc. Proprietary

```
  syslog|tacacs|talk|tftp|time|who|xdmcp) | (range <0-65535> <0-65535>) } ((dscp
  (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43|
  cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ))|) (flow-label <0-1048575>|)
  (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|) (sample|) ((redirect-to-port
  IFNAME)|)
no (<1-268435453>|)(deny|permit) (tcp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|
  daytime|discard|domain|drip|echo|exec|finger|ftp |ftp-data|gopher|hostname
  |ident|irc|klogin|kshell|login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc
  |tacacs|talk|telnet|time|uucp|whois|www)| (range <0-65535> <0-65535>)|
  (fragments) |} (((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32|
  af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ))|)
  (flow-label <0-1048575>|) ({ack|established|fin|psh|rst|syn|urg}|)) (vlan <1-
  4094>|) (inner-vlan <1-4094>|) (log|) (sample|)
no (<1-268435453>|)(deny|permit) (tcp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  {(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|drip
  |echo|exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|kshell
  |login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www) | (range <0-65535> <0-65535>)} (X:X::X:X/M|X:X::X:X
  X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|
  domain|drip|echo|exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|
  kshell|login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk
  |telnet|time|uucp|whois|www) | (range <0-65535> <0-65535>)|} (((dscp (<0-63>|
  af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2|
  cs3| cs4| cs5| cs6| cs7| default| ef ))|) (flow-label <0-1048575>|)
  ({ack|established|fin|psh|rst|syn|urg}|)) (vlan <1-4094>|) (inner-vlan <1-
  4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|
no (<1-268435453>|)(deny|permit) (udp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-
  65535>|biff|bootpc|bootps|discard|dnsix|domain|echo|isakmp|mobile-
  ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|ntp|pim-auto-
  rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xdmcp) | (range <0-
  65535> <0-65535>) | (fragments) |} ((dscp (<0-63>| af11| af12| af13| af21| af22|
  af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7|
  default| ef ))|) (flow-label <0-1048575>|) (vlan <1-4094>|) (inner-vlan <1-
  4094>|) (log|) (sample|) ((redirect-to-port IFNAME)|)
no (<1-268435453>|)(deny|permit) (udp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  {(eq|gt|lt|neq) (<0-
  65535>|biff|bootpc|bootps|discard|dnsix|domain|echo|isakmp|mobile-
  ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|ntp|pim-auto-
  rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xdmcp) | (range <0-
  65535> <0-65535>) } (X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-
  65535>|biff|bootpc|bootps|discard|dnsix|domain|echo|isakmp|mobile-
  ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|ntp|pim-auto-
  rp|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xdmcp) | (range <0-
  65535> <0-65535>) } ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31|
  af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ))|)
  (flow-label <0-1048575>|) (vlan <1-4094>|) (inner-vlan <1-4094>|) (log|)
  (sample|) ((redirect-to-port IFNAME)|)
```

Parameters

`<1-268435453>` IPv6 ACL sequence number.

`deny`	Drop the packet.
`permit`	Accept the packet.
`tcp`	Transmission Control Protocol.
`udp`	User Datagram Protocol.
`X:X::X:X/M`	Source or destination IPv6 prefix and length.
`X:X::X:X X:X::X:X`	Source or destination IPv6 address and mask.
`host X:X::X:X`	A single source or destination host IPv6 address.
`any`	Any source or destination IPv6 address.
`eq`	Source or destination port equal to.
`gt`	Source or destination port greater than.
`lt`	Source or destination port less than.
`neq`	Source or destination port not equal to.
`<0-65535>`	Source or destination port number.
`range`	Range of source or destination port numbers:
`<0-65535>`	Lowest value in the range.
`<0-65535>`	Highest value in the range.
`ftp`	File Transfer Protocol (21).
`ssh`	Secure Shell (22).
`telnet`	Telnet (23).
`www`	World Wide Web (HTTP 80).
`tftp`	Trivial File Transfer Protocol (69).
`bootp`	Bootstrap Protocol (BOOTP) client (67).
`bgp`	Border Gateway Protocol.
`chargen`	Character generator.
`cmd`	Remote commands.
`daytime`	Daytime.
`discard`	Discard.
`domain`	Domain Name Service.
`drip`	Dynamic Routing Information Protocol.
`echo`	Echo.
`exec`	EXEC.
`finger`	Finger.
`ftp`	File Transfer Protocol.
`ftp-data`	FTP data connections.
`gopher`	Gopher.
`hostname`	NIC hostname server.
`ident`	Ident Protocol.
`irc`	Internet Relay Chat.

© 2021 IP Infusion Inc. Proprietary

`klogin`	Kerberos login.
`kshell`	Kerberos shell.
`login`	Login.
`lpd`	Printer service.
`nnt`	Network News Transport Protocol.
`pim-auto-rp`	PIM Auto-RP.
`pop2`	Post Office Protocol v2.
`pop3`	Post Office Protocol v3.
`smtp`	Simple Mail Transport Protocol.
`ssh`	Secure Shell.
`sunrpc`	Sun Remote Procedure Call.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`telnet`	Telnet.
`time`	Time.
`uucp`	UNIX-to-UNIX Copy Program.
`whois`	WHOIS/NICNAME
`www`	World Wide Web.
`nntp`	Range of source or destination port numbers:
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34
`af42`	AF42 DSCP (100100) decimal value 36.
`af43`	AF43 DSCP (100110) decimal value 38.
`cs1`	CS1 (precedence 1) DSCP (001000) decimal value 8.
`cs2`	CS2 (precedence 2) DSCP (010000) decimal value 16.
`cs3`	CS3 (precedence 3) DSCP (011000) decimal value 24.
`cs4`	CS4 (precedence 4) DSCP (100000) decimal value 32.
`cs5`	CS5 (precedence 5) DSCP (101000) decimal value 40.
`cs6`	CS6 (precedence 6) DSCP (110000) decimal value 48.

© 2021 IP Infusion Inc. Proprietary

cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).
priority	Match packets with priority precedence (1).
routine	Match packets with routine precedence (0).
ack	Match on the Acknowledgment (ack) bit.
established	Matches only packets that belong to an established TCP connection.
fin	Match on the Finish (fin) bit.
psh	Match on the Push (psh) bit.
rst	Match on the Reset (rst) bit.
syn	Match on the Synchronize (syn) bit.
urg	Match on the Urgent (urg) bit.
biff	Biff.
bootpc	Bootstrap Protocol (BOOTP) client.
bootps	Bootstrap Protocol (BOOTP) server.
discard	Discard.
dnsix	DNSIX security protocol auditing.
domain	Domain Name Service.
echo	Echo.
isakmp	Internet Security Association and Key Management Protocol.
mobile-ip	Mobile IP registration.
nameserver	IEN116 name service.
netbios-dgm	Net BIOS datagram service.
netbios-ns	Net BIOS name service.
netbios-ss	Net BIOS session service.
non500-isakmp	Non500-Internet Security Association and Key Management Protocol.
ntp	Network Time Protocol.
pim-auto-rp	PIM Auto-RP.
snmp	Simple Network Management Protocol.
snmptrap	SNMP Traps.
sunrpc	Sun Remote Procedure Call.

© 2021 IP Infusion Inc. Proprietary

`syslog`	System Logger.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`tftp`	Trivial File Transfer Protocol.
`time`	Time.
`who`	Who service.
`xdmcp`	X Display Manager Control Protocol.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).
`flow-label`	IPv6 Flow-label.
`<0-1048575>`	IPv6 Flow-label value.
`fragments`	Check non-initial fragments.
`vlan`	Match packets with given VLAN identifier.
`<1-4094>`	Enter VLAN identifier.
`inner-vlan`	Match packets with given inner VLAN identifier.
`<1-4094>`	Enter inner-VLAN identifier.
`redirect-to-port`	Redirect the packet (in-direction only)
`IFNAME`	Interface name to which packet to be redirected (switchport only)

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#deny udp any eq tftp
(config-ipv6-acl)#deny tcp fd22:bf66:78a4:10a2::/64 fdf2:860a:746a:e49c::/64
eq ssh
```

line vty

Use this command to move or change to ALL LINE VTY mode.

Command Syntax

```
line vty
```

Parameters

NA

Command Mode

Configure mode

Applicability

This command was introduced from OcNOS version 1.3.8

Examples

The following example shows entering all line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty
(config-all-line)#exit
```


© 2021 IP Infusion Inc. Proprietary

mac access-group

Use this command to attach a MAC access list to an interface to filter incoming packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

The `time-range` parameter is optional. If used, the access-group is tied to the timer specified.

After the access-group has been configured with the time-range, to detach the access-group from the time-range, use the `no` form of this command with a time-range parameter as shown in the syntax and examples below.

To delete the access-group, use the `no` form of this command without a time-range.

Note: An access-group on egress access-group on egress direction uses the TCAM group used by the QoS output service policy. Therefore, actions are unpredictable when conflicting matches are configured on same interface. IP Infusion Inc. recommends avoiding such a configuration. Otherwise, you need to configure the priority (in QoS) or the sequence number (in ACL) carefully to handle such cases.

Command Syntax

```
mac access-group NAME (in|out) (in|out) (time-range TR_NAME|)
no mac access-group NAME (in|out) (time-range TR_NAME|)
```

Parameters

`NAME`	Access list name.
`in`	Filter incoming packets.
`out`	Filter outgoing packets
`TR_NAME`	Time range name set with the time-range command

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3. The `time-range` parameter was added in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)#permit any any
(config-mac-acl)#exit

(config)#hardware-profile filter ingress-l2-ext enable
```

```
(config)#interface xe3
(config-if)#mac access-group mylist in
(config-if)#exit

(config)#interface xe3
(config-if)#mac access-group mylist in time-range TIMER1
(config-if)#exit

(config)#interface xe3
(config-if)#no mac access-group mylist in time-range TIMER1
(config-if)#exit

(config)#interface xe3
(config-if)#no mac access-group mylist in
(config-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

mac access-list

Use this command to define a MAC access control list (ACL) that determines whether to accept or drop an incoming packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Use the `no` form of this command to remove the ACL.

Command Syntax

```
mac access-list NAME
no mac access-list NAME
```

Parameters

`NAME`	Access-list name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#exit
```

mac access-list default

Use this command to modify the default rule action of access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the packets not matching any of the user defined rules match default rule.

Command Syntax

```
default (deny-all|permit-all) (log|) (sample|)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#default permit-all sample
```


© 2021 IP Infusion Inc. Proprietary

mac access-list filter

Use this command to define an access control entry (ACE) in a MAC access control list (ACL) that determines whether to permit or deny packets with the given source and destination MAC, ethertype, CoS, and VLAN identifiers.

Use the `no` form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (aarp|appletalk|decnet-
  iv|diagnostic|etype-6000|etype-8042 |ip4|ip6|mpls|lat|lavc-sca|mop-console|mop-
  dump|vines-echo|WORD|) (cos <0-7>|)(vlan <1-4094>|) (inner-vlan <1-4094>|) (log|)
  (sample|)
no (<1-268435453>|)(deny|permit) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (aarp|appletalk|decnet-
  iv|diagnostic|etype-6000|etype-8042 |ip4|ip6|mpls|lat|lavc-sca|mop-console|mop-
  dump|vines-echo|WORD|) (cos <0-7>|)(vlan <1-4094>|) (inner-vlan <1-4094>|) (log|)
  (sample|)
no (<1-268435453>)
```

Parameters

`deny`	Drop the packet.
`permit`	Accept the packet.
`<1-268435453>`	IPv4 ACL sequence number.
`any`	Source/Destination any.
`XX-XX-XX-XX-XX-XX`	Source/Destination MAC address (Option 1).
`XX:XX:XX:XX:XX:XX`	Source/Destination MAC address (Option 2).
`XXXX.XXXX.XXXX`	Source/Destination MAC address (Option 3).
`XX-XX-XX-XX-XX-XX`	Source/Destination wildcard (Option1).

`XX:XX:XX:XX:XX:XX`	Source/Destination wildcard (Option2).
`XXXX.XXXX.XXXX`	Source/Destination wildcard (Option3).
`host`	A single source/destination host.
`aarp`	Ethertype - 0x80f3.
`appletalk`	Ethertype - 0x809b.
`decnet-iv`	Ethertype - 0x6003.
`diagnostic`	Ethertype - 0x6005.
`etype-6000`	Ethertype - 0x6000.
`etype-8042`	Ethertype - 0x8042.
`ip4`	Ethertype - 0x0800.
`ip6`	Ethertype - 0x86dd.
`mpls`	Ethertype - 0x8847.
`lat`	Ethertype - 0x6004.
`lavc-sca`	Ethertype - 0x6007.
`mop-console`	Ethertype - 0x6002.
`mop-dump`	Ethertype - 0x6001.
`vines-echo`	Ethertype - 0x0baf.
`WORD`	Any Ethertype value.
`cos <0-7>`	Cos value.
`vlan <1-4094>`	VLAN identifier.
`inner-vlan <1-4094>`	Inner-VLAN identifier.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#permit 0000.1234.1234 0000.0000.0000 any sample
```


© 2021 IP Infusion Inc. Proprietary

mac access-list remark

Use this command to add a description to an MAC access control list (ACL).

Use the `no` form of this command to remove an ACL description.

Command Syntax

```
remark LINE
no remark
```

Parameters

`LINE`	ACL description up to 100 characters.

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)# remark Permit the inside admin address
```

mac access-list resequence

Use this command to modify the sequence numbers of MAC access list specifications.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting sequence number.
`INCREMENT`	Sequence number increment steps.

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)#resequence 15 15
```


© 2021 IP Infusion Inc. Proprietary

show access-lists

Use this command to display access lists.

Command Syntax

```
show access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show access-lists expanded
IP access list Iprule1
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
default deny-all
MAC access list Macrule1
10 permit host 0000.1234.1234 any
default deny-all
IPv6 access list ipv6-acl-01
10 deny ahp 3ffe::/64 4ffe::/64
default deny-all

#show access-lists summary
IPV4 ACL Iprule1
statistics enabled
Total ACEs Configured: 1
Configured on interfaces:
xe3/1 - egress (Router ACL)
Active on interfaces:
xe1/3 - ingress (Router ACL)
MAC ACL Macrule1
statistics enabled
Total ACEs Configured: 0
Configured on interfaces:
Active on interfaces:
IPV6 ACL ipv6-acl-01
statistics enabled
Total ACEs Configured: 2
Configured on interfaces:
xe7/1 - ingress (Router ACL)
Active on interfaces:
```

show access-list log-cache

Use this command to show the ACL logging table entries

Command Syntax

```
show access-lists log-cache
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show access-lists log-cache
2016 Oct 26 12:08:37:xe1/1: 0000.0100.0a00 -> 0000.0100.0b00, ethertype IP
(0x800), proto tcp, vlan 2, 0.0.0.0:0 -> 0.0.0.0:0 ...suppressed 11 times

2016 Oct 26 12:07:51:xe1/1: 0000.0100.0a00 -> 0000.0100.0b00, ethertype IP
(0x800), proto 255, vlan 2, 0.0.0.0 -> 0.0.0.0 ...suppressed 10 times
```


© 2021 IP Infusion Inc. Proprietary

show arp access-lists

Use this command to display ARP access lists.

Command Syntax

```
show arp access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	ARP access-list name.
expanded	Expanded access-list.
summary	Access-list summary.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#show arp access-lists
ARP access list arp1
        remark "arp access-list created"
        10 permit ip any mac any
```

show ip access-lists

Use this command to display IP access list

Command Syntax

```
show ip access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip access-lists
IP access list Iprule2
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
12 deny ip 30.0.0.2 0.0.0.255 182.124.0.3/24
default deny-all

#show ip access-lists summary
IPV4 ACL Iprule3
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa1 - ingress (Port ACL)
sa3 - ingress (Router ACL)
sa8 - ingress (Port ACL)
vlan1.3 - ingress (Router ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
xe3/1 - egress (Router ACL)
Active on interfaces:
sa1 - ingress (Port ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```


© 2021 IP Infusion Inc. Proprietary

show ipv6 access-lists

Use this command to display IPv6 access lists.

Command Syntax

```
show ipv6 access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 access-lists
IPv6 access list ipv6-acl-01
10 deny ahp 3ffe::/64 4ffe::/64
20 permit ahp 78fe::1/48 68fe::1/48
30 permit ahp 3333::1/64 4444::1/48 fragments
40 permit ahp 5555::1/64 4444::1/48 dscp af23
default deny-all

#show ipv6 access-lists summary
IPV6 ACL ipv6-acl-01
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa3 - ingress (Router ACL)
vlan1.3 - ingress (Router ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
Active on interfaces:
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```

© 2021 IP Infusion Inc. Proprietary

show mac access-lists

Use this command to display MAC access lists.

Command Syntax

```
show mac access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

Command Mode

Privileged exec mode and exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac access-lists
MAC access list Macrule2
default deny-all
MAC access list Macrule3
10 permit host 0000.1234.1234 any
20 deny host 1111.1111.AAAA any 65535
30 permit host 2222.2222.AAAA any 65535
40 permit 0000.3333.3333 0000.0000.FFFF 4444.4444.4444 0000.0000.FFFF
default deny-all [match=1126931077]

# show mac access-lists summary
MAC ACL Macrule3
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa3 - ingress (Router ACL)
sa8 - ingress (Port ACL)
vlan1.3 - ingress (Router ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
Active on interfaces:
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```


© 2021 IP Infusion Inc. Proprietary

show running-config aclmgr

Use this command to display the entire access list configurations along with the attachment to interfaces.

Command Syntax

```
show running-config aclmgr (all|)
```

Parameters

`all`	Show running configuration with defaults.

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config aclmgr
ip access-list ip-acl-01
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
12 deny ip 30.0.0.2 0.0.0.255 182.124.0.3/24
mac access-list mac-acl-01
10 permit host 0000.1234.1234 any
20 permit host 0000.1111.AAAA any ipv4 cos 3 vlan 3
!
ipv6 access-list ipv6-acl-01
10 deny ipv6 3ffe::/64 4ffe::/64 dscp af43
20 permit ipv6 78fe::/64 68fe::/64 dscp cs3
!
interface xe1/1
ip access-group ip-acl-01 in
!
```

show running-config access-list

Use this command to show the running system status and configuration details for MAC and IP access lists.

Command Syntax

```
show running-config access-list
```

Parameters

None

Command Mode

Privileged exec mode, configure mode, and route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config access-list
ip access-list abd
10 deny any any any
!
mac access-list abc
remark test
10 deny any any
!
```


© 2021 IP Infusion Inc. Proprietary

show running-config ipv6 access-list

Use this command to show the running system status and configuration details for IPv6 access lists.

Command Syntax

```
show running-config ipv6 access-list
```

Parameters

None

Command Mode

Privileged exec mode, configure mode, and route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config ipv6 access-list
ipv6 access-list test
10 permit any any any
!
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 Authentication, Authorization and Accounting

This chapter is a reference for the authentication:

- Authentication identifies users by challenging them to provide a user name and password. This information can be encrypted if required, depending on the underlying protocol.
- Authorization provides a method of authorizing commands and services on a per user profile basis.

Note: Authorization will be auto-enabled if user enables the Authentication.

- Accounting collects detailed system and command information and stores it on a central server where it can be used for security and quality assurance purposes.

The authentication feature allows you to verify the identity and, grant access to managing devices. The authentication feature works with the access control protocols as described in these chapters:

- Chapter 18, *RADIUS*
- Chapter 25, *TACACS+*

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF.

This chapter describes these commands:

- aaa authentication login default
- aaa accounting default
- aaa authentication login console
- aaa authentication login default
- aaa authentication login default fallback error
- aaa group server
- aaa local authentication attempts max-fail
- aaa local authentication unlock-timeout
- debug aaa
- server
- show aaa authentication
- show aaa authentication login
- show aaa accounting
- show aaa groups
- show running-config aaa

aaa authentication login

Use this command to set login authentication behavior.

Use the `no` form of this command to disable either authentication behavior.

Command Syntax

```
aaa authentication login error-enable (vrf management|)
no aaa authentication login error-enable (vrf management|)
```

Parameters

`error-enable`	Display login failure messages
`management`	Management VRF

Default

By default, aaa authentication login is local

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login error-enable vrf management
```


© 2021 IP Infusion Inc. Proprietary

aaa accounting default

Use this command to set a list of server groups to which to redirect accounting logs.

Use the `no` form of this command to only log locally.

Command Syntax

```
aaa accounting default (vrf management|) ((group LINE)|local)
no aaa accounting default (vrf management|) ((group)|local)
```

Parameters

`group`	Server group list for authentication
`LINE`	A space-separated list of up to 8 configured RADIUS or TACACS+ server group names
`local`	Use local authentication
`management`	Management VRF

Default

Default AAA method is local

Default groups: RADIUS or TACACS+

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa accounting default vrf management group radius
```

aaa authentication login console

Use this command to set the AAA authentication methods for console log ins.

Use the `no` form of this command to set the default AAA authentication method (local).

Command Syntax

```
aaa authentication login console ((group LINE) | (local (|none)) | (none))
no aaa authentication login console ((group LINE) | (local (|none)) | (none))
```

Parameters

`group`		Use a server group list for authentication
	`LINE`	Specify a space-separated list of up to 8 configured RADIUS or TACACS+ server group names followed by `local` or `none` or both `local` and `none`. The list can also include:
		`radius` All configured RADIUS servers
		`tacacs+` All configured TACACS+ servers
`local`		Use local authentication
`none`		No authentication

Default

Default AAA authentication method is local

Default groups: RADIUS or TACACS+

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login console group radius
```


© 2021 IP Infusion Inc. Proprietary

aaa authentication login default

Use this command to set the AAA authentication methods.

Use the `no` form of this command to set the default AAA authentication method (local).

Command Syntax

```
aaa authentication login default (vrf management|) ((group LINE) | (local (|none))
  | (none))
no aaa authentication login default (vrf management|) ((group) | (local (|none)) |
  (none))
```

Parameters

`group`		Use a server group list for authentication
	`LINE`	A space-separated list of up to 8 configured RADIUS or TACACS+, server group names followed by `local` or `none` or both `local` and `none`. The list can also include:
		`radius` All configured RADIUS servers
		`tacacs+` All configured TACACS+ servers
`local`		Use local authentication
`none`		No authentication
`management`		Management VRF

Default

By default, AAA authentication method is local

By default, groups: RADIUS or TACACS+

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login default vrf management group radius
```

aaa authentication login console fallback error

Use this command to enable fallback to local authentication for the console login if remote authentication is configured and all AAA servers are unreachable.

Use the `no` form of this command to disable fallback to local authentication.

Command Syntax

```
aaa authentication login console fallback error local
no aaa authentication login console fallback error local
```

Parameters

None

Default

By default, AAA authentication is local

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login console fallback error local
```


© 2021 IP Infusion Inc. Proprietary

aaa authentication login default fallback error

Use this command to enable fallback to local authentication for the default login if remote authentication is configured and all AAA servers are unreachable.

Use the `no` form of this command to disable fallback to local authentication.

Note: If you have specified `local` (use local authentication) in the aaa authentication login default command, you do not need to use this command to ensure that “fall back to local” occurs.

Command Syntax

```
aaa authentication login default fallback error local (vrf management|)
no aaa authentication login default fallback error local (vrf management|)
```

Parameters

`management`	Management VRF

Default

By default, AAA authentication is local.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login default fallback error local vrf management
```

aaa group server

Use this command to create a server group and enter server group configuration mode.

Use the `no` form of this command to remove a server group.

Command Syntax

```
aaa group server (radius|tacacs+) WORD (vrf management|)
no aaa group server (radius|tacacs+) WORD (vrf management|)
```

Parameters

`radius`	RADIUS server group
`tacacs+`	TACACS+ server group
`WORD`	Server group name; maximum 127 characters
`management`	Management VRF

Default

By default, the AAA group server option is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa group server radius maxsmart
(config-radius)#
```


© 2021 IP Infusion Inc. Proprietary

aaa local authentication attempts max-fail

Use this command to set the number of unsuccessful authentication attempts before a user is locked out.

Use the `no` form of this command to disable the lockout feature.

Command Syntax

```
aaa local authentication attempts max-fail <1-25>
no aaa local authentication attempts max-fail
```

Parameters

`<1-25>`	Number of unsuccessful authentication attempts

Default

By default, the maximum number of unsuccessful authentication attempts before a user is locked out is 3.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa local authentication attempts max-fail 2
```

aaa local authentication unlock-timeout

Use this command to set timeout value in seconds to unlock local user-account.

Use the no form of this command to set default timeout value in seconds.

Note: This command is applicable only to local user but not for user/s present at the server end to authenticate using TACACS+ or RADIUS.

Command Syntax

```
aaa local authentication unlock-timeout <1-3600>
no aaa local authentication unlock-timeout
```

Parameters

<1-3600>	Timeout in seconds to unlock local user-account. Default value is 1200.

Default

By default, the unlock timeout is 1200 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa local authentication unlock-timeout 1800
```


© 2021 IP Infusion Inc. Proprietary

debug aaa

Use this command to display AAA debugging information.

Use the `no` form of this command to stop displaying AAA debugging information.

Command Syntax

```
debug aaa
no debug aaa
```

Parameters

None

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug aaa
```

server

Use this command to add a server to a server group.

Use the `no` form of this command to remove from a server group.

Command Syntax

```
server (A.B.C.D | X:X::X:X | HOSTNAME)
no server (A.B.C.D | X:X::X:X | HOSTNAME)
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address

Default

None

Command Modes

RADIUS server group configure mode

TACACS+ server group configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature tacacs+
(config)#aaa group server tacacs+ TacacsGroup4
(config-tacacs)#server 203.0.113.127
```


© 2021 IP Infusion Inc. Proprietary

show aaa authentication

Use this command to display AAA authentication configuration.

Command Syntax

```
show aaa authentication (|vrf(management|all))
```

Parameters

None

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show aaa authentication

       VRF: default

default: local

console: local
```

Table 3-2 explains the output fields.

Table 3-2: show aaa authentication fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Default	Displays the aaa authentication method list.
Console	Authentication setting for the console access.

show aaa authentication login

Use this command to display AAA authentication configuration for login default and login console.

Command Syntax

```
show aaa authentication login error-enable (|vrf management|all))
```

Parameters

`error-enable`	Display setting for login failure messages
`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show aaa authentication login error-enable

       VRF: default

disabled
```

Table 3-3 explains the output fields.

Table 3-3: show aaa authentication login error-enable fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.

© 2021 IP Infusion Inc. Proprietary

show aaa groups

Use this command to display AAA group configuration.

Command Syntax

```
show aaa groups (vrf (management|all)|)
```

Parameters

`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show aaa groups

      VRF: default

radius
```

Table 3-4 explains the output fields.

Table 3-4: show aaa groups fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.

show aaa accounting

Use this command to display AAA accounting configuration.

Command Syntax

```
show aaa accounting (vrf (management|all)|)
```

Parameters

`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show aaa accounting

        VRF: default

default: group tacacs+
```

Table 3-5 explains the output fields.

Table 3-5: show aaa accounting fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.

© 2021 IP Infusion Inc. Proprietary

show running-config aaa

Use this command to display AAA settings in the running configuration.

Command Syntax

```
show running-config aaa (vrf(management|all)|)
```

Parameters

`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show aaa accounting

        VRF: default

default: local
```

Table 3-6 explains the output fields.

Table 3-6: show aaa accounting fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Default	Displays the aaa authentication method list.

© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 Basic Commands

This chapter describes basic commands.

- banner motd
- clock timezone
- clock set
- configure terminal
- configure terminal force
- copy running-config startup-config
- crypto pki generate rsa common-name ipv4
- debug nsm
- disable
- do
- enable
- enable password
- end
- exec-timeout
- exit
- help
- history
- hostname
- line console
- line vty (all line mode)
- line vty (line mode)
- logging cli
- logout
- max-session
- ping
- ping (interactive)
- privilege level
- quit
- reload
- service advanced-vty
- service password-encryption
- service terminal-length
- show clock
- show cli
- show cli history

© 2021 IP Infusion Inc. Proprietary

- show crypto csr
- show debugging nsm
- show list
- show logging cli
- show nsm client
- show nsm forwarding-timer
- show privilege
- show process
- show running-config
- show startup-config
- show timezone
- show users
- show version
- sys-reload
- sys-shutdown
- terminal length
- terminal monitor
- traceroute
- write
- write terminal

© 2021 IP Infusion Inc. Proprietary

banner motd

Use this command to set the message of the day (motd) at login.

After giving this command, you must write to memory using the write command. If you do not write to memory, the new message of the day is not available after the device reboots.

Use the `no` parameter to not display a banner message at login.

Command Syntax

```
banner motd LINE
banner motd default
no banner motd
```

Parameters

`LINE`	Custom message of the day.
`default`	Default message of the day.

Default

By default, the following banner is displayed after logging in:

```
OcNOS version 1.3.4.268-DC-MPLS-ZEBM 09/27/2018 13:44:22
```

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#banner motd default

#configure terminal
(config)#no banner motd
```

clock timezone

Use this command to set the system time zone.

Use `no` form of this command to set the default system time zone (UTC).

Command Syntax

```
clock timezone (WORD)
no clock timezone
```

Parameters

`WORD`	Timezone name. Use show timezone to get the list of city names.

Default

By default, system time zone is UTC

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#clock timezone Los_Angeles
```


© 2021 IP Infusion Inc. Proprietary

clock set

Use this command to set the system time manually.

Command Syntax

```
clock set <time> <day> <month> <year>
```

Parameters

TIME	Time of the day.
DAYS	pecify the day
MONTH	Month of the year
YEAR	Specify the Year

Examples

```
OcNOS#clock set 18:30:00 13 january 2021
 18:30:00 UTC Wed Jan 13 2021
```

configure terminal

Use this command to enter configure mode.

Command Syntax

```
configure terminal
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows entering configure mode (note the change in the command prompt).

```
#configure terminal
(config)#
```


© 2021 IP Infusion Inc. Proprietary

configure terminal force

Use the configure terminal force command to kick out the configure command mode to privileged EXEC mode, iff there is any session already in configure command mode.

Note: Configure terminal force with option 0 or without any option indicates immediate kick out the session which is locked to configure command mode. similarly, configure terminal force with option of any value indicates session locked to configure command mode will be exited to privileged Exec mode after the specified number of seconds completed.

Command Syntax

```
configure terminal force <0-600|>
```

Parameters

<0-600>	Timeout value in seconds for the session in config mode to exit to Privileged

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal force 0
(config)#
```

copy running-config startup-config

Use this command to a write the configuration to the file used at startup. This is the same as the write command.

Command Syntax

```
copy running-config startup-config
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#copy running-config startup-config
Building configuration...
[OK]
#
```


© 2021 IP Infusion Inc. Proprietary

crypto pki generate rsa common-name ipv4

Use this command to generate a private key and Certificate Signing Request (CSR) which are required for OcNOS to establish a Transport Layer Security (TLS) connection with a NetConf client.

Command Syntax

```
crypto pki generate rsa common-name ipv4 IPv4ADDR
```

Parameters

IPv4ADDR	IPv4 address for the Common Name field of the CSR

Default

N/A

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#crypto pki generate rsa common-name ipv4 7.7.7.7
#show crypto csr
-----BEGIN CERTIFICATE REQUEST-----
MIICVzCCAT8CAQAwEjEQMA4GA1UEAwwHNy43LjcuNzCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMkzIZaxNYPd8PW0hexecUFKq9pJn5IJzJkOQDtoVFOT
zeLPRxBaOt1NVd+lEF+wy3AgnGMw004g4AP7qaE+S5X1vKGAjagtfh/gfDAPDUtM
CpYLMCACM7n76OmyP9eUpkMbOSPkZDIBZfjUMxDTFwkzCBH+BF6SkSxtA24NUA9z
5heCIb1ArXYjdlIeB+9FfiVdOZ5yxQsLY8604ONL7Upl766SArGQo6oZ1dJ+bc91
sQVCEpF40SdCNn+Uw3R0cPfQF81BJD4H0EHf1VnHtYJwQ1yax6qc5ghT9R/rABDa
BFB3R09QpjV4Ihd/MyrdQmEIoXHeNNvSGDj9+eiEpksCAwEAAaAAMA0GCSqGSIb3
DQEBCwUAA4IBAQAwXkQmNf3yiL+pmpwvE+gU8KVp3i4cvD13Vjh7IQMkCT47WPaM
DUiYgwk+dPVAI+iWZq4qTvUNn6xahOyN5rnkTz9eipsQ1YHPpZB7hj5fimWwzJws
m4Tun0GZieEBCROqUpbuW+6QDvtR3XSzHhdGGSIteZv9cYyKhNuO07okwr67c2Ea
1lB7Pcu1tOb4wj3xjqaO/ENDG+nmdUPaIKZrAwf2fEOarOaHgKwcl1AHHbusbJWL
qH0fA1OyVgfvg/WuCPP6Peg/Cpla7bDWqeGYt9vFTtekKoOMQLzJwl6oINbtBCcw
DZJpeaQpUhFm+ZOjwibZ5NGPBRSTuYncp5xJ
-----END CERTIFICATE REQUEST-----
#
```

debug nsm

Use this command to enable NSM debugging.

Use the `no` form of this command or the `undebug` command to disable NSM debugging.

Command Syntax

```
debug nsm (all|)
no debug nsm (all|)
undebug nsm (all|)

debug nsm bfd
no debug nsm bfd
undebug nsm bfd

debug nsm events
no debug nsm events
undebug nsm events

debug nsm hal (all|) debug
debug nsm hal events
no debug nsm hal (all|)
no debug nsm hal events
undebug nsm hal events

debug nsm packet (recv|send|) (detail|)
no debug nsm packet (recv|send|) (detail|)
undebug nsm packet (recv|send|) (detail|)
```

Parameters

`all`	Enable all debugging.
`bfd`	Debug BFD events.
`events`	Debug NSM events.
`hal`	Debug HAL.
`events`	Debug HAL events.
`packet`	Debug packet events.
`recv`	Debug received packets.
`send`	Debug sent packets.
`detail`	Show detailed packet information.

© 2021 IP Infusion Inc. Proprietary

Default

By default, debugging is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug nsm all
#
#debug nsm bfd
#
#debug nsm events
#
#debug nsm hal all
#
#debug nsm packet
#
#debug nsm packet recv detail
```

disable

Use this command from to exit privileged exec mode and return to exec mode. This is the only command that allows you to go back to exec mode. The exit or quit commands in privileged exec mode end the session without returning to exec mode.

Command Syntax

```
disable
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#disable
>
```


© 2021 IP Infusion Inc. Proprietary

do

Use this command to run several exec mode or privileged exec mode commands from configure mode. The commands that can be run from configure mode using `do` are: `show`, `clear`, `debug`, `ping`, `traceroute`, `write`, and `no debug`.

Note: The `do` command supports only the following CLI commands only

Command Syntax

```
do LINE
```

Parameters

`LINE`	Command and its parameters.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#(config)#do show interface
Interface lo
  Hardware is Loopback index 1 metric 1 mtu 16436 duplex-half arp ageing
timeout 25
  <UP,LOOPBACK,RUNNING>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet 4.4.4.40/32 secondary
  inet 127.0.0.1/8
  inet6 ::1/128
  Interface Gifindex: 3
  Number of Data Links: 0
  GMPLS Switching Capability Type:
    Packet-Switch Capable-1 (PSC-1)
  GMPLS Encoding Type: Packet
  Minimum LSP Bandwidth 0
    input packets 10026, bytes 730660, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 10026, bytes 730660, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
#
```

enable

Use this command to enter privileged exec command mode.

Command Syntax

```
enable
```

Parameters

None

Default

No default value is specified

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows entering the Privileged Exec mode (note the change in the command prompt).

```
>enable
#
```


© 2021 IP Infusion Inc. Proprietary

enable password

Use this command to change or create a password to use when entering enable mode.

There are three methods to enable a password:

Plain Password

The plain password is a clear text string that appears in the configuration file as configured.

Encrypted Password

An encrypted password encrypts a clear text password. First, use this command to create a plain password. Then, use the service password-encryption command to encrypt the password. An encrypted password display as an encrypted string in configuration file. There are two methods to configure encrypted password.

Note: Use the above Hidden password method only if you know the encrypted string of the plain text string that you want to use as a password.

Use the `no` parameter to disable the password.

Command Syntax

```
enable password LINE
no enable password
no enable password LINE
```

Parameters

`LINE`	The HIDDEN “enable” password string.

Note: Password can be an alpha-numeric string between 6-32 characters, including spaces. the string cannot begin with a number.

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#enable password mypasswd
```

end

Use this command to return to privileged exec command mode from any other advanced command mode.

Command Syntax

```
end
```

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows returning to privileged exec mode directly from interface mode.

```
#configure terminal
(config)#interface eth0
(config-if)#exit
#
```


© 2021 IP Infusion Inc. Proprietary

exec-timeout

Use this command to set the interval the command interpreter waits for user input detected. That is, this sets the time a telnet session waits for an idle VTY session before it times out. A value of zero minutes and zero seconds (0 and 0) causes the session to wait indefinitely.

Use the `no` parameter to disable the wait interval.

Command Syntax

```
exec-timeout <0-35791> (<0-2147483>|)
no exec-timeout
```

Parameters

`<0-35791>`	Timeout value in minutes.
`<0-2147483>`	Timeout value in seconds.

Default

No default value is specified

Command Mode

Line mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, the telnet session will timeout after 2 minutes, 30 seconds if there is no response from the user.

```
Router#configure terminal
Router(config)#line vty 23 66
Router(config-line)#exec-timeout 2 30
```

exit

Use this command to exit the current mode and return to the previous mode. When used in exec mode or privileged exec mode, this command terminates the session.

Command Syntax

```
exit
```

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows exiting interface mode and returning to configure mode.

```
#configure terminal
(config)#interface eth0
(config-if)#exit
(config)#
```


© 2021 IP Infusion Inc. Proprietary

help

Use this command to display help for the OcNOS command line interface.

Command Syntax

```
help
```

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
```

history

Use this command to set the maximum number of commands stored in the command history.

Use the `no` parameter to remove the configuration.

Command Syntax

```
history max <0-2147483647>
no history max
```

Parameters

`<0-2147483647>` Number of commands.

Default

No default value is specified

Command Mode

Line mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#line vty 12 77
(config-line)#history max 123

(config-line)#no history max
```


© 2021 IP Infusion Inc. Proprietary

hostname

Use this command to set the network name for the device. OcNOS uses this name in system prompts and default configuration filenames.

Setting a host name using this command also sets the host name in the kernel.

Note: After giving the `hostname` command, you must write to memory using the write command. If you do not write to memory, the change made by this command (the new host name) is not set after the device reboots.

Use the `no` parameter to disable this function.

Command Syntax

```
hostname WORD
no hostname (WORD|)
```

Parameter

`WORD`	Network name for a system. Per RFC 952 and RFC 1123, a host name string can contain only the special characters period (“.”) and hyphen (“-”). These special characters cannot be at the start or end of a host name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#hostname ABC
(config)#

(config)#no hostname
(config)#exit
```

line console

Use the this command to move or change to the line console mode.

Command Syntax

```
line console <0-0>
```

Parameters

<0-0>	First line number.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example enters line mode (note the change in the prompt).

```
#configure terminal
(config)#line console 0
(config-line)#
```


© 2021 IP Infusion Inc. Proprietary

line vty (all line mode)

Use this command to move or change to “all lin”e VTY mode.

Command Syntax

```
line vty
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Example

The following example shows entering all line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty
(config-all-line)#exit
(config)#
```

line vty (line mode)

Use this command to move or change to VTY mode. This command is used to connect to a protocol daemon. This configuration is necessary for any session. This configuration should be in the daemon's config file before starting the daemon.

Use the `no` parameter to disable this command.

Command Syntax

```
line vty <0-871> <0-871>
no line vty <0-871> (<0-871>|)
```

Parameters

`<0-871>`	Specify the first line number.
`<0-871>`	Specify the last line number.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows entering line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty 9
(config-line)#exit
(config)no line vty 9
```


© 2021 IP Infusion Inc. Proprietary

logging cli

Use this command to enable logging commands entered by all users.

Use the `no` parameter to disable logging commands entered by all users.

Command Syntax

```
logging cli
no logging cli
```

Parameter

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#logging cli
(config)#no logging cli
```

logout

Use this command to exit the OcNOS shell.

Command Syntax

```
logout
```

Parameters

None

Default

No default value is specified

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

```
>logout
OcNOS login:

>enable
en#logout
>
```


© 2021 IP Infusion Inc. Proprietary

max-session

Use this command to set maximum VTY session limit.

Use `no` form of this command to unset session-limit.

User can configure session-limit for Telnet and SSH sessions separately but this max-session parameter value takes the precedence to restrict the maximum number of sessions. If user configured this max-session to be 4, then the device would allow only maximum of 4 SSH and Telnet sessions collectively irrespective of the individual SSH and Telnet max-session configuration. Active sessions won't be disturbed even if the configured max-session limit is lesser than the current active sessions.

Command syntax

```
max-session <1-40>
```

Parameters

`<1-40>`	Number of sessions

Default

By default, 40 sessions are allowed.

Command Mode

Line mode

Applicability

This command is introduced in OcNOS-DC version 5.0

Example

In the following example max-session is configured as 4, thus the device would allow only 4 management sessions of SSH and Telnet collectively.

```
Router#configure terminal
Router(config)#line vty 23 66
Router(config-line)#max-session 4
```

ping

Use this command to send echo messages to another host.

Command Syntax

```
ping WORD (vrf (NAME|management)|)
ping ip WORD (vrf (NAME|management)|)
ping ipv6 WORD (|IFNAME)
ping ipv6 WORD (|IFNAME) (vrf (NAME|management)|)
```

Parameters

WORD	Destination address (in A.B.C.D format for IPv4 or X:X::X:X for IPv6) or host name.
vrf	Virtual Routing and Forwarding instance.
NAME	Virtual Routing and Forwarding name.
management	Virtual Routing and Forwarding name.
ip	IPv4 echo.
WORD	Destination address in A.B.C.D format or host name.
ipv6	IPv6 echo.
WORD	Destination address in X:X::X:X format or host name.
IFNAME	Name of the interface.

Default

No default value is specified

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>enable
#ping 20.20.20.1 vrf management
Press CTRL+C to exit
PING 20.20.20.1 (20.20.20.1) 56(84) bytes of data.
64 bytes from 20.20.20.1: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 20.20.20.1: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 20.20.20.1: icmp_seq=3 ttl=64 time=0.033 ms
64 bytes from 20.20.20.1: icmp_seq=4 ttl=64 time=0.034 ms
64 bytes from 20.20.20.1: icmp_seq=5 ttl=64 time=0.034 ms
64 bytes from 20.20.20.1: icmp_seq=6 ttl=64 time=0.036 ms
64 bytes from 20.20.20.1: icmp_seq=7 ttl=64 time=0.036 ms
64 bytes from 20.20.20.1: icmp_seq=8 ttl=64 time=0.036 ms

--- 20.20.20.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6999ms
```


© 2021 IP Infusion Inc. Proprietary

```
rtt min/avg/max/mdev = 0.032/0.034/0.036/0.006 ms

#ping ipv6 3001:db8:0:1::129 vrf management
Press CTRL+C to exit
PING 3001:db8:0:1::129(3001:db8:0:1::129) 56 data bytes
64 bytes from 3001:db8:0:1::129: icmp_seq=1 ttl=64 time=0.038 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=4 ttl=64 time=0.049 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=5 ttl=64 time=0.044 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=6 ttl=64 time=0.048 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=7 ttl=64 time=0.046 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=8 ttl=64 time=0.048 ms

--- 3001:db8:0:1::129 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6999ms
```

© 2021 IP Infusion Inc. Proprietary

ping (interactive)

Use this command to send echo messages to another host interactively. You are prompted with options supported by the command.

Command Syntax

```
ping
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>enable
#ping
Protocol [ip]:
Target IP address: 20.20.20.1
Name of the VRF : management
Repeat count [5]: 6
Time Interval in Sec [1]: 2.2
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Ping Broadcast? Then -b [n]:
PING 20.20.20.1 (20.20.20.1) 100(128) bytes of data.
108 bytes from 20.20.20.1: icmp_seq=1 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=2 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=3 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=4 ttl=64 time=0.036 ms
108 bytes from 20.20.20.1: icmp_seq=5 ttl=64 time=0.037 ms
108 bytes from 20.20.20.1: icmp_seq=6 ttl=64 time=0.034 ms

--- 20.20.20.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 11000ms
rtt min/avg/max/mdev = 0.034/0.036/0.038/0.007 ms

#ping
Protocol [ip]: ipv6
Target IP address: 3001:db8:0:1::129
Name of the VRF : management
Repeat count [5]:
Time Interval in Sec [1]:
Datagram size [100]:
```


© 2021 IP Infusion Inc. Proprietary

```
Timeout in seconds [2]:
Extended commands [n]:
PING 3001:db8:0:1::129(3001:db8:0:1::129) 100 data bytes
108 bytes from 3001:db8:0:1::129: icmp_seq=1 ttl=64 time=0.050 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=2 ttl=64 time=0.047 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=3 ttl=64 time=0.042 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=4 ttl=64 time=0.048 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=5 ttl=64 time=0.051 ms

--- 3001:db8:0:1::129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.042/0.047/0.051/0.008 ms
```

The input prompts are described in Table 4-7:

Table 4-7: ping output fields

Protocol [ip]	IPv4 or IPv6. The default is IPv4 if not specified.
Target IP address	IPv4 or IPv6 address or host name.
Name of the VRF	Name of the Virtual Routing and Forwarding instance.
Repeat count [5]	Number of ping packets to send. The default is 5 if not specified.
Time Interval in Sec [1]	Time interval between two ping packets. The default is 1 second if not specified.
Datagram size [100]	Ping packet size. The default is 100 bytes if not specified.
Timeout in seconds [2]	Time to wait for ping reply. The default is 2 seconds if not specified.
Extended commands [n]	Options for extended ping. The default is “no”.
Source address or interface	Source address or interface.
Type of service [0]	Types of service. The default is 0 if not specified.
Set DF bit in IP header? [no]	Do not fragment bit. The default value is “no” if not specified.
Data pattern [0xABCD]	Specify a pattern.
Ping Broadcast? Then -b [n]	Broadcast ping. The default is “no”. For a broadcast address, the value should be “y”.

privilege level

Use this command to set the command privilege level.

Note: Privilege levels 2-14 are undefined.

Use the `no` parameter with this command to disable the command privilege level.

Command Syntax

```
privilege level <1-15>
privilege level (16)
no privilege level (<1-15>|)
no privilege level (16)
```

Parameters

`16`	Maximum privilege level for a line.
`<1-15>`	Default privilege level for a line.

Default

No default value is specified

Command Mode

Line mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#line vty 0 5
(config-line)#privilege level 15
```


© 2021 IP Infusion Inc. Proprietary

quit

Use this command to exit the current mode and return to the previous mode. When this command is executed in one of the exec modes, it closes the shell and logs you out.

Command Syntax

```
quit
```

Parameters

None

Default

No default value is specified

Command Mode

All modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#quit
(config)#

>enable
#quit
[root@TSUP-123 sbin]#
```

reload

Use this command to shut down the device and perform a cold restart. You call this command when:

- You detect a configuration issue such as `show running-config` displaying a configuration but when you try to remove that configuration, you get a message that it is not configured.
- You have replaced the start-up configuration file (in this case you specify the `flush-db` parameter).

Command Syntax

```
reload (flush-db|)
```

Parameters

`flush-db`	Delete the database file and recreate it from the start-up configuration file.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows replacing a start-up configuration file and then synchronizing it to the configuration database:

```
#copy file /home/TEST.conf startup-config
Copy Success
#
#reload flush-db
The system has unsaved changes.
Would you like to save them now? (y/n): n

Configuration Not Saved!
Are you sure you would like to reset the system? (y/n): y
```

For both of these prompts, you must specify whether to save or discard the changes. Abnormal termination of the session without these inputs can impact the system behavior.

For the `unsaved changes` prompt:

```
Would you like to save them now?
```

You should always say “no” to this prompt because otherwise the command takes the current *running configuration* and applies it to the current start-up configuration.

© 2021 IP Infusion Inc. Proprietary

service advanced-vty

Use this command to set multiple options to list when the tab key is pressed while entering a command. This feature applies to commands with more than one option.

Use the `no` parameter to not list options when the tab key is pressed while entering a command.

Command Syntax

```
service advanced-vty
no service advanced-vty
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#service advanced-vty
(config)#no service advanced-vty
```

service password-encryption

Use this command to encrypt passwords created with the enable password command. Encryption helps prevent observers from reading passwords.

Use the `no` parameter to disable this feature.

Only network administrators can execute these commands. For more, see the username command.

Command Syntax

```
service password-encryption
no service password-encryption
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#enable password mypasswd
(config)#service password-encryption
```


© 2021 IP Infusion Inc. Proprietary

service terminal-length

Use this command to set the number of lines that display at one time on the screen for the current terminal session.

Use the `no` parameter to disable this feature.

Command Syntax

```
service terminal-length <0-512>
no service terminal-length (<0-512>|)
```

Parameters

`<0-512>`	Number of lines to display. A value of 0 prevents pauses between screens of output.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#service terminal-length 60
```

show clock

Use this command to display the current system time.

Command Syntax

```
show clock
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show clock
12:54:02 IST Fri Apr 29 2016
```


© 2021 IP Infusion Inc. Proprietary

show cli

Use this command to display the command tree of the current mode.

Command Syntax

```
show cli
```

Parameters

None

Default

None

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show cli
Exec mode:
+-clear
  +-arp-cache [clear arp-cache]
  +-ethernet
    +-cfm
      +-errors
        +-domain
          +-DOMAIN_NAME [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
            +-bridge
              +-<1-32> [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
        +-level
          +-LEVEL_ID [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
            +-bridge
              +-<1-32> [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
      +-maintenance-points
        +-remote
          +-domain
            +-DOMAIN_NAME [clear ethernet cfm maintenance-points remote(domain
D
--More--
```

show cli history

Use this command to list the commands entered in the current session. The history buffer is cleared automatically upon reboot.

Command Syntax

```
show cli history
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show cli history
   1 en
   2 show ru
   3 con t
   4 show spanning-tree
   5 exit
```


© 2021 IP Infusion Inc. Proprietary

show crypto csr

Use this command to display the Certificate Signing Request (CSR) created with the crypto pki generate rsa common-name ipv4 command.

Command Syntax

```
show crypto csr
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#crypto pki generate rsa common-name ipv4 7.7.7.7
#show crypto csr
-----BEGIN CERTIFICATE REQUEST-----
MIICVzCCAT8CAQAwEjEQMA4GA1UEAwwHNy43LjcuNzCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMkzIZaxNYPd8PW0hexecUFKq9pJn5IJzJkOQDtoVFOT
zeLPRxBaOt1NVd+lEF+wy3AgnGMw004g4AP7qaE+S5X1vKGAjagtfh/gfDAPDUtM
CpYLMCACM7n76OmyP9eUpkMbOSPkZDIBZfjUMxDTFwkzCBH+BF6SkSxtA24NUA9z
5heCIb1ArXYjdlIeB+9FfiVdOZ5yxQsLY8604ONL7Upl766SArGQo6oZ1dJ+bc91
sQVCEpF40SdCNn+Uw3R0cPfQF81BJD4H0EHf1VnHtYJwQ1yax6qc5ghT9R/rABDa
BFB3R09QpjV4Ihd/MyrdQmEIoXHeNNvSGDj9+eiEpksCAwEAAaAAMA0GCSqGSIb3
DQEBCwUAA4IBAQAwXkQmNf3yiL+pmpwvE+gU8KVp3i4cvD13Vjh7IQMkCT47WPaM
DUiYgwk+dPVAI+iWZq4qTvUNn6xahOyN5rnkTz9eipsQ1YHPpZB7hj5fimWwzJws
m4Tun0GZieEBCROqUpbuW+6QDvtR3XSzHhdGGSIteZv9cYyKhNuO07okwr67c2Ea
1lB7Pcu1tOb4wj3xjqaO/ENDG+nmdUPaIKZrAwf2fEOarOaHgKwcl1AHHbusbJWL
qH0fA1OyVgfvg/WuCPP6Peg/Cpla7bDWqeGYt9vFTtekKoOMQLzJwl6oINbtBCcw
DZJpeaQpUhFm+ZOjwibZ5NGPBRSTuYncp5xJ
-----END CERTIFICATE REQUEST-----
```

show debugging nsm

Use this command to display debugging information.

Command Syntax

```
show debugging nsm
```

Parameters

None

Default

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging nsm
NSM debugging status:
  NSM event debugging is on
  NSM packet debugging is on
  NSM kernel debugging is on
#
```


© 2021 IP Infusion Inc. Proprietary

show list

Use this command to display the commands relevant to the current mode.

Command Syntax

```
show list
```

Parameters

None

Default

None

Command Mode

All command modes except IPv4 access-list and IPv6 access-list mode.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>show list
 clear arp-cache
  clear bgp *
  clear bgp * in
  clear bgp * in prefix-filter
  clear bgp * out
  clear bgp * soft
  clear bgp * soft in
  clear bgp * soft out
  clear bgp <1-4294967295>
  clear bgp <1-4294967295> in
  clear bgp <1-4294967295> in prefix-filter
  clear bgp <1-4294967295> out
  clear bgp <1-4294967295> soft
  clear bgp <1-4294967295> soft in
  clear bgp <1-4294967295> soft out
  clear bgp (A.B.C.D|X:X::X:X)
  clear bgp (A.B.C.D|X:X::X:X) in
  clear bgp (A.B.C.D|X:X::X:X) in prefix-filter
  clear bgp (A.B.C.D|X:X::X:X) out
  clear bgp (A.B.C.D|X:X::X:X) soft
  clear bgp (A.B.C.D|X:X::X:X) soft in
  clear bgp X:X::X:X soft out

--more--
```

show logging cli

Use this command to display command history for all users.

Command Syntax

```
show logging cli ((logfile LOGFILENAME)|) (match-pattern WORD |)
show logging cli last <1-9999>
show logging logfile list
```

Parameters

`LOGFILENAME`	Name of a saved command history log file. The default path is `/var/log/messages`, but you can specify a full path to override the default.
`WORD`	Display only lines with this search pattern.
`<1-9999>`	Number of lines to display from the end of the command history.
`logfile list`	Display a list of command history files.

Default

LOGFILENAME Name of a saved command history log file. The default path is /var/log/messages, but you can specify a full path to override the default.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh logging cli
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli logfile ipi
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli match-pattern root
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli logfile ipi match-pattern root
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#show logging cli last 2
2017 Mar 1 16:34:26.302 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging info'
2017 Mar 1 16:34:37.317 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging cli last 2'
#show logging logfile list
file1
file2
```


© 2021 IP Infusion Inc. Proprietary

show nsm client

Use this command to display NSM client information including the services requested by the protocols, statistics and the connection time

Command Syntax

```
show nsm client
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show nsm client
NSM client ID: 1

NSM client ID: 19
 IMI, socket 23
  Service: Interface Service, Router ID Service, VRF Service
  Messsage received 1, sent 58
  Connection time: Thu Jul 22 11:03:12 2010
  Last message read: Service Request
  Last message write: Link Up
NSM client ID: 25
 ONMD, socket 24
  Service: Interface Service, Bridge service, VLAN service
  Messsage received 2, sent 74
  Connection time: Thu Jul 22 11:03:15 2010
  Last message read: OAM  LLDP msg
  Last message write: Link Up
#
```

show nsm forwarding-timer

Use this command to display the information of Graceful Restart capable MPLS clients to NSM that are currently shutdown. Use the option LDP or RSVP to see the particular module information.

Command Syntax

```
show nsm (ldp| rsvp) forwarding-timer
```

Parameters

`ldp`	Use this parameter to display the protocol LDP information.
`rsvp`	Use this parameter to display the protocol RSVP information.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Example

```
OcNOS#
OcNOS#sh nsm rsvp forwarding-timer
Protocol-Name  GR-State  Time Remaining (sec)   Disconnected-time
    RSVP        ACTIVE           100           2021/08/18 04:49:23
OcNOS#sh nsm ldp forwarding-timer
Protocol-Name  GR-State  Time Remaining (sec)   Disconnected-time
     LDP        ACTIVE           111           2021/08/18 04:50:37
OcNOS#sh nsm forwarding-timer
Protocol-Name  GR-State  Time Remaining (sec)   Disconnected-time
     LDP        ACTIVE           110           2021/08/18 04:50:37
    RSVP        ACTIVE            96           2021/08/18 04:49:23
```


© 2021 IP Infusion Inc. Proprietary

show privilege

Use this command to display the current privilege level. The privilege level range is 1-15.

Command Syntax

```
show privilege
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show privilege
Current privilege level is 15
#
```

show process

Use this command to display the OcNOS daemon processes that are running.

Command Syntax

```
show process
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show process
 PID NAME             TIME     FD
   1 nsm          00:56:29    7
   2 ripd         00:56:29    11
   3 ripngd       00:56:29    12
   4 ospfd        00:56:29    9
   5 ospf6d       00:56:29    10
   6 bgpd         00:56:29    14
   9 isisd        00:56:29    8
#
```

Table 4-8 explains the output fields.

Table 4-8: show process fields

Entry	Description
PID Name	Process identifier name.
TIME	(S): Number of system and user CPU seconds that the process has used. (None, D, and E): Total amount of time that the command has been running.
FD	The Flexible Data-Rates (FD) of the interface.

© 2021 IP Infusion Inc. Proprietary

show running-config

Use this command to show the running system status and configuration.

Command Syntax

```
show running-config
show running-config full
```

Parameters

`full`	Display the full configuration information.

Command Mode

Privileged exec mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#show running-config
no service password-encryption
!
no service dhcp
ip domain-lookup
!
mpls propagate-ttl
!
vrrp vmac enable
spanning-tree mode provider-rstp
no data-center-bridging enable
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 no shutdown
!
interface eth0
 ip address 10.1.2.173/24
 no shutdown
!
interface eth1
 shutdown

!
line con 0
 login
!
end
(config)#
```

show startup-config

Use this command to display the startup configuration.

Command Syntax

```
show startup-config
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show startup-config
!   2001/04/21 11:38:52
!
hostname ripd
password zebra
log stdout
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
!
router rip
 redistribute connected
 network 10.10.10.0/24
 network 10.10.11.0/24
!
line vty
 exec-timeout 0 0
```


© 2021 IP Infusion Inc. Proprietary

show timezone

Use this command to display the list of timezone names.

Command Syntax

```
show timezone(all|africa|america|antarctica|arctic|asia|atlantic|australia|brazil|
  canada|chile|europe|indian|mexico|pacific|us)
```

Parameters

`africa`	Africa timezone list
`all`	All timezone list
`america`	America timezone list
`antarctica`	Antarctica timezone list
`arctic`	Arctic timezone list
`asia`	Asia timezone list
`atlantic`	Atlantic timezone list
`australia`	Australia timezone list
`brazil`	Brazil timezone list
`canada`	Canada timezone list
`chile`	Chile timezone list
`europe`	Europe timezone list
`indian`	Indian timezone list
`mexico`	Mexico timezone list
`pacific`	Pacific timezone list
`us`	US timezone list

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS 1.3.7

Examples

```
#show timezone asia
Asia:
Kuwait
Samarkand
Novosibirsk
Hebron
Singapore
Dushanbe
Rangoon
Riyadh
Thimphu
Shanghai
```

```
Phnom_Penh
Taipei
Qyzylorda
Ho_Chi_Minh
Urumqi
Chita
Khandyga
Nicosia
Jerusalem
Ashkhabad
Gaza
Tel_Aviv
Baghdad
Anadyr
Tehran
Ashgabat
Saigon
Damascus
Sakhalin
Yekaterinburg
Baku
Bangkok
Kashgar
Macao
Seoul
Jakarta
Aden
Katmandu
Amman
Ujung_Pandang
Kuching
Hong_Kong
Ulan_Bator
Dhaka
Macau
Omsk
Vientiane
Pyongyang
Ust-Nera
Manila
Srednekolymsk
Tbilisi
Kamchatka
Magadan
Istanbul
Chongqing
Jayapura
Yerevan
Makassar
Colombo
Karachi
Hovd
Novokuznetsk
Krasnoyarsk
Irkutsk
Kabul
Kolkata
```


© 2021 IP Infusion Inc. Proprietary

```
Dacca
Brunei
Calcutta
Kathmandu
Bishkek
Qatar
Tashkent
Aqtau
Oral
Kuala_Lumpur
Pontianak
Harbin
Aqtobe
Bahrain
Muscat
Vladivostok
Dubai
Tokyo
Chungking
Almaty
Choibalsan
Thimbu
Beirut
Dili
Yakutsk
Ulaanbaatar
```

show users

Use this command to display information about current users.

Command Syntax

```
show users
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

      Line      User     Idle     Location/Session      PID     TYPE        Role
(*) 130 vty 0 [C]root   00:00:36      pts/0            20872    Local    network-admin
(#)   NA      [N]root     NA           1                NA       NA      network-admin
      NA      [N]root     NA           2                NA       NA      network-admin
    131 vty 1 [C]joyce  00:00:26     pts/1             17593    Remote   network-admin
```


© 2021 IP Infusion Inc. Proprietary

show version

Use this command to display OcNOS version information.

Command Syntax

```
show version
```

Parameters

None

Default

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show version
Software version: EC_AS5812-54X-OcNOS-1.3.4.268-DC_MPLS_ZEBM-S0-P0 09/27/2018
13:44:22
 Copyright (C) 2018 Coriant. All rights reserved

 Software Product: OcNOS, Version: 1.3.4.268
 Hardware Model: Edgecore 5812-54X-O-AC-F
 Software Feature Code: DC-MPLS-ZEBM
 System Configuration Code: S0
 Package Configuration Code: P0
 Software Baseline Version: 1.3.4.208

Installation Information:
 Image Filename: EC_AS5812_54X-OcNOS-1.3.4.268-DC_MPLS_ZEBM-S0-P0-installer
 Install method: http
 ONIE SysInfo: x86_64-accton_as5812_54x-r0
#
```

Table 4-9: Show version output

Entry	Description
Software version	The software version including hardware device name and date.
Software Product	Product name and version.
Hardware Model	Hardware platform.
Software Feature Code	SKU that specifies the capabilities of this version of the software.
System Configuration Code	System configuration number.

Table 4-9: Show version output (Continued)

Entry	Description
Package Configuration Code	ONIE package installer versions.
Software Baseline Version	Version from which this release branch is created.
Installation Information	Information about the installation.
Image Filename	The file name of the installed image.
Install method	The type of server (or USB stick) from which the software was installed.
ONIE SysInfo	ONIE version.

© 2021 IP Infusion Inc. Proprietary

sys-reload

Use this command to cold restart the device.

Note: This command is an alias for the reload command.

Command Syntax

```
sys-reload
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.7.

Example

```
>sys-reload
The system has unsaved changes.
Would you like to save them now? (y/n): y
Building Configuration...
[OK]
Are you sure you would like to reset the system? (y/n): n
```

sys-shutdown

Use this command to shut down the device gracefully. After giving this command, you can remove the device power cable.

Note: Some of the switch hardwares doesn't support system shutdown. On such devices this command will make the switch to go for a reboot.

Command Syntax

```
sys-shutdown
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.7.

Example

```
>sys-shutdown
The system has unsaved changes.
Would you like to save them now? (y/n): y
Building Configuration...
[OK]
Are you sure you would like to shutdown the system? (y/n): y
For both of these prompts, you must specify whether to save or discard the
changes.
For the unsaved changes prompt:
Would you like to save them now?
```


© 2021 IP Infusion Inc. Proprietary

terminal length

Use this command to set the number of lines displayed on the screen.

Use the `no` option to unset the number of lines on a screen.

Command Syntax

```
terminal length <0-511>
terminal no length <0-511>
```

Parameters

`<0-511>`	Number of lines on screen. Specify 0 for no pausing.

Default

By default, terminal length is 25 lines.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>enable
#terminal length 0
```

The following example sets the terminal length to 30 lines.

```
#terminal length 30
```

terminal monitor

Use this command to display debugging output on a terminal.

Use one of the optional parameters to display debugging output for the Privileged Virtual Router (PVR) or VR user. When the command is used without a parameter, it can be used by a PVR user or non-PVR user to display the debug output on the terminal for the user local VR. When used with a parameter, it may be used only by a PVR user.

The `no` form of the command terminates the debug output on the terminal. Both the PVR and VR user can use this command. In addition, the PVR user can cancel a debug output from a specific VR or all VRs.

Command Syntax

```
terminal monitor
terminal monitor (all|WORD|)
terminal no monitor
terminal no monitor (WORD|)
```

Parameters

`WORD`	Used in the PVR context, and contains the VR name to be included in the debugging session.
`all`	Used the PVR context to include all VR in a PVR debugging session.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>Enable
#terminal monitor
#terminal no monitor
```


© 2021 IP Infusion Inc. Proprietary

traceroute

Use this command to trace an IPv4/v6 route to its destination.

Command Syntax

```
traceroute WORD
traceroute WORD (vrf (NAME|management)|)
traceroute ipv6 WORD
traceroute ipv6 WORD (vrf (NAME|management)|)
```

Parameters

WORD	Destination address (in A.B.C.D format for IPv4 or X:X::X:X for IPv6) or host name.
vrf	Virtual Routing and Forwarding instance.
NAME	Virtual Routing and Forwarding name.
management	Virtual Routing and Forwarding name.
ip	IPv4 echo.
WORD	Destination address in A.B.C.D format or host name.
ipv6	IPv6 echo.
WORD	Destination address in X:X::X:X format or host name.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#traceroute ip 10.10.100.126 vrf management
traceroute to 10.10.100.126 (10.10.100.126), 30 hops max, 38 byte packets
 1  10.1.2.1 (10.1.2.1)  0.386 ms  0.315 ms  0.293 ms
 2  10.10.100.126 (10.10.100.126)  1.944 ms  1.497 ms  1.296 ms
#
```

write

Use this command to a write the configuration to the file used at startup or to a specified file. This is the same as the copy running-config startup-config command.

Command Syntax

```
write file FILE
write memory
write WORD
```

Parameters

FILE	Write to a given path and file. If you do not give a file path, the file is added to /root.
memory	Write to non-volatile memory.
WORD	Write to running configuration file path.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows writing the configuration to the startup configuration file:

```
#write
Building configuration...
[OK]
```

This example shows writing the configuration to a specified file:

```
#write file /home/test.txt
Building configuration...
[OK]
```


© 2021 IP Infusion Inc. Proprietary

write terminal

Use this command to display the current configuration.

Command Syntax

```
write terminal
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#write terminal

Current configuration:
!
hostname ripd
password zebra
log stdout
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
!
!
router rip
 network 10.10.10.0/24
 network 10.10.11.0/24
 redistribute connected
!
line vty
 exec-timeout 0 0
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 Chassis Management Module Commands

This chapter provides a description, syntax, and examples of CMM feature commands:

- cpu-core-usage
- debug cmm
- locator led
- show hardware-information
- show system-information
- system-load-average

You can retrieve the same set of information through SNMP that these commands display. This MIB is defined in `CMM-CHASSIS-MIB.txt`:

IP Infusion Inc. enterprise identifier	36673
Chassis MIB identifier	100

The MIB definition is available at:

- https://github.com/IPInfusion/OcNOS/branches

Navigate to the directory for the version of OcNOS that you are using.

cpu-core-usage

Use this command to configure user threshold values for monitoring cpu core uses.

Use no form of this command to set default thresholds.

Command Syntax

```
cpu-core-usage warning <51-100> alarm <91-100>
```

Parameters

`warning`	Warning
`<51-100>`	51-100
`alarm`	alarm
`<91-100>`	91-100

Defaul

Check the default thresholds using `show system-information cpu-load` CLI command.

Command Mode

Config Mode

Applicability

This command was introduced in OcNOS-1.3.6.

Example

```
OcNOS#con t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#
OcNOS(config)#cpu-core-usage warning 56 alarm 97
OcNOS(config)#cpu-core-usage warning 56 alarm 97
OcNOS(config)#end
OcNOS#show system-information cpu-load

System CPU-Load Information
===========================

Uptime                    : 64 Days 18 Hours 20 Minutes 12 Seconds

Load Average(1 min)       : 4.24% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)       : 2.87% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)      : 3.37% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage             : 2.02%
CPU core 1 Usage          : 0.89% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 2 Usage          : 0.00% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 3 Usage          : 5.41% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 4 Usage          : 2.68% (Crit Thresh : 56%, Alert Thresh : 97%)
```


© 2021 IP Infusion Inc. Proprietary

```
OcNOS#con t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#no cpu-core-usage
OcNOS(config)#end
OcNOS#show system-information cpu-load

System CPU-Load Information
===========================

Uptime                     : 64 Days 18 Hours 21 Minutes 46 Seconds

Load Average(1 min)        : 2.44% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)        : 2.49% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)       : 3.27% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage              : 1.82%
CPU core 1 Usage           : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage           : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage           : 4.59% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage           : 1.82% (Crit Thresh : 50%, Alert Thresh : 90%)
OcNOS#
```

debug cmm

Use this command to enable or disable debugging for CMM.

Command Syntax

```
debug cmm
no debug cmm
```

Parameters

None

Default

By default, debug command is not configured.

Command Mode

Configuration mode and exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug cmm
(config)#no debug cmm
```


© 2021 IP Infusion Inc. Proprietary

locator led

Use this command to turn on the locator LED.

Use the no form of this command to turn off the locator LED.

Command Syntax

```
locator-led on
no locator-led on
```

Parameters

None

Default

By default, locator LED is turned off.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#locator-led on
```

show hardware-information

Use this command to display hardware information.

Command Syntax

```
show hardware-information (memory|fan|temperature|led|power|transceiver|all)
```

Parameter

`all`	Hardware details of all modules.
`fan`	Fan status of the boards.
`led`	LED status of the boards.
`memory`	Memory information of the boards.
`power`	PSU information.
`temperature`	Temperature sensor information of the boards.
`transceiver`	Transceiver presence status and supported list of transceivers.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
    #show hardware-information all
-------------------------------------------------------
               RAM INFORMATION
-------------------------------------------------------

Total                                    : 16028 MB
Used                                     : 654 MB (4 %)
Free                                     : 15373 MB (96 %)
Shared                                   : 57 MB
Buffers                                  : 153 MB
Total Swap                               : 0 MB
Free Swap                                : 0 MB
Current Processes                        : 203
Total High Memory                        : 0 MB
Available High Memory                    : 0 MB
Unit Size                                : 1 Bytes
Alert Threshold                          : 90 %
Critical Threshold                       : 80 %
-------------------------------------------------------
               HARD DISK INFORMATION
```


© 2021 IP Infusion Inc. Proprietary

```
-----------------------------------------------------

Serial Number                              : 99001151130000000031
Model Number                               : ATP mSATA
Firmware Revision                          : 20140730ATP mSATA
Cylinders                                  : 16383
Heads                                      : 16
Sectors                                    : 61865984
Unformatted Bytes/Track                    : 0
Unformatted Bytes/Sector                   : 0
Revision No                                : 508.0
Usage Alert Threshold                      : 90 %
Usage Critical Threshold                   : 80 %
-----------------------------------------------------------
Filesystem   Total        Used         Free         Use%
-----------------------------------------------------------
/            28858        4739         24119        16%
/cfg         476          60           416          13%
-----------------------------------------------------------

Codes : R - Rear Fan, F - Front Fan, U - Unknown
-----------------------------------------------------------
FAN TRAY     FAN          RPM          MINRPM       MAXRPM
-----------------------------------------------------------
1            1(F)         9200         6718         21500
1            2(R)         7800         5625         18000
2            1(F)         9200         6718         21500
2            2(R)         7700         5625         18000
3            1(F)         9100         6718         21500
3            2(R)         7800         5625         18000
4            1(F)         8900         6718         21500
4            2(R)         7600         5625         18000
5            1(F)         9100         6718         21500
5            2(R)         7700         5625         18000
6            1(F)         8600         6718         21500
6            2(R)         7300         5625         18000

Board Temp Sensors Temperature in Degree C
-------------------------------------------------------------------------------
----------------------
SENSOR TYPE                      CURR  EMER  ALRT CRIT CRIT ALRT EMER   MIN-TEMP
  MAX-TEMP  AVG-TEMP
                                 TEMP  MIN   MIN  MIN  MAX  MAX  MAX  (Monitored
 since 72 hour,00 min)

-------------------------------------------------------------------------------
----------------------
CPU                              29.00  0    10   14   52   57   60      25.00
   32.00     28.45
Mainboard Front middle           42.00  0    10   14   61   66   69      37.00
```

```
   44.00     41.13
Mainboard Rear middle            40.00  0    10   14   56   61   67      35.00
   42.00     38.84
Mainboard left                   34.00  0    10   14   51   56   59      29.00
   36.00     32.38
BCM Chip                         55.00  0    10   14   82   87   95      48.60
   56.90     53.70

BCM Chip Internal Temperature
-----------------------------------------
TEMP MONITOR    CURRENT TEMP    PEAK TEMP
                (Degree C)      (Degree C)
-----------------------------------------
1               54.00           56.40
2               54.00           55.90
3               55.00           56.90
4               53.00           55.50
5               53.00           55.90
6               54.50           56.40
7               54.50           56.40
8               54.00           55.50

-----------------------------------------------------
                System Power Information
-----------------------------------------------------
CMM_PS1_12V_PG                          : GOOD
CMM_PS2_12V_PG                          : FAIL
CMM_PS1_AC_ALERT                        : GOOD
CMM_PS2_AC_ALERT                        : FAIL

Codes:     * Not Supported by device    NA Not Applicable

PSU        VOLT-IN    VOLT-OUT   CURR-IN    CURR-OUT   PWR-IN     PWR-OUT    TEM
P-1     TEMP-2     FAN-1      FAN-2      PWR_OUT_MAX
           (Volt)     (Volt)     (Ampere)   (Ampere)   (Watt)     (Watt)     (Ce
lsius)  (Celsius)  (Rpm)      (Rpm)
-------------------------------------------------------------------------------
-------------------------------------------------
1          NA*        12.06*     NA*        15.42*     NA*        186.00*    31.
00*     39.00*     9600*      NA         650.00*

-------------------------------------------------
LED             COLOR              DESCRIPTION
-------------------------------------------------
POWER 1         GREEN              PSU1 operates Normally
POWER 2         OFF                PSU2 Not Present
FAN TRAY 1      GREEN              Normal
FAN TRAY 2      GREEN              Normal
FAN TRAY 3      GREEN              Normal
FAN TRAY 4      GREEN              Normal
```


© 2021 IP Infusion Inc. Proprietary

```
FAN TRAY 5      GREEN             Normal
FAN TRAY 6      GREEN             Normal
SYSTEM          AMBER             Minor Fault
LOCATOR         OFF               Locator Function is disabled
FRONT FAN       GREEN             Fan operates normally

-----------------------------------------------------
           Transceiver DDM support list
-----------------------------------------------------
Type                        :TSFP
Vendor Name                 :OCLARO,INC.
Vendor Part Number          :TRS7081AHCPA00A
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :AVAGO
Vendor Part Number          :AFBR-79E4Z
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :FINISAR CORP
Vendor Part Number          :FCCN410QD3C
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :FINISAR CORP
Vendor Part Number          :FTL410QE4C
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :DELL
Vendor Part Number          :119N6
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :Skylane Optics
Vendor Part Number          :QFP85P1040PD000
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :Skylane Optics
Vendor Part Number          :QFPQL010400D000
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :Skylane Optics
Vendor Part Number          :QFPQL010400B000
DDM Supported               :Yes

Type                        :QSFP
```

```
Vendor Name                :Skylane Optics
Vendor Part Number         :QFPQL002400D000
DDM Supported              :Yes

Type                       :QSFP
Vendor Name                :Skylane Optics
Vendor Part Number         :QFP85P3040PD000
DDM Supported              :Yes

Type                       :QSFP
Vendor Name                :Skylane Optics
Vendor Part Number         :QFP85P1040PB000
DDM Supported              :Yes

Type                       :QSFP
Vendor Name                :Skylane Optics
Vendor Part Number         :DAPQQC504000000
DDM Supported              :NO

Type                       :QSFP
Vendor Name                :Skylane Optics
Vendor Part Number         :DAPQQM014000000
DDM Supported              :NO

Type                       :QSFP
Vendor Name                :Skylane Optics
Vendor Part Number         :DAPQQM034000000
DDM Supported              :NO

Type                       :QSFP
Vendor Name                :Skylane Optics
Vendor Part Number         :DAPQQM054000000
DDM Supported              :NO

Type                       :QSFP
Vendor Name                :Skylane Optics
Vendor Part Number         :QFP1301040PD000
DDM Supported              :Yes

Type                       :QSFP
Vendor Name                :Skylane Optics
Vendor Part Number         :QFPQL040400D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :DELL
Vendor Part Number         :4WJ41
DDM Supported              :Yes

Type                       :QSFP28
```

 © 2021 IP Infusion Inc. Proprietary

```
Vendor Name               :FINISAR CORP
Vendor Part Number        :FCBN425QE1C
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :FINISAR CORP.
Vendor Part Number        :FTLC1151RDPL
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :FINISAR CORP
Vendor Part Number        :FTLC9551REPM
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :INPHI CORP
Vendor Part Number        :IN-Q2AY2
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :FS
Vendor Part Number        :QSFP28-SR4-100G
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-QSFP28-SR4
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-QSFP28-LR4
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD010C07D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q2885P30C0PF000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD020C00D000
DDM Supported             :Yes

Type                      :QSFP28
```

```
Vendor Name                :Skylane Optics
Vendor Part Number         :DAOQQM01C00D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :DAOQQM02C00D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :DAOQQM03C00D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :DAOQQM05C00D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :DAOQQM07C00D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :DAOQQM10C00D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :DAOQQM20C00D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :DAOQQM30C00D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :DAOQQP10C00D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :Q2885P10C0PF000
DDM Supported              :Yes

Type                       :QSFP28
```

 © 2021 IP Infusion Inc. Proprietary

```
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD040C00F000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD010C00D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD010C04D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD040C05F000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD040C05D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQM03C000000
DDM Supported             :NO

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQM01C000000
DDM Supported             :NO

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQM02C000000
DDM Supported             :NO

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQM05C000000
DDM Supported             :NO

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQC50C000000
DDM Supported             :NO

Type                      :QSFP28
```

```
Vendor Name                :Skylane Optics
Vendor Part Number         :Q28QL002C00F000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :Q2C31002C00F000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :Q2C31P50C00F000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :Q2B85M70C00D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :Q28QD080C05F000
DDM Supported              :Yes


TX     : Transmit status
RX-Los : Receive status
RESET  : Normal (Out of reset), Reset (In reset)
POWER  : Power level Low/High
 -     : NotApplicable

SFP:[0-0]
---------------------------------------------
PORT   PRESENCE        Tx         Rx-Los
---------------------------------------------

QSFP:[1-32]
------------------------------------------------------------------------------
------------
PORT   PRESENCE        RESET      POWER                                LANE

------------------------------------------------------------------------------
------------
                                                        1          2          3
         4
------------------------------------------------------------------------------
------------
1      Present         Normal     -          Tx         on         on         on
         on
                                              Rx-Los     Off        Off        Of
```

 © 2021 IP Infusion Inc. Proprietary

```
f       Off
                                        Tx-Los    Off       Off       Of
f       Off
2     Not Present    Reset     -        Tx        off       off       of
f       off
                                        Rx-Los    Off       Off       Of
f       Off
                                        Tx-Los    Off       Off       Of
f       Off
3     Present        Normal    -        Tx        on        on        on
        on
                                        Rx-Los    Off       Off       Of
f       Off
                                        Tx-Los    Off       Off       Of
f       Off
4     Present        Normal    -        Tx        on        on        on
        on
                                        Rx-Los    Off       Off       Of
f       Off
                                        Tx-Los    Off       Off       Of
f       Off
5     Not Present    Reset     -        Tx        off       off       of
f       off
                                        Rx-Los    Off       Off       Of
f       Off
                                        Tx-Los    Off       Off       Of
f       Off
6     Not Present    Reset     -        Tx        off       off       of
f       off
                                        Rx-Los    Off       Off       Of
f       Off
                                        Tx-Los    Off       Off       Of
f       Off
7     Present        Normal    -        Tx        on        on        on
        on
                                        Rx-Los    Off       Off       Of
f       Off
                                        Tx-Los    Off       Off       Of
f       Off
8     Present        Normal    -        Tx        on        on        on
        on
                                        Rx-Los    Off       Off       Of
f       Off
                                        Tx-Los    Off       Off       Of
f       Off
9     Not Present    Reset     -        Tx        off       off       of
f       off
                                        Rx-Los    Off       Off       Of
f       Off
                                        Tx-Los    Off       Off       Of
```

```
f       Off
10    Not Present    Reset      -          Tx          off         off         of
f       off
                                          Rx-Los      Off         Off         Of
f       Off
                                          Tx-Los      Off         Off         Of
f       Off
11    Not Present    Reset      -          Tx          off         off         of
f       off
                                          Rx-Los      Off         Off         Of
f       Off
                                          Tx-Los      Off         Off         Of
f       Off
12    Not Present    Reset      -          Tx          off         off         of
f       off
                                          Rx-Los      Off         Off         Of
f       Off
                                          Tx-Los      Off         Off         Of
f       Off
13    Present        Normal     -          Tx          on          on          on
        on
                                          Rx-Los      Off         Off         Of
f       Off
                                          Tx-Los      Off         Off         Of
f       Off
14    Present        Normal     -          Tx          on          on          on
        on
                                          Rx-Los      Off         Off         Of
f       Off
                                          Tx-Los      Off         Off         Of
f       Off
15    Not Present    Reset      -          Tx          off         off         of
f       off
                                          Rx-Los      Off         Off         Of
f       Off
                                          Tx-Los      Off         Off         Of
f       Off
16    Not Present    Reset      -          Tx          off         off         of
f       off
                                          Rx-Los      Off         Off         Of
f       Off
                                          Tx-Los      Off         Off         Of
f       Off
17    Present        Normal     -          Tx          on          on          on
        on
                                          Rx-Los      Off         Off         Of
f       Off
                                          Tx-Los      Off         Off         Of
f       Off
18    Present        Normal     -          Tx          on          on          on
```


© 2021 IP Infusion Inc. Proprietary

```
        on
                                                Rx-Los     Off        Off        Of
f       Off
                                                Tx-Los     Off        Off        Of
f       Off
19      Not Present     Reset       -           Tx         off        off        of
f       off
                                                Rx-Los     Off        Off        Of
f       Off
                                                Tx-Los     Off        Off        Of
f       Off
20      Not Present     Reset       -           Tx         off        off        of
f       off
                                                Rx-Los     Off        Off        Of
f       Off
                                                Tx-Los     Off        Off        Of
f       Off
21      Present         Normal      -           Tx         on         on         on
        on
                                                Rx-Los     Off        Off        Of
f       Off
                                                Tx-Los     Off        Off        Of
f       Off
22      Present         Normal      -           Tx         on         on         on
        on
                                                Rx-Los     Off        Off        Of
f       Off
                                                Tx-Los     Off        Off        Of
f       Off
23      Not Present     Reset       -           Tx         off        off        of
f       off
                                                Rx-Los     Off        Off        Of
f       Off
                                                Tx-Los     Off        Off        Of
f       Off
24      Not Present     Reset       -           Tx         off        off        of
f       off
                                                Rx-Los     Off        Off        Of
f       Off
                                                Tx-Los     Off        Off        Of
f       Off
25      Present         Normal      -           Tx         on         on         on
        on
                                                Rx-Los     Off        Off        Of
f       Off
                                                Tx-Los     Off        Off        Of
f       Off
26      Present         Normal      -           Tx         on         on         on
        on
                                                Rx-Los     Off        Off        Of
```

```
f        Off
                                          Tx-Los     Off        Off        Of
f        Off
27     Not Present     Reset      -         Tx         off        off        of
f        off
                                          Rx-Los     Off        Off        Of
f        Off
                                          Tx-Los     Off        Off        Of
f        Off
28     Not Present     Reset      -         Tx         off        off        of
f        off
                                          Rx-Los     Off        Off        Of
f        Off
                                          Tx-Los     Off        Off        Of
f        Off
29     Not Present     Reset      -         Tx         off        off        of
f        off
                                          Rx-Los     Off        Off        Of
f        Off
                                          Tx-Los     Off        Off        Of
f        Off
30     Not Present     Reset      -         Tx         off        off        of
f        off
                                          Rx-Los     Off        Off        Of
f        Off
                                          Tx-Los     Off        Off        Of
f        Off
31     Not Present     Reset      -         Tx         off        off        of
f        off
                                          Rx-Los     Off        Off        Of
f        Off
                                          Tx-Los     Off        Off        Of
f        Off
32     Not Present     Reset      -         Tx         off        off        of
f        off
                                          Rx-Los     Off        Off        Of
f        Off
                                          Tx-Los     Off        Off        Of
f        Off

System Over all status   : Minor Fault

---------------------------
Components status
---------- -----------------
CPU        : Normal
RAM        : Normal
DISK       : Normal
TEMP       : Normal
FAN        : Normal
```


© 2021 IP Infusion Inc. Proprietary

```
POWER       : Minor Fault
SOFTWARE    : Normal

Codes: H-Mi- High Minor H-Ma- High Major L-Mi- Low Minor L-Ma- Low Major

Component  Fault  Timestamp            Thresh   Violation-Status
---------  -----  ---------            ------   ----------------
CPU        H-Mi   06-18-2021 15:03:15  > 50.00  50.72%(Cpu Core)

FAN        H-Mi   06-18-2021 15:02:24           Tray[6] Fan[2] set to MIN RPM[31
.25]
                  06-18-2021 15:02:24           Tray[6] Fan[1] set to MIN RPM[31
.25]
                  06-18-2021 15:02:24           Tray[5] Fan[2] set to MIN RPM[31
.25]

POWER      H-Mi   06-18-2021 15:02:21           Psu [2] Not Found

OcNOS#end
```

Table 5-10 explains the show command output fields.

Table 5-10: show hardware-information all output

Entry	Description
Ram Information	Displays the used memory, free memory, shared, buffers, total swap, and free swap memory.
Hard Disk Information	Displays hard drive serial number, model, firmware revision, cylinders, heads, and sectors, as well as revision number and total size.
Fans	Displays the fan tray numbers, numbers of fans per tray, and their speed in RPM.
Board Temp Sensors Temperature	Displays sensor type, current temperature, and operating range.
BCM Chip Internal Temperature	Displays broadcom chips current internal temperature, Operating range and average temperature.
System Power Information	Displays system power Information. Shows Voltage on all rails, and whether the power is up or has failed.
PSU	Show main power supply statistics – Volts in, Volts out, current in and out Amperes, power in and out in Watts, temperature of each power supply, and fan speed in RPM.
LED	Shows a list of what the LEDs represent, what state the LEDs mean, and a description of what the LEDs current color means.
Transceiver DDM support list	Show a list of transceivers that support Digital Diagnostic Monitoring (DDM) – type, vendor name, part number, and whether DDM is supported.
Port Number	Displays a list of the port numbers, port type (SFP,QSFP, etc) and whether a transceiver is or is not in the port.

show system-information

Use this command to display system information.

Command Syntax

```
show system-information (all|fan|psu|os|cpu|bios|cpu-load|board-info)
```

Parameter

`all`	System information of all modules.
`bios`	BIOS information.
`board-info`	Board EEPROM details.
`cpu`	Processor information.
`cpu-load`	CPU load information.
`fan`	Fan Field Replaceable Units (FRU) EEPROM information.
`os`	OS and Kernel version information.
`psu`	Power Supply Field Replaceable Units (FRU) EEPROM information.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show system-information psu
System PSU FRU Information
=========================
PSU 2 Country of Origin          : CN
PSU 2 PPID Part Number           : 0T9FNW
PSU 2 PPID Part Number Rev       : A00
PSU 2 Manufacturer ID            : 28298
PSU 2 Date Code                  : 52R
PSU 2 Serial Number              : 0298
PSU 2 Part Number                : 0T9FNW
PSU 2 Part Number Revision       : A00
PSU 2 Number of Fans in the tray : 1
PSU 2 Type                       : AC Normal
PSU 2 Service Tag                : AEIOU
```

The following tables explain the show command output fields.

© 2021 IP Infusion Inc. Proprietary

Table 5-11: Show fan topic displays

System Fan FRU Information	Description
Fan Tray “#” PPID Part Number	The vendor’s part number for the fan.
Fan Tray Serial Number	As stated
Service Tag	The Service Tag can help identify your device for on-line support and upgrading drivers
Vendor Name	As stated

Table 5-12: Show system BIOS information

BIOS Information	Description
# dmidecode	The dmidecode is a tool for dumping a computer's DMI table contents in a human-readable format. This table contains a description of the system's hardware components, as well as other useful pieces of information such as serial numbers and BIOS revisions.
SMBIOS	The System Management BIOS (SMBIOS) defines data structures (and access methods) that can be used to read management information produced by the BIOS of a computer. Also, it is involved with the DMI Address –
Handle 0x0000, DMI type 0, 24 bytes	Handle of the Desktop Management Interface (DMI) and the DMI type, where type value identifies what the DMI contains. DMI = 0 indicates the following information is specific to BIOS properties, and is 24 bytes long.
BIOS Physical Information	• Vendor – The manufacture of the BIOS. • Version – The Version number. • Release Date – as stated. • Address – starting address (in memory) of the BIOS.
Characteristics	• Is PCI supported. • Is BIOS upgradeable. • Is boot from a CD supported. • Is selectable boot devices supported. • Is BIOS ROM socketed. • Is Enhanced Disk Drive (EDD) vectoring supported. • Is 5.25"/1.2 MB floppy services supported (int 13h) • Is 3.5"/720 kB floppy services supported (int 13h) • Is 3.5"/2.88 MB floppy services supported (int 13h) • Is Print screen service supported (int 5h) • Is 8042 keyboard services supported (int 9h) • Is Serial services supported (int 14h) • Is Printer services supported (int 17h) • Is Advanced Configuration and Power Interface (ACPI) supported • Is USB legacy supported • Is BIOS boot specification supported • Is Targeted content distribution supported • Is Unified Extensible Firmware Interface (UEFI) supported
BIOS Revision	The BIOS revision number.

Table 5-12: Show system BIOS information (Continued)

BIOS Information	Description
Handle 0x0043, DMI type 13, 22 bytes	Handle of the Desktop Management Interface (DMI) and the DMI type, where type value identifies what the DMI contains. DMI = 13 indicates the following information is specific to BIOS language information, and is 22 bytes long.
BIOS Language Informantion	• Language Description Format – A term that describes the number of bits used to represent the BIOS Language information parameters. • Installable Languages – The number of languages that can be used by the BIOS at any time. • Currently Installed Language – United States English (or Latin-1) as described by the ISO standard, en|US|iso8859-1.

Table 5-13: Show CPU information

System CPU Information	Description
processor	The processor number of each CPU
model name	Details about each CPU. For example, Intel(R) Atom(TM) CPU C2538 @ 2.40GHz.

Table 5-14: Show system CPU load information

Load Information	Description
Uptime	As stated in days, hours, minutes, and seconds.
Load Average for past 1min	As stated in percent.
Load Average for past 5 min	As stated in percent.
Load Average for past 15 min	As stated in percent.
CPU Usage at this instant	As stated in percent.
Max threshold for CPU-usage	As stated in percent.

Table 5-15: Show system board information

System Information	Description
Product Name	Model number of the device.
Serial Number	As stated
Base MAC Address	As stated
Manufacture Date	As state

© 2021 IP Infusion Inc. Proprietary

Table 5-15: (Continued)Show system board information

System Information	Description
Platform Name	The platform on which the product is based.
ONIE Version	The version of the Open Network Install Environment (ONIE).
MAC addresses	Number of MAC addresses related to the device.
Manufacture	As stated
Country Code	The code that represents the country of manufacture. For example, US = United States, TW = Taiwan, and so on.
Diag Version	As stated
CRC-32	Cyclic Redundancy Check value.
Switch Chip Revision	As stated
MAIN BOARD REVISION	As stated
CPU CPLD VERSION	The version of the Complex Programmable Logic Device (CPLD) use by the CPU.
SW CPLD VERSION	The version of the Complex Programmable Logic Device (CPLD) use by the switch.
MAIN BOARD TYPE	An identifying string for the main board.
CPU BOARD ID	An identifying string for the CPU board.
CPU BOARD VERSION	As stated
SW BOARD ID	NA
SW BOARD VERSION	As stated
VCC 5V	The state of the VCC 5V power rail (Enabled \ Disabled)
MAC 1V	The state of the MAC 1V power rail Enabled \ Disabled
VCC 1.8V	The state of the VCC 1.8V power rail (Enabled \ Disabled)
MAC AVS 1V	The state of the MAC AVS 1V power rail (Enabled \ Disabled)
HOT SWAP1	Enabled \ Disabled
HOT SWAP2	Enabled \ Disabled

Table 5-16: Show host system details

Host Information	Description
OS Distribution	The operating system on which the device is to run.
Kernel Version	A string that identifies the operating kernel.

system-load-average

Use this command to configure user threshold values for monitoring system load average for last 1 minute, 5 minute and 15 minute.

Use no form of this command to set default thresholds.

Command Syntax

```
system-load-average (1min warning <41-100> alarm <51-100> 5min alarm <51-100> 15min
  alarm <51-100>)
```

Parameters

`1min`	1min
`warning`	Warning
`<41-100>`	41-100
`alarm`	alarm
`<51-100>`	51-100
`5min`	5min
`alarm`	alarm
`<51-100>`	51-100
`15min`	15min
`alarm`	alarm
`<51-100>`	51-100

Default

Check the default thresholds using `show system-information cpu-load` CLI command.

Command Mode

Config Mode

Applicability

This command was introduced in OcNOS-1.3.6.

Example

```
OcNOS#con t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#
OcNOS(config)#system-load-average 1min warning 45 alarm 55 5min alarm 65 15min
alarm 75

OcNOS#show system-information cpu-load

System CPU-Load Information
===========================
```


© 2021 IP Infusion Inc. Proprietary

```
Uptime                     : 64 Days 17 Hours 56 Minutes 22 Seconds

Load Average(1 min)        : 5.74% (Crit Thresh : 45%, Alert Thresh : 55%)
Load Average(5 min)        : 3.71% (Crit Thresh : N/A, Alert Thresh : 65%)
Load Average(15 min)       : 3.21% (Crit Thresh : N/A, Alert Thresh : 75%)

Avg CPU Usage              : 4.67%
CPU core 1 Usage           : 4.42% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage           : 2.68% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage           : 6.19% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage           : 5.36% (Crit Thresh : 50%, Alert Thresh : 90%)

OcNOS#con t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#no system-load-average
OcNOS(config)#end
OcNOS#show system-information cpu-load

System CPU-Load Information
===========================

Uptime                     : 64 Days 18 Hours 16 Minutes 34 Seconds

Load Average(1 min)        : 0.63% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)        : 1.90% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)       : 3.11% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage              : 2.07%
CPU core 1 Usage           : 1.83% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage           : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage           : 6.36% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage           : 0.93% (Crit Thresh : 50%, Alert Thresh : 90%)
OcNOS#
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 6 Configuration Management

This chapter is a reference for commands that copy these types of files:

- Start-up configuration and running configuration
- System files such as boot files, core dumps, and debug logs

You can use these commands to copy files locally or to copy between the local device and a remote system.

The commands in this chapter use the techniques in Table 6-17 to remotely transfer files:

Table 6-17: File transfer techniques

Trivial File Transfer Protocol (TFTP)	No authentication or encryption; dangerous to use over the Internet, but might be acceptable in a trusted environment Address format: `tftp:[//server[:port]][/path]`
File Transfer Protocol (FTP)	Authenticates, but does not encrypt Address format: `ftp:[//server][/path]`
Secure copy (SCP)	Authenticates and encrypts using Secure Shell (SSH1) Address format: `scp:[//server][/path]`
SSH File Transfer Protocol (SFTP)	Authenticates and encrypts using Secure Shell (SSH2); this is the most secure technique Address format: `sftp:[//server][/path]`
Hyper text Transfer Protocol (HTTP)	Address format: `http:[//server][/path]` For download of running and startup configurations

This chapter contains these commands.

- copy empty-config startup-config
- copy running-config
- copy running-config (interactive)
- copy startup-config
- copy startup-config (interactive)
- copy system file
- copy system file (interactive)
- copy ftp startup-config
- copy scp startup-config
- copy sftp startup-config
- copy tftp startup-config
- copy http startup-config
- copy http startup-config (interactive)
- copy ftp startup-config (interactive)
- copy scp filepath
- copy scp startup-config (interactive)
- copy tftp startup-config (interactive)
- copy http startup-config (interactive)
- copy file startup-config

© 2021 IP Infusion Inc. Proprietary

copy empty-config startup-config

Use this command to clear the contents of the startup configuration.

Command Syntax

```
copy empty-config startup-config
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#copy empty-config startup-config
#
```


© 2021 IP Infusion Inc. Proprietary

copy running-config

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy running-config (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL|http HTTP-
  URL) (vrf (NAME|management)|)
```

Parameters

`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`HTTP-URL`	Destination: `http:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy running-config sftp sftp://sftp.mysite.com/running_conf vrf management
```

copy running-config (interactive)

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy running-config (ftp|tftp|scp|sftp|http) (vrf (NAME|management)|)
```

Parameters

`ftp`	Destination: FTP server
`tftp`	Destination: TFTP server
`scp`	Destination: SCP server
`sftp`	Destination: SFTP server
`http`	Destination: HTTP server
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy running-config sftp vrf management
```


© 2021 IP Infusion Inc. Proprietary

copy startup-config

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy startup-config (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL|http
  HTTP_URL) (vrf (NAME|management)|)
```

Parameters

`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`HTTP-URL`	Destination: `http:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy startup-config sftp sftp://sftp.mysite.com/start-up_conf vrf management
```

copy startup-config (interactive)

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy startup-config (ftp|tftp|scp|sftp|http) (vrf (NAME|management)|)
```

Parameters

`ftp`	Destination: FTP server
`tftp`	Destination: TFTP server
`scp`	Destination: SCP server
`sftp`	Destination: SFTP server
`http`	Destination: HTTP server
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy startup-config sftp vrf management
```


© 2021 IP Infusion Inc. Proprietary

copy system file

Use this command to copy a system file to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Note: The names of the options for the source in the first parameter refer to symbolic locations. The specific locations for Linux are noted below. The locations on a specific device can vary depending on the platform.

Command Syntax

```
copy (core|debug|log|techsupport|filepath) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-
  URL|sftp SFTP-URL)(vrf (NAME|management)|)
```

Parameters

`core`	Core file storage; on Linux this refers to `/var/log/crash/cores/`
`debug`	Debug file storage; on Linux this refers to `/log/`
`log`	Log file storage; on Linux this refers to `/var/log/`
`techsupport`	Copy techsupport log files to remote machine
`filepath`	Copy device file to remote machine
`FILE`	Source file name
`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy core myFile sftp sftp://sftp.mysite.com/dst_filename vrf management
```

copy system file (interactive)

Use this command to copy a system file to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Note: The names of the options for the source in the first parameter refer to symbolic locations. The specific locations for Linux are noted below. The locations on a specific device can vary depending on the platform.

Command Syntax

```
copy (core|debug|log|techsupport|filepath) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-
  URL|sftp SFTP-URL)(vrf (NAME|management)|)
```

Parameters

`core`	Core file storage; on Linux this refers to `/var/log/crash/cores/`
`debug`	Debug file storage; on Linux this refers to `/log/`
`log`	Log file storage; on Linux this refers to `/var/log/`
`techsupport`	Copy techsupport log files to remote machine
`filepath`	Copy device file to remote machine
`FILE`	Source file name
`ftp`	Destination: FTP server
`tftp`	Destination: TFTP server
`scp`	Destination: SCP server
`sftp`	Destination: SFTP server
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy log myFile sftp vrf management
```


© 2021 IP Infusion Inc. Proprietary

copy ftp startup-config

Use this command to copy the start up configuration from an FTP server to the local device.

Command Syntax

```
copy ftp FTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`FTP-URL`	Configuration source: `ftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy ftp ftp://ftp.mysite.com/scr filename startup-config vrf management
```

copy scp startup-config

Use this command to copy the start up configuration from a SCP server to the local device.

Command Syntax

```
copy scp SCP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`SCP-URL`	Configuration source: `scp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy scp scp://scp.mysite.com/scr filename startup-config vrf management
```


© 2021 IP Infusion Inc. Proprietary

copy sftp startup-config

Use this command to copy the start up configuration from a SFTP server to the local device.

Command Syntax

```
copy sftp SFTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`SFTP-URL`	Configuration source: `sftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy sftp sftp://sftp.mysite.com/scr filename startup-config vrf management
```

copy tftp startup-config

Use this command to copy the start up configuration from a TFTP server to the local device.

Command Syntax

```
copy tftp TFTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`TFTP-URL`	Configuration source: `tftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy tftp tftp://tftp.mysite.com/scr filename startup-config vrf management
```


© 2021 IP Infusion Inc. Proprietary

copy http startup-config

Use this command to copy the start up configuration from an HTTP server to the local device.

Command Syntax

```
copy http HTTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`HTTP-URL`	Configuration source: `http:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy http http://http.mysite.com/scr filename startup-config vrf management
```

copy ftp startup-config (interactive)

Use this command to copy the start up confguration from an FTP server to the local device.

Command Syntax

```
copy ftp startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy ftp startup-config vrf management
```


© 2021 IP Infusion Inc. Proprietary

copy scp filepath

Use this command to copy the remote system file using SCP to the local device.

Note: OcNOS has a dedicated partition called `/cfg` for storing system level configurations, OcNOS configurations and license data. This is persistent across reboots and upgrades and consists of directories `/cfg/` and `/usr/local/etc`. Copying `user/general` files under `/cfg` partition is discouraged because the size of this partition is very small and impacts normal system operations like `bootup/upgrades` and important system files copy when it doesn't have enough space. Users are recommended to use `/home` to copy the general files. Please note that the contents placed in `/home` directory are deleted upon software upgrade.

Command Syntax

```
copy scp SCP-URL (filepath FILEPATH) (vrf (NAME|management)|)
```

Parameters

`SCP-URL`	Configuration source: `scp:[//server][/path]`
`FILEPATH`	Enter the local filesystem path with filename
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 1.3.9.

Examples

```
#copy scp scp://10.12.65.89/root/cmlsh filepath /root/cmlsh vrf management
```

copy scp startup-config (interactive)

Use this command to copy the start up confguration from a SCP server to the local device.

Command Syntax

```
copy scp startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy scp startup-config vrf management
```


© 2021 IP Infusion Inc. Proprietary

copy sftp startup-config (interactive)

Use this command to copy the start up confguration from an SFTP server to the local device.

Command Syntax

```
copy sftp startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy sftp startup-config vrf management
```

copy tftp startup-config (interactive)

Use this command to copy the start-up confguration from a TFTP server to the local device.

Command Syntax

```
copy tftp startup-config (vrf (NAME|management)|)
```

Parameters

`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy tftp startup-config vrf management
```


© 2021 IP Infusion Inc. Proprietary

copy http startup-config (interactive)

Use this command to copy the start-up confguration from an HTTP server to the local device.

Command Syntax

```
copy http startup-config (vrf (NAME|management)|)
```

Parameters

`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy http startup-config vrf management
```

copy file startup-config

Use this command to copy and store a local file into the startup configuration.

Command Syntax

```
copy file FILE startup-config
```

Parameters

FILE	File name

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy file myFile startup-config
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 7 Common Management Layer Commands

This chapter is a reference for the Common Management Layer (CML) commands.

Transaction are enabled by default. You can disable the feature by using the cmlsh transaction command outside of configuration mode, but IP Infusion Inc. does *not* recommend this.

These are the steps to follow to use transactions:

- When transactions are enabled, any changes done in configure mode are stored in a separate *candidate* configuration that you can view with the show transaction current command.
- When a configuration is complete, apply the candidate configuration to the running configuration with the commit command.
- If a commit fails, no configuration is applied as the entire transaction is considered failed. You can continue to change the candidate configuration and then retry the commit.
- Discard the candidate configuration with the abort transaction command.
- Check the last aborted transaction with the show transaction last-aborted command.

This chapter describes these commands:

- abort transaction
- cml logging
- cml netconf translation
- cmlsh transaction
- cmlsh transaction limit
- commit
- debug cml
- show max-transaction limit
- show transaction current
- show transaction last-aborted
- show (xml|json) running-config

abort transaction

Use this command to end a configuration session and discard all uncommitted changes.

Command Syntax

```
abort transaction
```

Parameters

None

Default

N/A

Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#
(config)#interface eth2
(config-if)#ip address 10.12.3.4/24
(config-if)#exit
(config)#abort transaction
(config)#exit
#show running-config interface eth2
!
interface eth2
!
#
```


© 2021 IP Infusion Inc. Proprietary

cml logging

Use this command to enable or disable CML logging. The logging level and debug cml should also be configured.

Command Syntax

```
cml logging (enable | disable)
```

Parameters

`enable`	Enable CML logging
`disable`	Disable CML logging

Default

By default CML Logging is enabled.

Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#cml logging disable
```

cml netconf translation

Use this command to enable or disable NetConf support for OpenConfig-based YANG translation.This allows OcNOS to handle OpenConfig YANG files in its NetConf server.

Command Syntax

```
cml netconf translation (disable|openconfig)
```

Parameters

`disable`	Do not translate NetConf to YANG
`openconfig`	Translate NetConf to YANG

Default

By default NetConf-to-YANG translation is disabled.

Mode

Exec mode

Applicability

This command was introduced before OcNOS-SP version 4.2.

Example

```
#cml netconf translation openconfig
```


© 2021 IP Infusion Inc. Proprietary

cmlsh transaction

Use this command to enable or disable the transaction-based command-line interface.

Note: IP Infusion Inc. recommends that you do *not* disable transactions.

Command Syntax

```
cmlsh transaction (enable | disable)
```

Parameters

`enable`	Enable transaction-based command-line interface
`disable`	Disable transaction-based command-line interface

Default

The transaction-based command-line interface is enabled by default.

Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
>en
#cmlsh transaction disable
% Deprecated CLI. Disabling transaction mode is not recommended
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#router ipv6 ospf test
(config-router)#exit
(config)#show running-config router ipv6 ospf
!
router ipv6 ospf test
!
(config)#
```

cmlsh transaction limit

Use this command to set the maximum number of transactions.

To verify, give the show max-transaction limit command in exec mode.

Command Syntax

```
cml transaction limit <0-300000>
```

Parameters

<0-300000>	Maximum number of transactions with zero (0) indicating unlimited transactions.

Default

300,000 transactions

Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#cml transaction limit 1500
(config)#exit
#show max-transaction limit
Max-Transaction Limit is 1500
```


© 2021 IP Infusion Inc. Proprietary

commit

Use this command to commit the candidate configuration to the running configuration.

Note: After a successful `commit` command, you must give the write command to save the running configuration to the startup configuration.

Command Syntax

```
commit
```

Parameters

None

Default

N/A

Mode

All configuration modes

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#router ospf 1
(config-router)#exit
(config)#router isis 3
(config-router)#commit
(config-router)#exit
(config)#show running-config ospf
!
router ospf 1
!
(config)#show running-config isis
!
router isis 3
!
(config)#
```

If you try to `exit` or `end`, you are prompted to commit or abort first:

```
(config)#router bgp 10
(config-router)#bgp as-local-count 34
(config-router)#exit
(config)#exit
% Un-committed transactions present. Please do commit or abort before exiting.
(config)#end
% Un-committed transactions present. Please do commit or abort before exiting.
(config)#commit
(config)#show running-config bgp
```

```
!
router bgp 10
 bgp as-local-count 34
!
(config)#
```

Usage

OcNOS validates dependencies when you commit. In this example, bridge 1 must exist before you can create a VLAN on it:

```
(config)#vlan database
(config-vlan)#vlan 10 bridge 1
(config-vlan)#exit
(config)commit
```

Because of the unmet dependency, you get an error when you try to commit.

If you also create the bridge, the commit succeeds:

```
(config)#bridge 1 protocol mstp
(config)#vlan database
(config-vlan)#vlan 10 bridge 1
(config-vlan)#exit
(config)commit
```

In a single transaction, dependent configurations can be given in any order. Using the same example as before, you can create the bridge *after* the VLAN:

```
(config)#vlan database
(config-vlan)#vlan 10 bridge 1
(config-vlan)#exit
(config)#bridge 1 protocol mstp
(config)commit
```

OcNOS supports “hitless merges” and does not write to the candidate configuration if you make the same configuration in separate transactions. In this example, subinterface xe1.1 is not created the second time because it already exists:

```
(config)#interface xe1.1
(config-if)#commit
(config)#interface xe1.1
(config-if)#commit
```

OcNOS does not write to the candidate configuration if you create and delete the same entity in the same transaction. You must create the entity and delete it with separate commits.

Mode changes, action items (such as `clear interface counters`), and `show` commands are not part of a transaction and are not displayed by the show transaction current command.

© 2021 IP Infusion Inc. Proprietary

debug cml

Use this command to enable or disable CML sub-module logging.

Command Syntax

```
debug cml (enable|disable)(events|engine|transaction|database|replace|smi|all)
```

Parameters

`enable`	Enable debugging.
`disable`	Disable debugging.
`events`	Enable events debugging
`engine`	Enable engine debugging
`transaction`	Enable transaction debugging
`database`	Enable database debugging
`replace`	Enable replace debugging
`smi`	Enable SMI debugging
`all`	Enable all debugging

Defaault

By default, CML sub-module logging is disabled for all sub-modules.

Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.2.

Example

```
#debug cml enable transaction
```

show max-transaction limit

Use this command to display the maximum number of transactions.

Command Syntax

```
show max-transaction limit
```

Parameters

None

Default

N/A

Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#show max-transaction limit
Max-Transaction Limit is 30000
```


© 2021 IP Infusion Inc. Proprietary

show transaction current

Use this command to display the current transaction.

Mode changes, action items (such as `clear interface counters`), and `show` commands are not part of a transaction and are not displayed by this command.

Command Syntax

```
show transaction current
```

Parameters

None

Default

N/A

Mode

Exec mode and configure mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#interface eth3
(config-if)#description testing
(config-if)#mtu 664
(config-if)#exit
(config)#show transaction current
interface eth3
description testing
mtu 664
```

show transaction last-aborted

Use this command to display the last aborted transaction.

Command Syntax

```
show transaction last-aborted
```

Parameters

None

Default

N/A

Mode

Exec mode and configure mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#router isis 4
(config-router)#isis wait-timer 45
(config-router)#net 11.22.33
(config-router)#exit
(config)#commit
%% Invalid NET length -  /isis/isis-instance[instance='4']/config
(config)#show running-config isis
!
!
(config)#abort transaction
(config)#exit
#show transaction last-aborted
router isis 4
isis wait-timer 45
net 11.22.33
#
```


© 2021 IP Infusion Inc. Proprietary

show (xml|json) running-config

Use this command to display the running configuration for any top level object in data model in XML or JSON format.

Command Syntax

```
show (xml|json) running-config OBJECT_NAME
```

Parameters

`xml`	XML output format
`json`	JSON output format
`OBJECT_NAME`	Name of the object, such as ISIS or OSPF

Mode

Exec mode

Applicability

This command was introduced before OcNOS-SP version 4.2.

Example

To display the top level objects:

```
#show xml running-config
arp                 bfd                 bgp                 dhcp                evpn                evpn-mpls
interfaces          ip-global           isis                key-chains          lacp                layer2-global
ldp                 lldp                logging             mpls                neighbor-discovery  network-instances
ospfv2              pcep                ping                prefixes            routemaps           routing
rsvp-te             segment-routing     system-info         tacacs              time-ranges         vlan-classifier
vpls                vpws                vxlan
```

To show ISIS configuration in XML format:

```
#show xml running-config isis
<isis xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-isis">
<isis-instance xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-isis">
<instance>1</instance>
<config xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-isis">
<instance>1</instance>
<vrf-name>default</vrf-name>
</config>
</isis-instance>
</isis>
```

To show logging configuration in XML format:

```
#show xml running-config logging
<logging xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-logging">
<rsyslog>
<vrf>default</vrf>
<config>
<vrf>default</vrf>
```

```
<enable-rsyslog>rsyslog</enable-rsyslog>
</config>
</rsyslog>
</logging>
```

To show logging configuration in JSON format:

```
#show json running-config logging
{
"logging":{
"rsyslog":[
{
"vrf":"default",
"config":{
"vrf":"default",
"enable-rsyslog":"rsyslog"
}
}
]
}
}
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 8 DHCP Snooping Commands

This chapter describe the commands for DHCP snooping.

- debug ip dhcp snooping
- ip dhcp snooping database
- renew ip dhcp snooping binding database
- show debugging ip dhcp snooping
- show debugging ip dhcp snooping
- show ip dhcp snooping arp-inspection statistics bridge
- show ip dhcp snooping bridge
- show ip dhcp snooping binding bridge

© 2021 IP Infusion Inc. Proprietary

debug ip dhcp snooping

Use this command to enable the debugging DHCP snooping.

Use the `no` parameter to disable the debug options.

Command Syntax

```
debug ip dhcp snooping (event|rx|tx|packet|all)
no debug ip dhcp snooping (event|rx|tx|packet|all)
```

Parameters

`event`	Enable event debugging
`rx`	Enable receive debugging
`tx`	Enable transmit debugging
`packet`	Enable packet debugging
`all`	Enable all debugging

Default

By default all debugging options are disabled.

Command Mode

Exec mode and configure mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#debug ip dhcp snooping all
#no debug ip dhcp snooping packet
```


© 2021 IP Infusion Inc. Proprietary

ip dhcp snooping database

Use this command to write the entries in the binding table to persistent storage.

Command Syntax

```
ip dhcp snooping database bridge <1-32>
```

Parameters

<1-32>	Bridge number

Default

No default value is specified.

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#ip dhcp snooping database bridge 1
```

renew ip dhcp snooping binding database

Use this command to populate the binding table by fetching the binding entries from persistent storage.

Command Syntax

```
renew ip dhcp snooping (source|) binding database bridge <1-32>
```

Parameters

`<1-32>`	Bridge number
`source`	IP source guard

Default

No default value is specified.

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#renew ip dhcp snooping binding database bridge 1
```


© 2021 IP Infusion Inc. Proprietary

show debugging ip dhcp snooping

Use this command to display the enabled debugging options.

Command Syntax

```
show debugging ip dhcp snooping
```

Parameters

None

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#show debugging ip dhcp snooping
DHCP snoop debugging status:
DHCP snoop event debugging is on
DHCP snoop tx debugging is on
```

show ip dhcp snooping arp-inspection statistics bridge

Use this command to show dhcp dynamic ARP inspection related statistics on bridge.

Command Syntax

```
show ip dhcp snooping arp-inspection statistics bridge <1-32>
```

Parameters

`<1-32>`	Bridge number.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#show ip dhcp snooping arp-inspection statistics bridge 1

bridge      forwarded  dai dropped
------      ---------  -----------
1           9          1
```

Table 8-18 explains the fields in the output.

Table 8-18: show ip dhcp snooping arp-inspection statistics bridge fields

Field	Description
`bridge`	Bridge number.
`forwarded`	Number of forwarded packets.
`dai dropped`	Number of dropped packets.

© 2021 IP Infusion Inc. Proprietary

show ip dhcp snooping bridge

Use this command to display the DHCP configuration, including trusted ports, configured VLAN, active VLAN, and strict validation status.

Command Syntax

```
show ip dhcp snooping bridge <1-32>
```

Parameters

<1-32>	Bridge number

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#show ip dhcp snooping bridge 1

Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Disabled
Verification of hwaddr field is                       : Disabled
Strict validation of DHCP packet is                   : Disabled
DB Write Interval(secs)                               : 300
DHCP snooping is configured on following VLANs        : 20,30
DHCP snooping is operational on following VLANs       : 20,30

DHCP snooping trust is configured on the following Interfaces

Interface               Trusted
---------------         -------
xe1                     Yes

DHCP snooping IP Source Guard is configured on the following Interfaces

Interface               Source Guard
---------------         ------------
```

Table 8-19 explains the fields in the output.

Table 8-19: show ip dhcp snooping bridge fields

Field	Description
Bridge Group	Bridge number
DHCP snooping is	Whether DHCP snooping is enabled

Table 8-19: show ip dhcp snooping bridge fields (Continued)

Field	Description
DHCP snooping option82 is	Whether DHCP snooping option 82 is enabled
Verification of hwaddr field is	Whether verification of hwaddr field is enabled
Strict validation of DHCP packet is	Whether strict validation of DHCP packets is enabled
DB Write Interval(secs)	Database write interval in seconds
DHCP snooping is configured on following VLANs	VLANs on which DHCP snooping is enabled
DHCP snooping is operational on following VLANs	VLANs on which DHCP snooping is operating
Interface	Interface name
Trusted	Whether DHCP snooping trust is enabled on the interface
Source Guard	Whether DHCP snooping IP source guard is enabled on the interface

© 2021 IP Infusion Inc. Proprietary

show ip dhcp snooping binding bridge

Use this command to display the DHCP snooping binding table.

Command Syntax

```
show ip dhcp snooping binding bridge <1-32>
```

Parameters

<1-32>	Bridge number

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#show ip dhcp snooping binding bridge 1

Total number of static IPV4 entries                    : 0
Total number of dynamic IPV4 entries                   : 2
Total number of static IPV6 entries                    : 0
Total number of dynamic IPV6 entries                   : 0

MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   --------------
3cfd.fe0b.06e0       12.12.12.10       30         dhcp-snooping   20     xe12

3cfd.fe0b.06e0       30.30.30.30       480        dhcp-snooping   30     xe12
```

Table 8-20 explains the output .

Table 8-20: show ip dhcp snooping binding bridge fields

Field	Description
Total number of static IPV4 entries	Number of static IPV4 entries.
Total number of dynamic IPV4 entries	Number of dynamic IPV4 entries.
Total number of static IPV6 entries	Number of static IPV6 entries.
Total number of dynamic IPV6 entries	Number of dynamic IPV6 entries .
MacAddress	MAC address of the interface.
IP Address	IP address of the peer device.
Lease (sec)	DHCP lease time in seconds provided to untrusted IP addresses.
Type	Configured either statically or dynamically by the DHCP server.

Table 8-20: show ip dhcp snooping binding bridge fields

Field	Description
VLAN	Identifier of the number.
Interface	Interface is being snooped.

© 2021 IP Infusion Inc. Proprietary

CHAPTER 9 DHCPv6 Prefix delegation Commands

This chapter describes the Dynamic Host Configuration Protocol (DHCP) v6 Prefix delegation commands.

The prefix delegation feature lets a DHCP server assign prefixes chosen from a global pool to DHCP clients. The DHCP client can configure an IPv6 address on its LAN interface using the prefix it received. Then it send router advertisements including the prefix, allowing other devices to auto configure their own IPv6 addresses.

Enable OcNOS device DHCP Client to receive the prefixes from external DHCP Server and enable IPv6 address autoconfiguration of LAN interfaces and the respective host machines.

This feature enables the service providers to assign IP for the Customer Premise Equipment acting as a router between the service providers core network and subscribers internal network.

This chapter contains these commands:

- ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER
- ipv6 address PREFIX_FROM_SERVER X:X::X:X/M
- ipv6 address autoconfig
- show ipv6 dhcp interface

ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER

Use this command to enable the DHCPv6 client to request the prefix (IA_PD) for the interface.

Prefixes delegated by the DHCP server are stored in the general prefix called PREFIX_FROM_SERVER.

Use the no form of command to remove the IA_PD option from the DHCPv6 client request. And this CLI deletes the learned prefix if there are any.

Command Syntax

```
ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER
no ipv6 dhcp prefix-delegation
```

Parameters

`PREFIX_FROM_SERVER`

String with length of no more than 255 characters and designates the name of the learnt prefix.

Default

DHCPv6 Prefix delegation client is not enabled by default.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.9

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ipv6 dhcp prefix-delegation prefix_xe1
(config-if)#
```


© 2021 IP Infusion Inc. Proprietary

ipv6 address PREFIX_FROM_SERVER X:X::X:X/M

Use this command to configure the global IPv6 address using the learned prefix and user provided suffix.

Use the `no` form of this command to remove the configuration.

Command Syntax

```
ipv6 address PREFIX_FROM_SERVER X:X::X:X/M
no ipv6 address PREFIX_FROM_SERVER X:X::X:X/M
```

Parameters

`PREFIX_FROM_SERVER`
: Name of the prefix which stores the address-prefix learnt using prefix delegation enabled in the client interface

`X:X::X:X/M`
: Suffix address consists subnet id and host address. This value must start with '::', and end with /64 bit prefix.

Default

DHCPv6 IA_PD option is not requested by default.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.9

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ipv6 address dhcp
(config-if)#ipv6 dhcp prefix-delegation prefix_xe1
(config-if)#

(config)#interface xe3
(config-if)#ipv6 address prefix_xe1 ::1:0:0:0:1/64
(config-if)#
```

ipv6 address autoconfig

Use this command to enable autoconfiguration of IPv6 address in host interface. IPv6 address are formed using the Prefix learnt from RA and suffix formed using EUI-64 method.

Autoconfiguration of ipv6 address will be successful only when the received prefix length is 64.

Use the `no` form of this command to disable the ipv6 address autoconfiguration.

Command Syntax

```
ipv6 address autoconfig
```

Parameters

None

Default

No default value specified.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.9

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 address autoconfig
```


© 2021 IP Infusion Inc. Proprietary

show ipv6 dhcp interface

Use this command to display the DHCPv6 Prefix delegation information in the Requesting Router device

Command Syntax

```
show ipv6 dhcp interface
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 1.3.9

Examples

```
#show ipv6 dhcp interface
      xe1 is in client mode
      prefix name: prefix_xe1
      learned prefix: 1212:501:102::/48
      preferred lifetime 600, valid lifetime 600
      interfaces using the learned prefix
      xe3    1212:501:102:1::1
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 10 Digital Diagnostic Monitoring Commands

This chapter provides a description, syntax, and examples of DDM feature commands:

- clear ddm transceiver alarm
- clear ddm transceiver alarm all
- ddm monitor
- ddm monitor all
- ddm monitor interval
- debug ddm
- service unsupported-transceiver
- show controller details
- show supported-transceiver
- show interface transceiver details

clear ddm transceiver alarm

Use this command to clear the transceiver alarm in the DDM monitor at interface level.

Command Syntax

```
clear ddm transceiver alarm
```

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

To configure at interface level:

```
(config)#interface xe1
(config-if)#clear ddm transceiver alarm
```


© 2021 IP Infusion Inc. Proprietary

clear ddm transceiver alarm all

Use this command to clear the transceiver DDM alarm for alll interfaces.

Command Syntax

```
clear ddm transceiver alarm all
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

To configure at overall interface level:

```
OcNOS#clear ddm transceiver alarm all
```

ddm monitor

Use this command to enable DDM monitoring for interfaces which have a supported transceiver.

Use the `no` form of this command to disable DDM monitoring for all transceivers.

Command Syntax

```
ddm monitor
no ddm monitor
```

Parameters

None

Default

By default, DDM monitoring is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#ddm monitor
(config-if)#exit

(config)#interface xe1
(config-if)#no ddm monitor
(config-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

ddm monitor all

Use this command to enable DDM monitoring for all transceiver.s

Use the `no` form of this command to disable DDM monitoring for all transceivers.

Command Syntax

```
ddm monitor all
no ddm monitor all
```

Parameters

None

Default

By default, DDM monitoring is disabled.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ddm monitor all

(config)#no ddm monitor all
```

ddm monitor interval

Use this command to set the monitoring interval for the transceiver.

Use no form with this command to set the monitoring interval to its default.

Command Syntax

```
ddm monitor interval <60-3600>
no ddm monitor interval
```

Parameters

<60-3600>	Interval period in seconds.

Default

The default monitoring interval is 60 seconds.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ddm monitor interval 60
```


© 2021 IP Infusion Inc. Proprietary

debug ddm

Use this command to enable or disable debugging for DDM.

Command Syntax

```
debug ddm
no debug ddm
```

Parameters

None

Default

By default, debug command is not configured.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ddm
(config)#no debug ddm
```

service unsupported-transceiver

Use this command to allow an unsupported transceiver to be enabled for DDM monitoring.

Use the `no` form of this command to disable DDM on an unsupported transceiver.

Command Syntax

```
service unsupported-transceiver
no service unsupported-transceiver
```

Parameters

None

Default

By default, DDM on an unsupported transceiver is disabled.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#service unsupported-transceiver

(config)#no service unsupported-transceiver
```


© 2021 IP Infusion Inc. Proprietary

show controller details

Use this command to display the EEPROM details of transceiver.s

Command Syntax

```
show interface (IFNAME|) controllers
```

Parameters

IFNAME	Interface name. If not specified, this command displays details of all connected transceivers.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe52/1 controllers

Port Number             : 52
Vendor oui              : 0x0 0x17 0x6a
Vendor name             : AVAGO
Vendor part_no          : AFBR-79E4Z
serial_number           : QB380161
transceiver_type        : QSFP OR LATER
connector_type          : MPO 1x12
qsfp_transceiver_code   : 1X-LX
vendor_rev              : 01
date_code               : 110920   (yymmddvv, v=vendor specific)
encoding                : SONET
br_nominal              : 103     (100 MHz)
length_km               : 0
length_mtr              : 50
length_50mt             : 0
length_62_5mt           : 0
length_cu               : 0
cc_base                 : 0x7d
cc_ext                  : 0x28
DDM Support             : yes
```

show supported-transceiver

Use this command to display supported transceivers.

Command Syntax

```
show supported-transceiver
```

Parameters

None

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#show supported-transceiver
-----------------------------------------------------
          Transceiver DDM support list
-----------------------------------------------------
Type                        :SFP
Vendor Name                 :FINISAR CORP
Vendor Part Number          :FTLF8519P2BNL
DDM Supported               :Yes

Type                        :SFP
Vendor Name                 :EVERTZ
Vendor Part Number          :SFP10G-TR13S
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :AVAGO
Vendor Part Number          :AFBR-79E4Z
DDM Supported               :Yes
```


© 2021 IP Infusion Inc. Proprietary

show interface transceiver details

Use this command to display details of transceivers and threshold violations.

Command Syntax

```
show interface (IFNAME|) transceiver (detail|threshold violation|)
```

Parameters

`IFNAME`	Interface name. If not specified, this command displays details of all connected transceivers.
`detail`	Transceiver information such as voltage, temperature, power, and current.
`threshold violation`	Transceiver threshold violations.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface transceiver detail
PORT     Temp     High Alarm High Warn Low Warn Low Alarm
       (Celsius) (Celsius) (Celsius) (Celsius) (Celsius)

-------------------------------------------------------
5        30.060      95          90       -20      -25
6        30.463      95          90       -20      -25
52       34.486      75          70         0       -5
53       30.764      75          70         0       -5

         Voltage  High Alarm High Warn Low Warn Low Alarm
         (Volts)    (Volts)   (Volts)   (Volts)   (Volts)
-------------------------------------------------------
5        3.339       3.900     3.700    2.900     2.700
6        3.365       3.900     3.700    2.900     2.700
52       3.360       3.630     3.465    3.135     2.970
53       3.353       3.630     3.465    3.135     2.970

         Current  High Alarm High Warn Low Warn Low Alarm
          (mA)       (mA)       (mA)      (mA)     (mA)
-------------------------------------------------------
5        6.468       17.000    14.000   2.000     0.034
6        7.014       17.000    14.000   2.000     0.034
52       7.250       10.000    9.500    1.000     0.500
53       7.284       10.000    9.500    1.000     0.500
```

```
          RxPower  High Alarm High Warn Low Warn Low Alarm
          (dBm)       (dBm)       (dBm)      (dBm)     (dBm)
-----------------------------------------------------------
5         0.332        1.259      0.794     0.016      0.010
6         0.321        1.259      0.794     0.016      0.010
52        0.727        2.188      1.738     0.112      0.000
53        0.352        2.188      1.738     0.112      0.000

          TxPower  High Alarm High Warn Low Warn Low Alarm
           (mW)        (mW)        (mW)       (mW)      (mW)
-----------------------------------------------------------
5         0.342        0.631      0.631     0.079      0.067
6         0.342        0.631      0.631     0.079      0.067
```

Table 10-21 explains the output fields.

Table 10-21: show interface transceiver details output

Field	Description
Port	The number of the transceiver port.
Temp	Temperature in degrees Celsius of the transceiver.
Voltage	Voltage in Volts on the transceiver.
Current	Current in Milliamperes used by the transceiver.
Rx Power	Power received in Decibel-milliwatts (dBm) by the transceiver.
Tx Power	Power being transmitted in milliWatts by the transceiver.
High Alarm	The level that is needed to be reached to trigger a high alarm.
High Warn	The level that is needed to be reached to trigger a high warning.
Low Warn	The level that is needed to be reached to trigger a low warning.
Low Alarm	The level that is needed to be reached to trigger a low alarm.

© 2021 IP Infusion Inc. Proprietary

CHAPTER 11 Dynamic Host Configuration Protocol Client

This chapter describes the Dynamic Host Configuration Protocol (DHCP) client commands.

DHCP is used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). DHCP is implemented in a client-server model where DHCP clients request configuration data, such as an IP address, a default route, or DNS server addresses from a DHCP server.

This chapter contains these commands:

- feature dhcp
- ip address dhcp
- ip dhcp client request
- ipv6 address dhcp
- ipv6 dhcp address-prefix-length
- ipv6 dhcp client request
- ipv6 dhcp client
- show ipv6 dhcp vendor-opts

feature dhcp

Use this command to enable the DHCP client and DHCP relay on the device.

Use the `no` form of this command to disable the DHCP client and DHCP relay and delete any DHCP-related configuration.

Command Syntax

```
feature dhcp
no feature dhcp
```

Parameters

None

Default

By default, feature dhcp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature dhcp
```


© 2021 IP Infusion Inc. Proprietary

ip address dhcp

Use this command to get an IP address from a DHCP server for this interface.

Use the `no` form of this command to disable the DHCP client for this interface.

You can give the ip dhcp client request command before giving this command to request additional options.

Command Syntax

```
ip address dhcp
no ip address dhcp
```

Parameters

None

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip address dhcp
(config-if)#
```

ip dhcp client request

Use this command to add an option to a DHCP request.

Use the `no` form of this command to remove an option from a DHCP request.

Command Syntax

```
ip dhcp client request dns-nameserver
ip dhcp client request host-name
ip dhcp client request log-server
ip dhcp client request ntp-server
no ip dhcp client request dns-nameserver
no ip dhcp client request host-name
no ip dhcp client request log-server
no ip dhcp client request ntp-server
```

Parameters

`dns-nameserver`	List of DNS name servers (DHCP option 6)
`host-name`	Name of the client (DHCP option 12)
`ntp-server`	List of NTP servers (DHCP option 42)
`log-server`	List of log servers (DHCP option 7)

Default

By default, ip dhcp client request is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip dhcp client request ntp-server
```


© 2021 IP Infusion Inc. Proprietary

ipv6 address dhcp

Use this command to get an IPV6 address from a DHCP server for this interface.

Use the `no` form of this command to disable the DHCP client for this interface.

You can give the ipv6 dhcp client request command before giving this command to request additional options.

Command Syntax

```
ipv6 address dhcp
no ipv6 address dhcp
```

Parameters

None

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 address dhcp
(config-if)#
```

ipv6 dhcp address-prefix-length

Use this command to configure the prefix-length for dynamically allocated IPv6 address.

Use the `no` form of this command to unconfigure the prefix-length.

Command Syntax

```
ipv6 dhcp address-prefix-length <1-128>
no ipv6 dhcp address-prefix-length
```

Parameters

`<1-128>`	IPv6 address prefix length

Default

Default ipv6 address prefix length is 128

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ipv6 dhcp address-prefix-length 64
(config-if)
```


© 2021 IP Infusion Inc. Proprietary

ipv6 dhcp client request

Use this command to add an option to a DHCPv6 request.

Use the `no` form of this command to remove an option from a DHCPv6 request.

Note:

- Vendor-specific options allow a specific vendor to define a set of DHCP options that really make sense for their device or operating system.
- By default DHCPv6 uses four messages exchange (Solicit, Advertise, Request, and Reply) to obtain configuration parameters from a server. But when rapid-commit is specified, `dhcp6-client` will include a rapid-commit option in solicit messages and wait for an immediate reply instead of advertisements.The Rapid Commit option is used to signal the use of the two message exchange for address assignment.

Command Syntax

```
ipv6 dhcp client request dns-nameserver
ipv6 dhcp client request ntp-server
ipv6 dhcp client request domain-search
ipv6 dhcp client request vendor-specific-information
ipv6 dhcp client request rapid-commit
no ipv6 dhcp client request rapid-commit
no ipv6 dhcp client request vendor-specific-information
no ipv6 dhcp client request domain-search
no ipv6 dhcp client request ntp-server
no ipv6 dhcp client request dns-nameserver
```

Parameters

`dns-nameserver`	List of DNS name servers
`ntp-server`	Request for IPv6 NTP server
`domain-search`	Request for IPv6 domain search
`vendor-specific-information`	Request for IPv6 vendor-specific-information
`rapid-commit`	Request to enable rapid-commit

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3 and modified in OcNOS-DC version 5.0

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 dhcp client request dns-nameserver
(config-if)#

(config)#interface eth0
(config-if)#ipv6 dhcp client request ntp-server
(config-if)#exit

(config)#interface eth0
(config-if)#ipv6 dhcp client request domain-search
(config-if)#exit

(config)#interface eth0
(config-if)#ipv6 dhcp client request vendor-specific-information
(config-if)#exit

(config)#interface eth0
(config-if)#ipv6 dhcp client request rapid-commit
(config-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

ipv6 dhcp client

Use this command to configure DHCP client options to a DHCPv6 request.

Use the `no` form of this command to remove client options from a DHCPv6 request.

Note:

- `ipv6 dhcp client information-request` is used to get only stateless configuration parameters (i.e., without address).
- DAD-wait-time value is the maximum time (in seconds) that the client should wait for the duplicate address detection (DAD) to complete on an interface.
- DUID option override the default when selecting the type of DUID to use. By default, DHCPv6 dhclient creates an identifier based on the link-layer address (DUID-LL) if it is running in stateless mode (with -S, not requesting an address), or it creates an identifier based on the link-layer address plus a timestamp (DUID-LLT) if it is running in stateful mode (without -S, requesting an address).

Command Syntax

```
ipv6 dhcp client information-request
ipv6 dhcp client dad-wait-time <1-600>
ipv6 dhcp client duid (ll | llt)
no ipv6 dhcp client duid
no ipv6 dhcp client dad-wait-time
no ipv6 dhcp client information-request
```

Parameters

`information-request`	
	Request to enable information-request
`<1-600>`	DAD wait-time in seconds
`ll`	Link-layer address
`llt`	Link-layer address plus timestamp

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3 and modified in OcNOS-DC version 5.0

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 dhcp client information-request
(config-if)#exit
```

```
(config)#interface eth0
(config-if)#ipv6 dhcp client dad-wait-time 20
(config-if)#exit

(config)#interface eth0
(config-if)#ipv6 dhcp client duid ll
(config-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

show ipv6 dhcp vendor-opts

Use this command to display vendor-specific-information option value given by DHCP server.

Command Syntax

```
show ipv6 dhcp vendor-opts
```

Parameters

None

Command Mode

Executive mode

Applicability

This command is introduced in OcNOS-DC version 5.0

Examples

```
OcNOS#sh ipv6 dhcp vendor-opts
ifName              vendor-opts
==========          ====================
xe5                 IP Infusion Inc
OcNOS#
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 12 Dynamic Host Configuration Protocol Relay

This chapter describes the Dynamic Host Configuration Protocol (DHCP) relay commands.

In small networks with only one IP subnet, DHCP clients communicate directly with DHCP servers. When DHCP clients and associated servers do not reside on the same subnet, a DHCP relay agent can forward DHCP client messages to a DHCP server.

The DHCP client broadcasts on the local link, the relay agents receive the broadcast DHCP messages, and then generates a new DHCP message to send out on another interface.

The relay agent sets the gateway IP address (`giaddr` field of the DHCP packet) and, if configured, adds the relay agent information option (option 82) to the packet and forwards it to the DHCP server. The DHCP server replies to the client and the relay agent then retransmits the response on the local network.

This chapter contains these commands:

- clear ip dhcp relay option statistics
- clear ip dhcp relay statistics
- ip dhcp relay (configure mode)
- ip dhcp relay (interface mode)
- ip dhcp relay address
- ip dhcp relay information option
- ip dhcp relay information source-ip
- ip dhcp relay (L3VPN)
- ipv6 dhcp relay (configure mode)
- ipv6 dhcp relay (interface mode)
- ipv6 dhcp relay address
- ipv6 dhcp relay subscriber-id
- ipv6 dhcp relay (L3VPN)
- show ip dhcp relay
- show ip dhcp relay address
- show ip dhcp relay option statistics
- show ip dhcp relay statistics
- show ipv6 dhcp relay
- show ipv6 dhcp relay address
- show running-config dhcp

© 2021 IP Infusion Inc. Proprietary

clear ip dhcp relay option statistics

Use this command to clear ipv4 relay option statistics.

command syntax

```
clear ip dhcp relay option statistics
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 1.3.9.

Examples

```
OcNOS#clear ip dhcp relay option statistics
```


© 2021 IP Infusion Inc. Proprietary

clear ip dhcp relay statistics

Use this command to clear ipv4 relay statistics.

Command syntax

```
clear ip dhcp relay statistics
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 1.3.9.

Examples

```
OcNOS#clear ip dhcp relay statistics
```

ip dhcp relay (configure mode)

Use this command to enable the DHCP relay agent. The DHCP relay starts forwarding packets to the DHCP server address once configured.

Use the `no` form of this command to disable the DHCP relay agent.

Command Syntax

```
ip dhcp relay
no ip dhcp relay
```

Parameters

None

Default

By default, this feature is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip dhcp relay

#configure terminal
(config)#no ip dhcp relay
```


© 2021 IP Infusion Inc. Proprietary

ip dhcp relay (interface mode)

Use this command to configure an interface as a DHCP client-facing port.

Use the `no` form of this command to remove an interface as a DHCP client-facing port.

Command Syntax

```
ip dhcp relay
no ip dhcp relay
```

Parameters

None

Default

By default, this feature is enabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ip dhcp relay
```

ip dhcp relay address

Use this command to set an IPv4 address of a DHCP server to which a DHCP relay agent forwards client requests.

Use the `no` form of this command to remove the IP address of a DHCP server.

You must enable the DHCP relay feature with the ip dhcp relay (configure mode) command before you give this command.

Command Syntax

```
ip dhcp relay address A.B.C.D
no ip dhcp relay address A.B.C.D
```

Parameters

`A.B.C.D`	IPv4 address of the DHCP server

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay address 198.51.100.127

#configure terminal
(config)#ip dhcp relay address 198.51.100.127
```


© 2021 IP Infusion Inc. Proprietary

ip dhcp relay information option

Use this command to enable the device to insert and remove option 82 information in DHCP packets forwarded by the relay agent.

The option 82 suboption remote-id can be configured either as hostname or any string you provide.

Use the `no` form of this command to disable inserting and removing option-82 information.

Command Syntax

```
ip dhcp relay information option (|remote-id (hostname|WORD))
no ip dhcp relay information option (|remote-id)
```

Parameters

`remote-id`	Remote host Identifier, either the system hostname or a user-specified string.
`hostname`	Name of the host
`WORD`	Specify a string as remote-id(Maximum 255 alphanumeric characters)

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay information option remote-id hostname

#configure terminal
(config)#ip dhcp relay information option

#configure terminal
(config)#no ip dhcp relay information option
```

ip dhcp relay information source-ip

Use this command to enable DHCP relay option 82 link selection.

Use the `no` form of this command to disable DHCP relay option 82 link selection.

Command Syntax

```
ip dhcp relay information source-ip A.B.C.D
no ip dhcp relay information source-ip
```

Parameters

`A.B.C.D`	IPv4 address

Command Mode

Configure mode

VRF mode

Default

No default value is specified.

Applicability

This command was introduced before OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay information option source-ip 2.2.2.2

#configure terminal
(config)#ip dhcp relay information option source-ip 3.3.3.3
```


© 2021 IP Infusion Inc. Proprietary

ip dhcp relay (L3VPN)

Use this command to specify IPv4 DHCP relay to use tunnel interfaces as Uplink/Downlink.

Use the `no` form of this command to remove the usage of tunnel interfaces in IPv4 DHCP relay.

Command Syntax

```
ip dhcp relay (uplink|downlink) (l3vpn)
no ip dhcp relay (uplink|downlink) (l3vpn)
```

Parameters

`uplink`	DHCP Relay uplink interface
`downlink`	DHCP Relay downlink interface
`l3vpn`	L3VPN interface

Default

No default value is specified.

Command Mode

Configure and VRF mode

Applicability

This command was introduced in OcNOS-DC version 5.0.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay uplink l3vpn
(config-vrf)#end

#configure terminal
(config)#ip dhcp relay uplink l3vpn
```

ipv6 dhcp relay (configure mode)

Use this command to enable the DHCP IPv6 relay agent.

Use the `no` form of this command to disable the DHCP IPv6 relay agent.

Command Syntax

```
ipv6 dhcp relay
no ipv6 dhcp relay
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 dhcp relay

#configure terminal
(config)#no ipv6 dhcp relay
```


© 2021 IP Infusion Inc. Proprietary

ipv6 dhcp relay (interface mode)

Use this command to configure an interface as a DHCP IPv6 client-facing port.

Use the no form of this command to remove an interface as a DHCP IPv6 client-facing port.

Command Syntax

```
ipv6 dhcp relay
no ipv6 dhcp relay
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 dhcp relay
```

ipv6 dhcp relay address

Use this command to set an IPv6 address of a DHCP server to which a DHCP relay agent forwards client requests.

Use the `no` form of this command to remove an IPv6 address of a DHCP server.

You must enable the IPv6 DHCP relay feature with the ipv6 dhcp relay (configure mode) command before you give this command.

Command Syntax

```
ipv6 dhcp relay address X:X::X:X
no ipv6 dhcp relay address X:X::X:X
```

Parameters

`X:X::X:X`	IPv6 address of the DHCP server

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp relay address 2001:db8::7F

#configure terminal
(config)#ipv6 dhcp relay address 2001:db8::7F
```


© 2021 IP Infusion Inc. Proprietary

ipv6 dhcp relay subscriber-id

Use this command to configure subscriber-ID for IPv6 DHCP relay.

Use `no` form of this command to disable subscriber-id.

Command Syntax

```
ipv6 dhcp relay information option subscriber-id WORD
no ipv6 dhcp relay information option subscriber-id
```

Parameters

`WORD`	Subscriber ID

Default

No default value is specified.

Command Mode

Configuration mode and VRF mode

Applicability

This command is introduced in OcNOS-DC version 5.0

Examples

```
#configure terminal
(config)#ipv6 dhcp relay information option subscriber-id test
(config)#exit
```

ipv6 dhcp relay (L3VPN)

Use this command to specify IPv6 DHCP relay to use tunnel interfaces as Uplink/Downlink.

Use the `no` form of this command to remove the usage of tunnel interfaces in IPv6 DHCP relay.

Command Syntax

```
ipv6 dhcp relay (uplink|downlink) (l3vpn)
no ipv6 dhcp relay (uplink|downlink) (l3vpn)
```

Parameters

`uplink`	DHCP Relay uplink interface
`downlink`	DHCP Relay downlink interface
`l3vpn`	L3VPN interface

Default

No default value is specified.

Command Mode

Configure and VRF mode

Applicability

This command was introduced in OcNOS-DC version 5.0.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp relay uplink l3vpn
(config-vrf)#end

#configure terminal
(config)#ipv6 dhcp relay uplink l3vpn
```


© 2021 IP Infusion Inc. Proprietary

show ip dhcp relay

Use this command to display DHCP snooping relay status including DHCP server addresses configured on interfaces.

Command Syntax

```
show ip dhcp relay
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: vrf1
  Option 82: Enabled
  Remote Id: ocnos-device
  Link selection Source-IP: 1.4.5.6
  DHCP Servers configured: 9.9.9.9 8.8.8.8
  Interface                Uplink/Downlink
  ---------                -------------
  ge10                     Uplink
  ge28                     Downlink
VRF Name: default
  Option 82: Enabled
  Remote Id: OcNOS
  Link selection Source-IP: 1.2.3.4
  DHCP Servers configured: 1.1.1.1 2.2.2.2
  Interface                Uplink/Downlink
  ---------                -------------
  ge11                     Uplink
  ge27                     Downlink
```

Table 12-22 explains the output fields.

Table 12-22: show ip dhcp relay fields

Entry	Description
DHCP relay service	Whether the DHCP relay service is enabled.
VRF Name	Name of the VRF.
Option 82	Whether option 82 is enabled.
Remote Id	Remote host Identifier.

Table 12-22: show ip dhcp relay fields (Continued)

Entry	Description
Link selection Source-IP	Option 82 link selection source IP address
DHCP Servers configured	Addresses of DHCP servers configured
Interface	Interface name
Uplink/Downlink	Whether the interface is a server-facing port (uplink) or a client-facing port (downlink).

© 2021 IP Infusion Inc. Proprietary

show ip dhcp relay address

Use this command to display DHCP relay addresses.

Command Syntax

```
show ip dhcp relay address
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ip dhcp relay address
VRF Name: vrf1
  DHCP Servers configured: 9.9.9.9 8.8.8.8
VRF Name: default
  DHCP Servers configured: 1.1.1.1 2.2.2.2
```

Table 12-23 explains the output.

Table 12-23: show ip dhcp relay address interface fields

Entry	Description
VRF Name	Name of the VRF.
DHCP Servers configured	Addresses of DHCP servers configured

show ip dhcp relay option statistics

Use this command to display IPv4 DHCP Relay Agent Option(Option82) packet statistics

command syntax

```
show ip dhcp relay option statistics
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 1.3.9.

Examples

```
OcNOS#sh ip dhcp relay option statistics
VRF Name: default
Remote ID : OcNOS
Circuit ID : ge5
Number of packets forwarded without agent options  : 0
Dropped pkts due to bad relay agent information option : 0
Dropped pkts due to no RAI option match found : 0
Circuit ID option is not matching with known circuit ID : 0
Circuit ID option in matching RAI option was missing : 0
OcNOS#
```


© 2021 IP Infusion Inc. Proprietary

show ip dhcp relay statistics

Use this command to display IPv4 DHCP relayed packet statistics.

command syntax

```
show ip dhcp relay statistics
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 1.3.9.

Examples

```
OcNOS#sh ip dhcp relay statistics
VRF Name: default
Packets sent with a bogus giaddr : 0
Packets relayed from client to server : 12
Errors sending packets to servers : 0
Packets relayed from server to client : 1
Errors sending packets to clients : 0
OcNOS#
```

show ipv6 dhcp relay

Use this command to display DHCP IPv6 snooping relay status including DHCP IPv6 server addresses configured on interfaces.

Command Syntax

```
show ipv6 dhcp relay
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: vrf1
  DHCPv6 Servers configured: 2001::1
  Interface                Uplink/Downlink
  ---------                -------------
  ge35                     Uplink
  xe50                     Downlink
VRF Name: default
  DHCPv6 Servers configured: 3001::1
  Interface                Uplink/Downlink
  ---------                -------------
  ge34                     Uplink
  xe49                     Downlink
```

Table 12-24 explains the output fields.

Table 12-24: show ipv6 dhcp relay fields

Entry	Description
IPv6 DHCP relay service	Whether the DHCP relay service is enabled.
VRF Name	Name of the VRF.
DHCPv6 Servers configured	Addresses of DHCP servers configured
Interface	Interface name
Uplink/Downlink	Whether the interface is a server-facing port (uplink) or a client-facing port (downlink).

© 2021 IP Infusion Inc. Proprietary

show ipv6 dhcp relay address

Use this command to display DHCP IPv6 relay addresses.

Command Syntax

```
show ipv6 dhcp relay address
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ipv6 dhcp relay address
VRF Name: vrf1
  DHCPv6 Servers configured: 2001::1
VRF Name: default
  DHCPv6 Servers configured: 3001::1
```

Table 12-25 explains the output fields.

Table 12-25: show ipv6 dhcp relay address fields

Entry	Description
VRF Name	Name of the VRF.
DHCPv6 Servers configured	Addresses of DHCP servers configured

show running-config dhcp

Use this command to display DHCP settings in the running configuration.

Command Syntax

```
show running-config dhcp
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show running-config dhcp
ip vrf vrf1
 ip dhcp relay information option remote-id hostname
 ip dhcp relay address 1.1.1.2
ip dhcp relay information option remote-id hostname
ip dhcp relay information source-ip 5.4.3.2
ip dhcp relay address 1.1.1.1
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 13 Domain Name System

This chapter describes Domain Name System (DNS) commands. DNS translates easily-to-remember domain names into numeric IP addresses needed to locate computer services and devices. By providing a worldwide, distributed keyword-based redirection service, DNS is an essential component of the Internet.

The DNS database is hierarchical. When a client such as a Web browser gives a request that specifies a host name, the DNS resolver on the client first contacts a DNS server to determine the server's IP address. If the DNS server does not contain the needed mapping, it forwards the request to a different DNS server at the next higher level in the hierarchy. After potentially several forwarding and delegation messages are sent within the DNS hierarchy, the IP address for the given host eventually arrives at the resolver, that in turn completes the request over Internet Protocol (IP).

Note: The commands below are supported only on the “management” VRF.

The chapter contains these commands:

- debug dns client
- ip domain-list
- ip domain-lookup
- ip domain-name
- ip host
- ip name-server
- show hosts
- show running-config dns

debug dns client

Use this command to display DNS debugging messages.

Use the `no` form of this command to stop displaying DNS debugging messages.

Command Syntax

```
debug dns client
no debug dns client
```

Parameters

None

Default

By default, disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug dns client
```


© 2021 IP Infusion Inc. Proprietary

ip domain-list

Use this command to define a list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.

The `ip domain-list` command is similar to the ip domain-name command, except that with the `ip domain-list` command you can define a list of domains, each to be tried in turn.

If there is no domain list, the default domain name specified with the `ip domain-name` command is used. If there is a domain list, the default domain name is not used.

Use the `no` form of this command to remove a domain.

Command Syntax

```
ip domain-list (vrf management|) DOMAIN-NAME
no ip domain-list (vrf management|) DOMAIN-NAME
```

Parameters

`management`	Virtual Routing and Forwarding name
`DOMAIN-NAME`	Domain string (e.g. company.com)(Max Size 64)

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip domain-list mySite.com
```

ip domain-lookup

Use this command to enable DNS host name-to-address translation.

Use the `no` form of this command to disable DNS.

Command Syntax

```
ip domain-lookup (vrf management|)
no ip domain-lookup (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip domain-lookup
```


© 2021 IP Infusion Inc. Proprietary

ip domain-name

Use this command to set the default domain name used to complete unqualified host names (names without a dotted-decimal domain name).

The ip domain-list command is similar to the `ip domain-name` command, except that with the `ip domain-list` command you can define a list of domains, each to be tried in turn.

If a domain list has been created with `ip domain-list`, the default domain name is not used. If there is no domain list, the default domain name is used.

Use the `no` form of this command to disable DNS.

Command Syntax

```
ip domain-name (vrf management|) DOMAIN-NAME
no ip domain-name (vrf management|) DOMAIN-NAME
```

Parameters

`management`	Virtual Routing and Forwarding name
`DOMAIN-NAME`	Domain string (e.g. company.com)(Max Size 64)

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip domain-name company.com
```

ip host

Use this command to define static hostname-to-address mappings in DNS. You can specify one or two mappings in a command.

Use the `no` form of this command remove a hostname-to-address mapping.

Command Syntax

```
ip host (vrf management|) WORD A.B.C.D
ip host (vrf management|) WORD A.B.C.D A.B.C.D
ip host (vrf management|) WORD (X:X::X:X | A.B.C.D)
ip host (vrf management|) WORD (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)
no ip host (vrf management|) WORD A.B.C.D
no ip host (vrf management|) WORD A.B.C.D A.B.C.D
no ip host (vrf management|) WORD (X:X::X:X | A.B.C.D)
no ip host (vrf management|) WORD (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)
```

Parameters

`management`	Virtual Routing and Forwarding name
`WORD`	Host name, such as company.com
`X:X::X:X`	IPv6 address of the host
`A.B.C.D`	IPv4 address of the host

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip host company.com 192.0.2.1
```


© 2021 IP Infusion Inc. Proprietary

ip name-server

Use this command to add a DNS server address that is used to translate hostnames to IP addresses.

Use the no form of this command to remove a DNS server address.

Command Syntax

```
ip name-server (vrf management|) (X:X::X:X | A.B.C.D)
no ip name-server (vrf management|) (X:X::X:X | A.B.C.D)
```

Parameters

`management`	Virtual Routing and Forwarding name
`A.B.C.D`	IPv4 address of the host
`X:X::X:X`	IPv6 address of the host

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip name-server 123.70.0.23
```

show hosts

Use this command to display the DNS name servers and domain names.

Command Syntax

```
show hosts (vrf management|all)
```

Parameters

vrf	management or all VRFs

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command displaying two name servers: 10.10.0.2 and 10.10.0.88.

```
#show hosts
       VRF: management

DNS lookup is enabled
 Default domain      : .com
 Additional Domain   : .in .ac
 Name Servers        : 10.12.3.23
Host                                                                    Address
----                                                                    -------
test                                                                    10.12.12.67
test                                                                    10::23

 * - Values assigned by DHCP Client.
```

Table 13-26 explains the output fields.

Table 13-26: show hosts fields

Entry	Description
VRF: management	DNS configuration of specified VRF.
DNS lookup is enabled	DNS feature enabled or disabled.
Default domain	Default domain name used to complete unqualified host names (names without a dotted decimal domain name).
Additional Domain	A list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.
Name Servers	DNS server addresses that are used to translate hostnames to IP addresses.

© 2021 IP Infusion Inc. Proprietary

Table 13-26: show hosts fields

Entry	Description
Host	Static hostname-to-address mappings in DNS.
Test	Static hostname-to-address mappings in DNS.
* - Values assigned by DHCP Client.	Name-server indicates it has been learned dynamically.

show running-config dns

Use this command to show the DNS settings of the running configuration.

Command Syntax

```
show running-config dns (vrf management|)
```

Parameters

vrf	management

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config dns
ip domain-lookup vrf management
ip domain-name vrf management .com
ip domain-list vrf management .in
ip domain-list vrf management .ac
ip name-server vrf management 10.12.3.23
ip host vrf management test 10.12.12.67 10::23
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 14 Interface Commands

This chapter is a reference for each of the interface commands.

- admin-group
- bandwidth
- bandwidth-measurement uni-available-bandwidth static
- bandwidth-measurement uni-residual-bandwidth static
- bandwidth-measurement uni-utilized-bandwidth static
- clear hardware-discard-counters
- clear interface counters
- clear interface cpu counters
- clear interface fec
- clear ip prefix-list
- clear ipv6 neighbors
- clear ipv6 prefix-list
- debounce-time
- delay-measurement min-max-uni-link-delay
- delay-measurement uni-delay-variation
- delay-measurement uni-link-delay
- description
- duplex
- fec
- flowcontrol
- hardware-profile portmode
- if-arbiter
- interface
- ip address A.B.C.D/M
- ip address dhcp
- ip forwarding
- ip prefix-list
- ip proxy-arp
- ip remote-address
- ip unnumbered
- ip vrf forwarding
- ipv6 address
- ipv6 forwarding
- ipv6 prefix-list
- ipv6 unnumbered

© 2021 IP Infusion Inc. Proprietary

- link-debounce-time
- load interval
- loopback
- loss-measurement uni-link-loss
- monitor speed
- monitor queue-drops
- monitor speed threshold
- mtu
- multicast
- show flowcontrol
- show hardware-discard-counters
- show interface
- show interface capabilities
- show interface counters
- show interface counters drop-stats
- show interface counters error-stats
- show interface counters (indiscard-stats|outdiscard-stats)
- show interface counters protocol
- show interface counters queue-drop-stats
- show interface counters queue-stats
- show interface counters rate
- show interface counters speed
- show interface counters summary
- show interface fec
- show ip forwarding
- show ip interface
- show ip prefix-list
- show ip route
- show ip vrf
- show ipv6 forwarding
- show ipv6 interface brief
- show ipv6 route
- show ipv6 prefix-list
- show hosts
- show running-config interface
- show running-config interface ip
- show running-config interface ipv6
- show running-config ip
- show running-config ipv6

© 2021 IP Infusion Inc. Proprietary

- show running-config prefix-list
- shutdown
- speed
- switchport
- switchport allowed ethertype
- switchport protected
- transceiver

admin-group

Use this command to create an administrative group to be used for links. Each link can be a member of one or more, or no administrative groups.

When used in the interface mode, this command adds a link between an interface and a group. The name is the name of the group previously configured. There can be multiple groups per interface. The group is created in configure mode, then interfaces are added to the group in interface mode.

Use the `no` parameter with this command to disable this command.

Command Syntax

```
admin-group NAME
no admin-group NAME
```

Parameters

`NAME`	Name of the admin group to add.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, the `eth3` interface is added to the group `myGroup`:

```
#configure terminal
(config)#interface eth3
(config-if)#admin-group myGroup
```


© 2021 IP Infusion Inc. Proprietary

bandwidth

Use this command to specify a discrete, maximum bandwidth value for the interface.

Use the `no` parameter resets the interface's bandwidth to the default value.

Command Syntax

```
bandwidth BANDWIDTH
no bandwidth
```

Parameter

`BANDWIDTH`	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Default

Default bandwidth will be default speed of the interface. For LAG, default bandwidth will be collective bandwidth of its member ports. For VLAN interface, default bandwidth is 1 gigabits/sec.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe4
(config-if)#bandwidth 100m
```

bandwidth-measurement uni-available-bandwidth static

Use this command to advertise the available bandwidth between two directly connected OSPF/ISIS neighbors.

Use the `no` parameter with this command to unset available bandwidth on the current interface.

Command Syntax

```
bandwidth-measurement uni-available-bandwidth static BANDWIDTH
no bandwidth-measurement uni-available-bandwidth static
```

Parameter

`BANDWIDTH`	<0-999>k for 0 to 999 kilo bits/s
	<0-999>m for 0 to 999 mega bits/s
	<0-100>g for 0 to 100 giga bits/s

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
(config)#int eth2
(config-if)#bandwidth-measurement uni-available-bandwidth static 10k
(config-if)#commit

(config)#int eth2
(config-if)#no bandwidth-measurement uni-available-bandwidth static
(config-if)#commit
```


© 2021 IP Infusion Inc. Proprietary

bandwidth-measurement uni-residual-bandwidth static

Use this command to advertise the residual bandwidth between two directly connected OSPF/ISIS neighbors.

Use the `no` parameter with this command to unset residual bandwidth on the current interface.

Command Syntax

```
bandwidth-measurement uni-residual-bandwidth static BANDWIDTH
no bandwidth-measurement uni-residual-bandwidth static
```

Parameter

`BANDWIDTH`	<0-999>k for 0 to 999 kilo bits/s
	<0-999>m for 0 to 999 mega bits/s
	<0-100>g for 0 to 100 giga bits/s

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
(config)#interface ethernet 2
(config-if)#bandwidth-measurement uni-residual-bandwidth static 10g
(config-if)#commit

(config)#interface ethernet 2
(config-if)#no bandwidth-measurement uni-residual-bandwidth static
(config-if)#commit
```

bandwidth-measurement uni-utilized-bandwidth static

Use this command to advertise the utilized bandwidth between two directly connected OSPF/ISIS neighbors.

Use the `no` parameter with this command to unset utilized bandwidth on the current interface.

Command Syntax

```
bandwidth-measurement uni-utilized-bandwidth static BANDWIDTH
no bandwidth-measurement uni-utilized-bandwidth static
```

Parameter

`BANDWIDTH`	<0-999>k for 0 to 999 kilo bits/s
	<0-999>m for 0 to 999 mega bits/s
	<0-100>g for 0 to 100 giga bits/s

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
(config)#int eth2
(config-if)#bandwidth-measurement uni-utilized-bandwidth static 10m
(config-if)#commit

(config)#int eth2
(config-if)#no bandwidth-measurement uni-utilized-bandwidth static
(config-if)#commit
```


© 2021 IP Infusion Inc. Proprietary

clear hardware-discard-counters

Use this command to clear device level discard counters.

Command Syntax

```
clear hardware-discard-counters
```

Parameters

None

Command Mode

Exec mode

Applicability

The command is introduced before OcNOS version 1.3.

Examples

```
#clear hardware-discard-counters
```

clear interface counters

Use this command to clear the statistics on a specified interface or on all interfaces.

Note: This command is not supported on loopback interfaces or the out-of-band management (OOB) management interface.

Command Syntax

```
clear interface (IFNAME|) counters
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear interface xe0 counters
```


© 2021 IP Infusion Inc. Proprietary

clear interface cpu counters

Use this command to clear the CPU queue counters.

Command Syntax

```
clear interface cpu counters
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear interface cpu counters
```

clear interface fec

Use this command to clear FEC (forward error correction) statistics on a specified interface or on all interfaces.

Note: This command is not supported on loop-back interfaces or the out-of-band (OOB) management interface.

Command Syntax

```
clear interface (IFNAME|) fec
```

Parameters

IFNAME	Physical Interface name.

Default

None

Command Mode

Exec mode and Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear interface ce1/1 fec
```


© 2021 IP Infusion Inc. Proprietary

clear ip prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv4 interface.

Command Syntax

```
clear ip prefix-list
clear ip prefix-list WORD
clear ip prefix-list WORD A.B.C.D/M
```

Parameters

WORD	Name of the prefix-list.
A.B.C.D/M	IP prefix and length.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip prefix-list List1
```

clear ipv6 neighbors

Use this command to clear all dynamic IPv6 neighbor entries.

Command Syntax

```
clear ipv6 neighbors
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 neighbors
```


© 2021 IP Infusion Inc. Proprietary

clear ipv6 prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv6 interface.

Command Syntax

```
clear ipv6 prefix-list
clear ipv6 prefix-list WORD
clear ipv6 prefix-list WORD X:X::X:X/M
```

Parameters

WORD	Name of the prefix-list.
X:X::X:X/M	IP prefix and length.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 prefix-list List1
```

debounce-time

Use this command to set the debounce time for a interface.

The debounce timer avoids frequent updates (churn) to higher layer protocol during interface flapping. If the status of a link changes quickly from up to down and then back to up, the port debounce timer suppresses the link status notification. If the link transitions from up to down, but does not come back up, the port debounce timer delays the link status notification.

Note: Keep the following in mind when using the debounce timer:

- Debounce is not applicable for admin down operations.
- Debounce timer is supported only for physical L2 and L3 interfaces.
- The debounce flap-count refers to the number of flaps OcNOS receives while the debounce timer is running:
  - The flap-count is only updated if the timer is still running and OcNOS receives a link status event for the interface.
  - The flap-count is reset at the subsequent start of the debounce timer.
- Protocol-specific timers such as BFD which depend on the link status should be configured to a minimum of 1.5 times the value of the debounce timer. Otherwise it could affect the protocol states if the debounce timer is still running.

Use the `no` form of this command to turn-off the debounce timer on a interface.

Command Syntax

```
debounce-time <250-5000>
no debounce-time
```

Parameters

`<250-5000>`	Timer value in milliseconds.

Default

By default, disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#debounce-time 4000
```


© 2021 IP Infusion Inc. Proprietary

delay-measurement min-max-uni-link-delay

Use this command to advertise the minimum and maximum delay values between two directly connected IS-IS/OSPF neighbors.

The A bit is set when one or more measured values exceed a configured maximum threshold. The A bit is cleared when the measured value falls below its configured reuse threshold.

Use the no parameter with this command to unset min-max-uni-link-delay on the current interface.

Command Syntax

```
delay-measurement min-max-uni-link-delay (static <1-16777215> <1-16777215>) | (a-
  bit-threshold min <1-16777215> <1-16777215> max <1-16777215> <1-16777215>))
no delay-measurement min-max-uni-link-delay (static | a-bit-threshold)
```

Parameter

static	Static value
<1-16777215>	Minimum Unidirectional Link Delay in microseconds
<1-16777215>	Maximum Unidirectional Link Delay in microseconds
a-bit-threshold	Threshold values to set/clear A-bit
min	Reuse threshold
<1-16777215>	Reuse threshold value of Min-Delay in microseconds
<1-16777215>	Reuse threshold value of Max-Delay in microseconds
max	Maximum threshold
<1-16777215>	Maximum threshold value of Min-Delay in microseconds
<1-16777215>	Maximum threshold value of Max-Delay in microseconds

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#delay-measurement min-max-uni-link-delay static 12 23
(config-if)#no delay-measurement min-max-uni-link-delay static
(config-if)#delay-measurement min-max-uni-link-delay a-bit-threshold min 11 22
max 33 44
(config-if)#no delay-measurement min-max-uni-link-delay a-bit-threshold
```

delay-measurement uni-delay-variation

Use this command to advertise the average link delay variation between two directly connected IS-IS/OSPF neighbors.

Use the `no` parameter with this command to unset uni-delay-variation on the current interface.

Command Syntax

```
delay-measurement uni-delay-variation static <0-16777215>
no delay-measurement uni-delay-variation static
```

Parameter

`static`	Static value
`<0-16777215>`	Value in microseconds

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#delay-measurement uni-delay-variation static 12
(config-if)#no delay-measurement uni-delay-variation static
```


© 2021 IP Infusion Inc. Proprietary

delay-measurement uni-link-delay

Use this command to advertise average link delay between two directly connected IS-IS/OSPF neighbors.

a-bit-threshold represents the Anomalous (A) bit. The A bit is set when the static value exceeds its configured maximum threshold. The A bit is cleared when the static value falls below its configured reuse threshold.

Use the `no` parameter with this command to unset uni-link-delay on the current interface.

Command Syntax

```
delay-measurement uni-link-delay ((static <1-16777215>) | (a-bit-threshold min <1-16777215> max <1-16777215>))
no delay-measurement uni-link-delay (static | a-bit-threshold)
```

Parameter

`static`	Static value
`<1-16777215>`	Value in microseconds
`a-bit-threshold`	Threshold values to set/clear A-bit
`min`	Reuse threshold
`<1-16777215>`	Reuse threshold value in microseconds
`max`	Maximum threshold
`<1-16777215>`	Maximum threshold value in microseconds

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#delay-measurement uni-link-delay static 12
(config-if)#no delay-measurement uni-link-delay static
(config-if)#delay-measurement uni-link-delay a-bit-threshold min 11 max 22
(config-if)#no delay-measurement uni-link-delay a-bit-threshold
```

description

Use this command to assign an description to an interface.

Use the `no` parameter to remove an interface description.

Command Syntax

```
description LINE
no description
```

Parameter

`LINE`	Interface description.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example provides information about the connecting router for interface `eth1`.

```
Router#configure terminal
Router(config)#interface eth1
Router(config-if)#description Connected to Zenith's fas2/0
```


© 2021 IP Infusion Inc. Proprietary

duplex

Use this command to set the duplex mode for each interface.

Use the `no` parameter to remove the duplex mode.

Command Syntax

```
duplex (half|full)
no duplex
```

Parameter

`half`	Half-duplex mode.
`full`	Full-duplex mode.

Default

By default, duplex mode is full duplex.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#duplex full

(config-if)#no duplex
```

fec

Use this command to force/auto configure forward error correction (FEC) on a physical port.

Use the `no` parameter to enable automatic FEC configuration provisioning based on medium.

Command Syntax

```
fec (on|off|auto)
no fec
```

Parameter

`on`	Enable FEC.
`off`	Disable FEC.
`auto`	Automatically apply FEC for the below transceiver Ethernet compliance codes. Transceiver compliance codes can be fetched via the `show interface controller` command. Also, `fec auto` behavior is the same as `no fec`. 100G AOC (Active Optical Cable) or 25GAUI C2M AOC 100G ACC (Active Copper Cable) or 25GAUI C2M ACC 100G ACC or 25GAUI C2M ACC 100G AOC or 25GAUI C2M AOC 100GBASE-SR4 or 25GBASE-SR 100G AOC (Active Optical Cable) or 25GAUI C2M AOC

Default

By default, FEC mode is set to `auto`.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS-SP version 4.1.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#fec on
(config-if)#fec off

(config-if)#fec auto
```


© 2021 IP Infusion Inc. Proprietary

flowcontrol

Use this command to enable or disable flow control.

Flow control enables connected Ethernet ports to control traffic rates during periods of congestion by allowing congested nodes to pause link operations at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When a local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the period of congestion.

Use the `no` parameter with this command to disable flow control.

Command Syntax

```
flowcontrol both
flowcontrol send on
flowcontrol send off
flowcontrol receive on
flowcontrol receive off
no flowcontrol
```

Parameters

`both`	Specify flow control mode for sending or receiving.
`send`	Specify flow control mode for sending.
`receive`	Specify the flow control mode for receiving.
`off`	Turn off flow control.
`on`	Turn on flow control.

Default

The flow control is enabled globally and auto-negotiation is on, flow control is enabled and advertised on 10/100/1000M ports. If auto-negotiation is off or if the port speed was configured manually, flow control is neither negotiated with nor advertised to the peer.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#flowcontrol receive off

#configure terminal
(config)#interface eth1
(config-if)#flowcontrol receive on
```

```
(config)#interface eth1
(config-if)#no flowcontrol
```


© 2021 IP Infusion Inc. Proprietary

hardware-profile portmode

Use this command to set the global port mode.

Command Syntax

```
hardware-profile portmode (4X10g|40g)
```

Parameter

`4X10g`	Split all the 40G flex ports on the system
`40g`	Disable splitting on all flex ports and make all ports 40G

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#hardware-profile portmode 40g
```

if-arbiter

Use this command to discover new interfaces recently added to the kernel and add them to the OcNOS database.

This command starts the arbiter to check interface information periodically. OcNOS dynamically finds any new interfaces added to the kernel. If an interface is loaded dynamically into the kernel when OcNOS is already running, this command polls and updates the kernel information periodically.

Use the `no` parameter with this command to revert to default.

Command syntax

```
if-arbiter (interval <1-65535>|)
no if-arbiter
```

Parameter

`interval`	Interval (in seconds) after which NSM sends a query to the kernel.

Default

By default, `if-arbiter` is disabled. When interface-related operations are performed outside of OcNOS (such as when using the `ifconfig` command), enable `if-arbiter` for a transient time to complete synchronization. When synchronization is complete, disable it by giving the `noif-arbiter` command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#if-arbiter interval 5
```


© 2021 IP Infusion Inc. Proprietary

interface

Use this command to select an interface to configure, and to enter the `Interface` command mode.

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
interface IFNAME
no interface IFNAME
```

Parameter

`IFNAME`	Name of the interface.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows the use of this command to enter the `Interface` mode (note the change in the prompt).

```
#configure terminal
(config)#interface eth3
(config-if)#
```

ip address A.B.C.D/M

Use this command to specify that an IP address and prefix length will be used by this interface. If the `secondary` parameter is not specified, this command overwrites the primary IP address. If the `secondary` parameter is specified, this command adds a new IP address to the interface. The secondary address cannot be configured in the absence of a primary IP address. The primary address cannot be removed when a secondary address is present.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax

```
ip address A.B.C.D/M label LINE
ip address A.B.C.D/M (secondary|)
ip address A.B.C.D/M secondary label LINE
no ip address A.B.C.D/M label LINE
no ip address A.B.C.D/M secondary label LINE
no ip address (A.B.C.D/M (secondary|)|)
```

Parameters

`LINE`	Label of this address.
`secondary`	Make the IP address secondary.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth3
(config-if)#ip address 10.10.10.50/24
(config-if)#ip address 10.10.11.50/24 secondary
```


© 2021 IP Infusion Inc. Proprietary

ip address dhcp

Use this command to specify that a DHCP client will be used to obtain an IP address for an interface.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax

```
ip address dhcp
no ip address dhcp
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth3
(config-if)#ip address 10.10.10.50/24
(config-if)#ip address 10.10.11.50/24 secondary
(config-if)#ip address dhcp
```

ip forwarding

Use this command to turn on IP forwarding.

Use the `no` parameter with this command to turn off IP forwarding.

Command Syntax

```
ip forwarding
ip forwarding vrf NAME
no ip forwarding
no ip forwarding vrf NAME
```

Parameters

`NAME`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip forwarding
```


© 2021 IP Infusion Inc. Proprietary

ip prefix-list

Use this command to create an entry for a prefix list.

A router starts to match prefixes from the top of the prefix list and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

Use the parameters `ge` and `le` specify the range of the prefix length to be matched. When setting these parameters, set `le` to be less than 32 and `ge` to be less than `le` value.

Use the `no` parameter with this command to delete the prefix-list entry.

Command Syntax

```
ip prefix-list WORD
 (deny|permit) (A.B.C.D/M|any)
 (deny|permit) A.B.C.D/M eq <0-32>
 (deny|permit) A.B.C.D/M ge <0-32>
 (deny|permit) A.B.C.D/M ge <0-32> le <0-32>
 (deny|permit) A.B.C.D/M le <0-32>
 (deny|permit) A.B.C.D/M le <0-32> ge <0-32>
 seq <1-4294967295> (deny|permit) (A.B.C.D/M|any)
 seq <1-4294967295> (deny|permit) A.B.C.D/M eq <0-32>
 seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32>
 seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32> le <0-32>
 seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32>
 seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32> ge <0-32>
 description LINE
 no seq <1-4294967295> (deny|permit) (A.B.C.D/M|any)
 no description LINE
 no description
no ip prefix-list WORD
ip prefix-list sequence-number
no ip prefix-list sequence-number
```

Parameters

`WORD`	Name of the prefix list.
`deny`	Reject packets.
`permit`	Accept packets.
`A.B.C.D/M`	IP address mask and length of the prefix list mask.
`eg`	Exact prefix length match
`le`	Maximum prefix length match
`ge`	Minimum prefix length match

`<0-32>`	Prefix length to match
`<1-4294967295>`	Sequence number of the prefix list.
`any`	Take all packets of any length. This parameter is the same as using 0.0.0.0/0 le 32 for `A.B.C.D/M`.
`sequence-number`	To suppress sequence number generation, give the `no ip prefix-list sequence-number` command. If you disable the generating sequence numbers, you must specify the sequence number for each entry using the sequence number parameter in the `ip prefix-list` command. To enable sequence number generation, give the `ip prefix-list sequence-number` command.
`LINE`	Up to 80 characters describing this prefix-list.

Default

No default value is specified

Command Mode

Configure mode

IP prefix-list mode

Applicability

This command was introduced before OcNOS Version SP 4.0.

Examples

In this configuration, the `ip prefix-list` command matches all, but denies the IP address range, 76.2.2.0.

```
#conf t
(config)#router bgp 100
(config-router)#network 172.1.1.0
(config-router)#network 172.1.2.0
(config-router)#
(config-router)#neighbor 10.6.5.3 remote-as 300
(config-router)#neighbor 10.6.5.3 prefix-list mylist out
(config-router)#exit
(config)#ip prefix-list mylist
(config-ip-prefix-list)#seq 5 deny 76.2.2.0/24
(config-ip-prefix-list)#seq 10 permit 0.0.0.0/0
```


© 2021 IP Infusion Inc. Proprietary

ip proxy-arp

Use this command to enable the proxy ARP feature on an interface.

Use the `no` parameter to disable the proxy ARP feature on an interface.

Command Syntax

```
ip proxy-arp
no ip proxy-arp
```

Parameters

None

Default

By default, the ip proxy-arp is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ip proxy-arp
```

ip remote-address

Use this command to set the remote address (far end) on a point-to-point non multi-access link. This command can be used only on unnumbered interfaces. When a new remote-address is configured, the old address gets overwritten.

Use the `no` parameter to disable this function.

Command Syntax

```
ip remote-address A.B.C.D/M
no ip remote-address
```

Parameter

`A.B.C.D/M`	IP address and prefix length of the link remote address.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface ppp0
(config-if)#ip unnumbered eth1
(config-if)#ip remote-address 1.1.1.1/32
```


© 2021 IP Infusion Inc. Proprietary

ip unnumbered

Use this command to enable IP processing without an explicit address on a point-to-point non multi-access link. Moreover, this command lets an interface borrow the IP address of a specified interface to enable IP processing on a point-to-point interface without assigning it an explicit IP address. In this way, the IP unnumbered interface can borrow the IP address of another interface already configured on the router to conserve network and address space.

Use the `no` parameter with this command to remove this feature on an interface.

Command Syntax

```
ip unnumbered IFNAME
no ip unnumbered
```

Parameter

`IFNAME`	Interface name.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example creates a tunnel on `eth1`.

```
(config)#interface lo
(config-if)#ip address 127.0.0.1/8
(config-if)#ip address 33.33.33.33/32 secondary
(config-if)#exit
(config)#interface eth1
(config-if)#ip address 10.10.10.145/24
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode vxlan
(config-if)#ip unnumbered eth1
(config-if)#exit
(config)#router ospf
(config-router)#network 10.10.10.0/24 area 0
```

ip vrf forwarding

This command associates an interface with a VRF.

Use the `no` parameter with this command to unbind an interface.

Note: When you give this command in interface configuration or subinterface configuration mode of the parent VR, the IP address and other attributes of the interface are deleted from the interface. After giving this command, the IP attributes must then be configured in the context of the VRF.

Note: The Out Of Band (OOB) management port is part of the “management” VRF. Also, this port cannot be moved out of “management” VRF.

Command Syntax

```
ip vrf forwarding WORD
no ip vrf forwarding WORD
```

Parameter

`WORD`	Name of the VRF.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf myVRF
(config-vrf)#exit
(config)#interface eth1
(config-if)#ip vrf forwarding myVRF
```


© 2021 IP Infusion Inc. Proprietary

ipv6 address

Use this command to set the IPv6 address of an interface.

Use the `no` form of this command to disable this function.

Note: This command is also used to configure an IPv6 link-local address for an interface.

Command Syntax

```
ipv6 address X:X::X:X/M
ipv6 address X:X::X:X/M anycast
no ipv6 address X:X::X:X/M
```

Parameters

`X:X::X:X/M`	IP destination prefix and a mask length.
`anycast`	Make an anycast address which is assigned to a set of interfaces that belong to different devices. A packet sent to an anycast address is delivered to the closest interface (as defined by the routing protocols in use) identified by the anycast address

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 address 3ffe:506::1/64

#configure terminal
(config)#interface eth4
(config-if)#ipv6 address fe80::ab8/64
```

ipv6 forwarding

Use this command to turn on IPv6 forwarding.

Use the `no` parameter with this command to turn off IPv6 forwarding.

Command Syntax

```
ipv6 forwarding
ipv6 forwarding vrf NAME
no ipv6 forwarding
no ipv6 forwarding vrf NAME
```

Parameters

`NAME`	Virtual Routing or Forwarding name

Default

No default value is specified

Command Mode

Command mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 forwarding
```


© 2021 IP Infusion Inc. Proprietary

ipv6 prefix-list

Use this command to create an entry for an ipv6 prefix-list.

Router starts to match prefixes from the top of the prefix list, and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

The parameters `ge` and `le` specify the range of the prefix length to be matched.

Use the `no` parameter with this command to delete the prefix-list entry.

Command Syntax

```
ipv6 prefix-list WORD
 (deny|permit) (X:X::X:X/M|any)
 (deny|permit) X:X::X:X/M ge <0-128>
 (deny|permit) X:X::X:X/M ge <0-128> le <0-128>
 (deny|permit) X:X::X:X/M le <0-128>
 (deny|permit) X:X::X:X/M le <0-128> ge <0-128>
 seq <1-4294967295> (deny|permit) (X:X::X:X/M|any)
 seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128>
 seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128> le <0-128>
 seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128>
 seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128> ge <0-128>
 description LINE
 no seq <1-4294967295> (deny|permit) (X:X::X:X/M|any)
 no description
no ipv6 prefix-list WORD
ipv6 prefix-list sequence-number
no ipv6 prefix-list sequence-number
```

Parameters

`WORD`	Name of the prefix list.
`deny`	Reject packets.
`permit`	Accept packets.
`X:X::X:X/M`	IP address mask and length of the prefix list mask.
`any`	Take all packets of any length. This is the same as specifying ::/0 for X:X::X:X/M.
`eg`	Exact prefix length match
`le`	Maximum prefix length match
`ge`	Minimum prefix length match
`<0-128>`	Prefix length to match
`<1-4294967295>`	Sequence number of the prefix list.
`sequence-number`	

	To suppress sequence number generation, give the `no ipv6 prefix-list sequence-number` command. If you disable the generating sequence numbers, you must specify the sequence number for each entry using the sequence number parameter in the `ipv6 prefix-list` command. To enable sequence number generation, give the `ipv6 prefix-list sequence-number` command.
`LINE`	Up to 80 characters describing this prefix-list.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 prefix-list mylist
(config-ipv6-prefix-list)#seq 12345 deny 3ffe:345::/16 le 22 ge 14
```


© 2021 IP Infusion Inc. Proprietary

ipv6 unnumbered

Use this command to enable IPv6 processing without an explicit address, on a point-to-point non multi-access link.

This command lets an interface borrow the IPv6 address of a specified interface to enable IPv6 processing on a point-to-point interface without assigning it an explicit IPv6 address. In this way, the IPv6 unnumbered interface can borrow the IPv6 address of another interface already configured on the router to conserve network and address space.

Use the `no` parameter with this command to remove this feature on an interface.

Command Syntax

```
ipv6 unnumbered IFNAME
no ipv6 unnumbered
```

Parameter

`IFNAME`	Interface name.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example creates a tunnel on eth1:

```
#configure terminal
(config)#interface lo
(config-if)#ipv6 address::1/128
(config-if)#exit
(config)#interface eth1
(config-if)#ipv6 address fe80::20e:cff:fe6e:56dd/64
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode vxlan
(config-if)#ipv6 unnumbered eth1
(config-if)#ipv6 router ospf area 0 tag 1
(config-if)#exit
(config)#router ipv6 ospf 1
(config-router)#router-id 10.70.0.145
```

link-debounce-time

Use this command to set the debounce time for linkup and linkdown transitions for the interface.

User can set only one of the timers (either linkup or linkdown) by setting the other one to 0.

Use the `no` form of this command to turn off the link debounce timer on the interface.

Command Syntax

```
link-debounce-time <0-5000> <0-5000>
no link-debounce-time
```

Parameter

`<0-5000>`	timer value in milliseconds for the linkup transition
`<0-5000>`	timer value in milliseconds for the linkdown transition

Default

By default, it is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#link-debounce-time 4000 5000
(config-if)#link-debounce-time 0 5000
(config-if)#link-debounce-time 3000 0
```


© 2021 IP Infusion Inc. Proprietary

load interval

Use this command to configure the interval for which average traffic rate need to be shown. Intervals can be configured in steps of 30 seconds.

Use the no parameter with this command to set the load interval to its default.

Command Syntax

```
load-interval <30-300>
no load-interval
```

Parameter

<30-300>	Load period in multiples of 30 seconds.

Default

By default, load interval is 300 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#load-interval 30
(config-if)#no load-interval
```

loopback

Use this command to set the ethernet loopback mode on the interface.

Use the `no` form of this command to remove loopback on the interface.

Note: Remote PHY loopback supported only on a single serdes lane of serdes-quad at a time. So below cases are not supported:

1. 100G and 40G interface mode.
2. 2x50G port breakout mode.
3. In 4x10 or 4x25G breakout mode, at a time only one interface is supported.
4. If interface is part of port-group, at a time only one interface is supported.

Command Syntax

```
loopback ((tx (mac|phy))|(rx phy))
```

Parameter

The parameters for Tx are MAC or PHY and for Rx is PHY.

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command is introduced before OcNOS-DC version 5.0.

Example

```
#configure terminal
(config)#interface xe0
(config-if)#loopback tx mac
(config-if)#exit

(config)#interface xe0
(config-if)#loopback tx phy
(config-if)#exit

(config)#interface xe0
(config-if)#loopback rx phy
(config-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

loss-measurement uni-link-loss

Use this command to advertise the loss (as a packet percentage) between two directly connected IS-IS/OSPF neighbors.

The A bit is set when the measured value of this parameter exceeds its configured maximum threshold. The A bit is cleared when the measured value falls below its configured reuse threshold.

Use the `no` parameter with this command to unset uni-link-loss on the current interface.

Command Syntax

```
loss-measurement uni-link-loss ((static VALUE) | (a-bit-threshold min VALUE max
  VALUE))
no loss-measurement uni-link-loss (static | a-bit-threshold)
```

Parameter

`static`	Static value
`VALUE`	Loss percentage in six precision float format. eg: 3.123456
`a-bit-threshold`	Threshold values to set/clear A-bit
`min`	Reuse threshold
`VALUE`	Reuse threshold percentage in six precision float format. eg:3.123456
`max`	Maximum threshold
`VALUE`	Maximum threshold percentage in six precision float format. eg:3.123456

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#loss-measurement uni-link-loss static 12.3
(config-if)#no loss-measurement uni-link-loss static
(config-if)#loss-measurement uni-link-loss a-bit-threshold min 1.12 max 2.2
(config-if)#no loss-measurement uni-link-loss a-bit-threshold
```

monitor speed

Use this command to enable speed monitoring on interface.

Use the `no` parameter with this command to disable monitoring.

Command Syntax

```
monitor speed
no monitor speed
```

Default

By default, speed monitoring will be disabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#monitor speed
(config-if)#no monitor speed
```


© 2021 IP Infusion Inc. Proprietary

monitor queue-drops

Use this command to enable queue-drops monitoring on interface.

Use the `no` parameter with this command to disable monitoring.

Command Syntax

```
monitor queue-drops
no monitor queue-drops
```

Default

By default, queue-drops monitoring will be disabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#monitor queue-drops
(config-if)#no monitor queue-drops
```

monitor speed threshold

Use this command to modify default speed monitor threshold on interface.

Use the `no` parameter with this command to set the monitor speed threshold to its default.

Note: Warning threshold must be greater than recovery threshold and it is recommended to keep a difference of 10 percent to avoid frequent notifications caused by variations in average speed.

Command Syntax

```
monitor speed threshold warning <1-100> recovery <1-100>
no monitor speed threshold
```

Parameter

`<1-100>`	Warning level threshold value in percentage
`<1-100>`	Recovery level threshold value in percentage

Default

By default, warning threshold is 90 percentage and recovery is 80 percentage.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)# monitor speed threshold warning 80 recovery 70
(config-if)#no monitor speed threshold
```


© 2021 IP Infusion Inc. Proprietary

mtu

Use this command to set the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) for an interface

Use the `no` parameter with this command to set the MTU to its default.

Command Syntax

```
mtu <64-65536>
no mtu
```

Parameter

`<64-65536>`	Specify the size of MTU in bytes: `<64-16338>` for L2 packet `<576-9216>` for L3 IPv4 packet `<1280-9216>` for L3 IPv6 packet `<576-65536>` for IPv4 packet `<1280-65536>` for IPv6 packet on loopback interface

Default

By default, MTU is 1500 bytes

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#mtu 120
```

multicast

Use this command to set the multicast flag for the interface.

Use the `no` form of this command to disable this function.

Command Syntax

```
multicast
no multicast
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#multicast
```


© 2021 IP Infusion Inc. Proprietary

show flowcontrol

Use this command to display flow control information.

Command Syntax

```
show flowcontrol
show flowcontrol interface IFNAME
```

Parameters

`interface IFNAME`	Specify the name of the interface to be displayed.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show flowcontrol interface` command displaying flow control information:

```
#show flowcontrol interface ge1
Port    Send FlowControl    Receive FlowControl RxPause TxPause

        admin    oper         admin    oper

-----   ------- --------     ------- --------      ------- -------
ge1      on       on            on       on             0       0
#
```

Table 14-27 explains the show command output fields.

Table 14-27: show flow control output

Entry	Description
Port	Interface being checked for flowcontrol.
Send admin	Displays whether the flowcontrol send process is administratively on or off.
FlowControl oper	Displays whether send flowcontrol is on or off on this interface.
Received admin	Displays whether the flowcontrol receive process is administratively on or off.
FlowControl oper	Displays whether receive flowcontrol is on or off on this interface.
RxPause	Number of received pause frames.
TxPause	Number of transmitted pause frames.

© 2021 IP Infusion Inc. Proprietary

show hardware-discard-counters

Use this command to check device level discard counters.

Command Syntax

```
show hardware-discard-counters
```

Parameters

None

Command Mode

Exec mode

Applicability

The command is introduced before OcNOS version 1.3.

Qumran devices do not support discard counters per interface. Only global level counters are available for advanced debugging using the show hardware-discard-counters command.

Examples

```
#show hardware-discard-counters
+-------------------------------------------------+--------------------+
| Registers                                       | Core 0             |
+-------------------------------------------------+--------------------+
 CGM_VOQ_SRAM_ENQ_RJCT_PKT_CTR                     437
   Reason : QNUM_NOT_VALID                         Y
 EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER            8894
   Reason : SRC_EQUAL_DEST_INT                     Y
```

See Table 14-28 and Table 14-29 for details:

Table 14-28: Table detailing about counters supported

Register	Description
CGM_VOQ_SRAM_ENQ_RJCT_PKT_CTR for QAX	Drop is due to PPdecision to drop, or invalid destination received from PPblocks.
IQM_QUEUE_ENQ_DISCARDED_PACKET_COUNTER for QMX	The packet DP (Drop Precedence) is higher than the configured Drop DP.
EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER	Seen with unknown unicast frames, source and destination learnt from same interface.

© 2021 IP Infusion Inc. Proprietary

Table 14-29: Table detailing about reasons supported

Register	Description
QNUM_NOT_VALID for QAX QUEUE_NOT_VALID_STATUS for QMX	Seen with Vlan Discards, ACL Drops, Storm Control, STP Blocked Port.
DP_LEVEL_RJCT for QAX DP_LEVEL_STATUS for QMX	Seen with Policer Discards.
SRC_EQUAL_DEST_INTF	Seen when traffic is not learned, but is still forwarded/flooded.

show interface

Use this command to display interface configuration and status information.

Command Syntax

```
show interface (IFNAME|)
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1
Interface xe1/1
  Scope: both
  Flexport: Breakout Control Port (Active): Break Out Enabled
  Hardware is ETH  Current HW addr: ecf4.bb6e.934b
  Physical:ecf4.bb6e.934b  Logical:(not set)
  Port Mode is access
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full(auto) link-speed 1g(auto)
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
DHCP client is disabled.
  Last Flapped: 2016 Nov 05 22:40:23 (00:19:25 ago)
  Statistics last cleared: 2016 Nov 05 04:49:55 (18:09:53 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 256 bits/sec, 0 packets/sec
  RX
    unicast packets 39215813 multicast packets 0 broadcast packets 0
    input packets 39215813 bytes 2666662432
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 38902 multicast packets 437 broadcast packets 0
    output packets 437 bytes 28018
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```


© 2021 IP Infusion Inc. Proprietary

Table 14-30 explains the output fields.

Table 14-30: show interface output details

Field	Description
Scope	Interface can be used for communication within the device and outside the device (Both).
Flexport	Specifies whether the ports has Breakout capabilities or is a Non-Control Port.
Breakout Control Port (Active)	Specifies whether Breakout is active or disabled.
Hardware is ETH Current HW addr	The MAC address of the interface.
Physical	Displays the physical MAC address of the interface.
Logical	Displays the logical MAC address (if any) of the interface.
Port Mode	Displays the port mode: Router, VLAN access, switch, or trunk.
Interface index	Index number, Metric, MTU size, duplex-full (auto) or half-duplex, minimum link speed in gigabits, and if the interface is up, broadcasting, and multicasting.
VRF Binding	Show whether the interface is VRF bound and (if bound) with what VRF, if Label Switching is enabled or disabled, and if a virtual circuit is configured.
DHCP client	The state of the DHCP client – whether this interface is connected to a DHCP server.
Last Flapped	Date and time when the interface last flapped.
Statistics last cleared	Date and time when the interface's statistics were cleared.
5 minute input rate	Input rate in bits/second and packets/second
5 minute output rate	Output rate in bits/second and packets/second
RX	Counters for unicast packets, multicast packets, broadcast packets, input packets, bytes, jumbo packets, runts, giants, CRC errors, fragments, jabbers, input errors, input with dribble input discards, and receive pause.
TX	Counters for unicast packets, multicast packets, broadcast packets, output packets, bytes, jumbo packets, output errors, collisions, differed packets, input late collisions, output discards, and transmit pause.

© 2021 IP Infusion Inc. Proprietary

show interface capabilities

Use this command to display interface capabilities

Command Syntax

```
show interface (IFNAME|) capabilities
```

Parameters

IFNAME	Displays the name of a specific interface for which status and configuration data is desired.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 capabilities
xe1/1
Speed(FD) : 10MB,100MB,1000MB,10GB,20GB,40GB
Interface : xgmii
Medium : copper
Loopback : none,MAC,PHY
Pause : pause_tx,pause_rx,pause_asymm
Flags : autoneg
Encap : IEEE,HIGIG,HIGIG2
```

Table 14-31 explains the show command output fields.

Table 14-31: show interface capabilities output details

Field	Description
Interface number	The identifying ID number of the interface – eht0, xe1, etc.
Speed (FD)	The Flexible Data-Rates (FD) of the interface
interface	XAUI is a standard for extending the XGMII (10 Gigabit Media Independent Interface) between the MAC and PHY layer of Gigabit Ethernet.
Medium	Members have to have the same medium type configured. This only applies to Ethernet port-channel. Copper, fiber optics, etc.
Loop back	The loop back between the MAC and PHY layers.
Pause	Pause transmit, pause receive, pause asymmetrically.

© 2021 IP Infusion Inc. Proprietary

Table 14-31: show interface capabilities output details

Field	Description
Flags	Interface flags set for Auto-negotiation.
Encap	Encapsulation – IEEE, HIGIG, and HIGIG2 specifications – HIGIG is a proprietary protocol that is implemented by Broadcom. The HIGIG protocol supports various switching functions. The physical signaling across the interface is XAUI, four differential pairs for receive and transmit (SerDes), each operating at 3.125 Gbit/s.

show interface counters

Use this command to display the ingress and egress traffic counters on the interface.

Note: Counters are meant for debugging purpose and the accuracy of the transmit discard counter is not guaranteed in all scenarios.

Command Syntax

```
show interface (IFNAME|) counters (active|)
show interface cpu counters
```

Parameter

IFNAME	Interface name.
active	Statistics for link-up interfaces.
cpu	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 counters
Interface xe1/1
  Scope: both
  Rx Packets: 1000
  Rx Bytes: 1000000
  Rx Unicast Packets: 1000
  Rx Packets from 512 to 1023 bytes: 1000
  Tx Packets: 3897
  Tx Bytes: 249408
  Tx Multicast Packets: 3897
  Tx Packets with 64 bytes: 3897
  Tx Packet rate: 1 pps
  Tx Bit rate: 255 bps

#show interface cpu counters
CPU Interface
  Tx Packets: 104508
  Tx Bytes: 7106272
  Tx Discard Packets: 89613672
  Tx Discard Bytes: 5735237844
  Rx Discard Packets: 11938
```

Table 14-32 explains the output fields.

© 2021 IP Infusion Inc. Proprietary

Table 14-32: show interface counters output details

Field	Description
Receive Counters	Rx Packets Rx Bytes Rx Unicast Packets Rx Multicast Packets Rx Broadcast Packets Rx Packets with 64 bytes Rx Packets from 65 to 127 bytes Rx Packets from 128 to 255 bytes Rx Packets from 256 to 511 bytes Rx Packets from 512 to 1023 bytes Rx Packets from 1024 to 1518 bytes Rx Packets from 1519 to 2047 bytes Rx Packets from 2048 to 4095 bytes Rx Packets from 4096 to 9216 bytes Rx Jumbo Packets Rx Discard Packets (not applicable for Qumran platform) Rx Packets with error Rx CRC Error Packets Rx Undersized Packets Rx Oversized Packets Rx Fragment Packets Rx Jabber Packets Rx MAC error Packets Rx Pause Packets Rx Unrecognized MAC Control Packets Rx Drop Events Rx Packet rate Rx Bit rate

Table 14-32: show interface counters output details

Field	Description
Transmit Counters	Tx Packets Tx Bytes Tx Unicast Packets Tx Multicast Packets Tx Broadcast Packets Tx Packets with 64 bytes Tx Packets from 65 to 127 bytes Tx Packets from 128 to 255 bytes Tx Packets from 256 to 511 bytes Tx Packets from 512 to 1023 bytes Tx Packets from 1024 to 1518 bytes Tx Packets from 1519 to 2047 bytes Tx Packets from 2048 to 4095 bytes Tx Packets from 4096 to 9216 bytes Tx Jumbo Packets Tx Discard Packets (not applicable for Qumran platform) Tx Packets with error Tx Collisions Tx Late Collisions Tx Excessive Collisions Tx Pause Packets Tx Packet rate Tx Bit rate
CPU Interface Counters	Tx Packets Tx Bytes Tx Discard Packets Tx Discard Bytes Rx Discard Packets

© 2021 IP Infusion Inc. Proprietary

show interface counters drop-stats

Use this command to display the ingress and egress traffic discard reason counters on the interface.

Note: You can only display statistics for physical ports and cpu ports, but not for the out-of-band management (OOB) management port or logical interfaces.

Note: Drops in the CPU queue are listed under `Tx Multicast Queue Drops`, whether the packet is unicast or multicast

Command Syntax

```
show interface (IFNAME|) counters drop-stats
show interface cpu counters drop-stats
```

Parameter

`IFNAME`	Physical interface name
`cpu`	CPU interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.1.

For Qumran devices, only error statistics are applicable and discard counters are not applicable. Only global level counters are available for advanced debugging using the command show hardware-discard-counters.

Example

```
#show interface xe32/2 counters drop-stats
+---------------------+----------------+----------------+--------------------+
| Counter Description | Count          | Last Increment | Last Increment Time
|
+---------------------+----------------+----------------+--------------------+
 Rx Bad CRC errors     0                0
 Rx Undersize errors   0                0
 Rx Oversize errors    0                0
 Rx Fragments errors   0                0
 Rx Jabbers errors     0                0
 Rx Port Block Drops   6                1                2016 Nov 09 08:59:33
 Rx Vlan Discards      0                0
 Rx ACL/QOS Drops      0                0
 Rx Policy Discards    0                0
 Rx EGR Port Unavail   38784            5                2016 Nov 09 18:19:31
 Rx IBP Discards       0                0
 Tx Port Block Drops   359              1                2016 Nov 09 08:59:33
 Tx Vlan Discards      0                0
 Tx TTL Discards       0                0
 Tx Unknown Discards   359              1                2016 Nov 09 08:59:33
 Tx Ucast Queue Drops  0                0
 Tx Mcast Queue Drops  0                0
+---------------------+----------------+----------------+--------------------+
```

Table 14-33 explains the output fields.

Table 14-33: show interface counters drop-stats output details

Field	Description
Counter Description	Shows the type of packet and/or the reason why the packet was dropped.
Count	The number of packets dropped for each reason.
Last Increment	Number of packets dropped since this command was last entered.
Last Increment Time	Date and time when the last packet was dropped.
Rx Bad CRC errors	Received packets dropped because they didn't pass the cyclic Redundancy Check (CRC).
Rx Undersize errors	Number of received runt packets dropped.
Rx Oversize errors	Number of received giant packets dropped
Rx Fragments errors	Number of received packet fragments dropped
Rx Jabbers errors	Received packets dropped because of jabber – long packet error.
Rx Port Block Drops	Received packets dropped because port blocking is enabled (not applicable for Qumran platform).
Rx Vlan Discards	VLAN received packets dropped because there is no VLAN configured on the port (not applicable for Qumran platform).
Rx ACL/QOS Drops	Received packets match a field processing entry with a drop or color drop action, such as: User-configured ACL that denies traffic Service policy with a police action that drops the traffic received at a rate higher than the configured limit. (not applicable for Qumran platform)
Rx Policy Discards	Received packets dropped because of device policies violated, such as a storm control rate violation (not applicable for Qumran platform).
Rx EGR Port Unavail	No output port can be determined for these received packets. This counter increments along with other counter types in this table because it is a "catchall" for multiple types of discards as shown below (not applicable for Qumran platform): VLAN check failed MTU check failed ACL/QoS drops Policy discards Source MAC is null Destination IP/source IP address is null Source MAC address and destination MAC address are the same Forwarding lookup failure
Rx IBP Discards	Ingress Back Pressure (ingress congestion) when the ingress packets buffer is full for an interface. (not applicable for Qumran platform)
Tx Port Block Drops	Transmitted packets dropped because port blocking is enabled (not applicable for Qumran platform).
Tx Vlan Discards	Transmitted VLAN packets dropped because there is no VLAN configured on the port (not applicable for Qumran platform).

© 2021 IP Infusion Inc. Proprietary

Table 14-33: show interface counters drop-stats output details (Continued)

Field	Description
Tx TTL Discards	Transmitted packets discarded because their Time To Live (TTL) has ended. (not applicable for Qumran platform)
Tx Unknown Discards	Transmitted packets dropped for unknown reason. May have something to do with the condition/configuration of the port at the other end of the connection (not applicable for Qumran platform).
Tx Ucast Queue Drops	Transmitted packets dropped as a result of Unicast buffer overflow.
Tx Mcast Queue Drops	Transmitted packets dropped as a result of Multicast buffer overflow.

show interface counters error-stats

Use this command to display the ingress error traffic counters on the interface.

Command Syntax

```
show interface (IFNAME|) counters error-stats
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 counters error-stats
+----------+-------------+--------+----------+---------+-----------+---------+
|Interface |Total errors |Bad CRC |Undersize |Oversize | Fragments | Jabbers |
+----------+-------------+--------+----------+---------+-----------+---------+
 xe1/1      120           8        100        10        2           0
```

Table 14-34 explains the columns in the output.

Table 14-34: error traffic counters

Column	Description	Causes
Interface	Name of the interface	Point of interconnection in network.
Total errors	Total number of all types of errors	Number of errors in network.
Bad CRC	Number of packets received by the port from the network, where the packets have no CRC or a bad CRC.	Packet data modified making the CRC invalid.
Undersize	Total number of packets received that are less than 64 octets long (which exclude framing bits, but include the FCS) and have a good FCS value.	Bad frame generated by the connected device.
Oversize	Number of packets received by the port from the network, where the packets were more than maximum transmission unit size.	Faulty hardware, dot1q, or ISL trunking configuration issues.
Fragments	Total number of frames whose length is less than 64 octets (which exclude framing bits, but which include the FCS) and have a bad FCS value.	Ports are configured at half-duplex. Change the setting to full-duplex.
Jabbers	Total number of frames whose length is more than the maximum MTU size. (which exclude framing bits, but which include FCS) and have a bad FCS value.	Ports are configured at half-duplex. Change the setting to full-duplex.

© 2021 IP Infusion Inc. Proprietary

show interface counters (indiscard-stats|outdiscard-stats)

Use this command to display the ingress and egress traffic discard reason counters on the interface.

Note: You can only display statistics for data ports and CPU ports, not for the out-of-band management (OOB) management port or logical interfaces.

Command Syntax

```
show interface (IFNAME|) counters (indiscard-stats|outdiscard-stats)
show interface cpu counters (indiscard-stats|outdiscard-stats)
```

Parameter

`IFNAME`	Physical Interface name.
`indiscard-stats`	Discard reasons for ingress dropped packets.
`outdiscard-stats`	Discard reasons for egress dropped packets.
`cpu`	CPU Interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

Examples

```
#show interface xe1/3 counters indiscard-stats
+---------------------+----------------+----------------+---------------------+
| Counter Description | Count          | Last Increment | Last Increment Time |
+---------------------+----------------+----------------+---------------------+
 STP Discards          0                0
 Vlan Discards         0                0
 ACL Drops             0                0
 Policy Discards       0                0
 EGR Port Unavail      1092867          1092867          2016 Oct 25 19:54:58
 IBP Discards          0                0
+---------------------+----------------+----------------+---------------------+

#show interface counters indiscard-stats
+-------------+------------------+---------------+---------------+-----------------+------------------+--------------+------
--------------+
|  Interface  | Port Block Drops | Vlan Discards | ACL/QOS Drops | Policy Discards | EGR Port Unavail | IBP Discards |   Total
Discards   |
+-------------+------------------+---------------+---------------+-----------------+------------------+--------------+------
--------------+
xe1           0                  0               35703           0                 11                 0              35714
xe2           0                  0               295744          0                 13604              0              309348
xe3           0                  0               9501            0                 20405              0              29906
xe5           0                  0               0               0                 13602              0              13602
xe49/1        0                  0               0               0                 0                  20658          20658
xe52/1        0                  3               856029          10                13613              0              869642
xe54/1        0                  5371            0               0                 5371               0              5371
cpu           0                  0               0               0                 6                  0              N/A

#show interface counters outdiscard-stats
```

```
+-------------+-----------------+--------------+-------------+-----------------+---------------+---------------+------
-------------+
|  Interface  | Port Block Drops | Vlan Discards | TTL Discards | Unknown Discards |  UcastQ Drops  |  McastQ Drops  |   Total
Discards   |
+-------------+-----------------+--------------+-------------+-----------------+---------------+---------------+------
-------------+
xe1           0                 0              0             204338            0               0               204338
xe2           0                 0              0             1094368           0               0               1094368
xe3           0                 0              0             818672            0               0               818672
xe52/1        0                 0              0             1275156           0               0               1275156
xe54/1        0                 0              0             13575             0               0               13575
cpu           0                 0              0             0                 N/A             1014224         N/A
```

Table 14-35 explain the fields in the command output.

Table 14-35: indiscard statistic output details

Statistic	Description
STP Discards	Packets received when the ingress interface is not in STP forwarding state.
Port Block Drops	Packets discarded on an ingress interface where port blocking is configured.
VLAN Discards	VLAN tagged packets received on a port which is not a member of the VLAN or untagged packets received on a trunk port.
ACL/QoS Drops	Incoming packets match a field processing entry with a drop or color drop action, such as: 1. User-configured ACL that denies traffic 2. Service policy with a police action that drops the traffic received at a rate higher than the configured limit
Policy Discards	Device policies violated, such as a storm control rate violation, source or destination discards when L2 tagged traffic received on router interface.
EGR (Egress) Port Unavail	No output port can be determined for this packet. This counter increments along with other counter types in this table because it is a “catchall” for multiple types of discards as shown below: 1. VLAN check failed 2. MTU check failed 3. ACL/QoS drops 4. Policy discards 5. Source MAC is null 6. Destination IP/source IP address is null 7. Source MAC address and destination MAC address are the same 8. Source MAC is configured as static on other interface 9. Forwarding lookup failure
IBP Drops	Ingress Back Pressure (ingress congestion) when the ingress packet buffer is full for an interface.
Total Discards	Total number of ingress dropped packets.

Table 14-36 explain the fields in the command output.

Table 14-36: outdiscard statistics

Statistics	Description
Port Block Drops	Packets discarded on an egress interface where port blocking is configured.
VLAN Discards	Packets discarded because an invalid VLAN tag is encountered at an egress interface.
TTL Discards	Packets discarded because the Time-To Live (TTL) of the outgoing packet has passed.

© 2021 IP Infusion Inc. Proprietary

Table 14-36: outdiscard statistics

Statistics	Description
Unknown Discards	Packets discarded for other possible reasons like ACL drop in egress or a policer drop in egress. Discards caused by congestion at queues and drops at queues are not counted under unknown discards.
Unicast Queue Drops	Packets dropped in the unicast queues because of congestion.
Multicast Queue Drops	Packets dropped in the multicast queues because of congestion.
Total Discards	Total number of egress dropped packets.

show interface counters protocol

Use this command to display protocol packets received at the CPU by the control plane.

Command Syntax

```
show interface (IFNAME|) counters protocol
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

Example

```
#show interface counters protocol
Interface ce1/1
  lacp                  : 4
  icmp6                 : 5
```

Table 14-37 explain the fields in the command output.

Table 14-37: show interface counters protocol output details

Field	Description
Interface	Name of the configured interface.
lacp	Total number of lacp protocol in the interface.
icmp6	Total number of icmp6 protocol in the interface.

© 2021 IP Infusion Inc. Proprietary

show interface counters queue-drop-stats

Use this command to display dropped packets in the CPU queue and the last increment time.

Command Syntax

```
show interface cpu counters queue-drop-stats
```

Parameters

`cpu`	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
show interface cpu counters queue-drop-stats
+------------------+---------------+---------------+--------------------+
|    Queue Name    |     Count     | Last Increment | Last Increment Time |
+------------------+---------------+---------------+--------------------+
arp                  169735545        9145653          2017 Oct 23 14:33:54
```

Table 14-38 explain the fields in the command output.

Table 14-38: show interface counters queue-drop-stats output details

Field	Description
Queue Name	Name of the protocol.
Count	Number of arp protocols in the interface.
Last Increment	Final increment number in the protocol.
Last Increment time	Time of the last increment in the protocol.

show interface counters queue-stats

Use this command to display transmitted and dropped packet and byte counts of individual queues.

Note: In Qumran devices, all packets dropped in a queue are counted (even policer drops).

Command Syntax

```
show interface (IFNAME|) counters queue-stats
show interface cpu counters queue-stats
```

Parameters

IFNAME	Interface name.
cpu	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Note: Default traffic counters are not supported on Qumran AX.

Example

```
#show interface counters queue-stats
D - Default Queue, U - User-defined Queue
+---------+----------------+------+-----------+------------+------------+---------------+
|Interface|Queue/Class-map|Q-Size|Output pkts|Output bytes|Dropped pkts|Dropped bytes  |
+---------+----------------+------+-----------+------------+------------+---------------+
xe1/1     q1           (D) 0      12          1368         0            0
xe1/1     mc-q7        (D) 0      1           82           0            0
xe25      q1           (D) 0      6           684          0            0

#show interface xe1/1 counters queue-stats
D - Default Queue, U - User-defined Queue
+---------------+------+-------+-  -------+------------+--------------+
|Queue/Class-map|Q-Size|Tx pkts| Tx bytes |Dropped pkts|Dropped bytes |
+---------------+------+-------+----------+------------+--------------+
q0             (D) 0     0       0          0            0
q1             (D) 0     12      1368       0            0
q2             (D) 0     0       0          0            0
q3             (D) 0     0       0          0            0
q4             (D) 0     0       0          0            0
q5             (D) 0     0       0          0            0
q6             (D) 0     0       0          0            0
q7             (D) 0     0       0          0            0
mc-q0          (D) 0     0       0          0            0
mc-q1          (D) 0     0       0          0            0
mc-q2          (D) 0     0       0          0            0
mc-q3          (D) 0     0       0          0            0
mc-q4          (D) 0     0       0          0            0
mc-q5          (D) 0     0       0          0            0
mc-q6          (D) 0     0       0          0            0
mc-q7          (D) 0     1       82         0            0

#show interface cpu counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+-----------------+-------------------+-----------------+-------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts     |     Tx bytes      |  Dropped pkts   |   Dropped bytes   |
+--------------------+--------+-----------------+-------------------+-----------------+-------------------+
igmp              (E) 800592   14519             987292              1304163           88683084
```


© 2021 IP Infusion Inc. Proprietary

```
arp             (E) 1250496  1008785          68597380           0               0
```

Table 14-39 explain the fields in the command output.

Table 14-39: queue flags detail

Flag	Meaning
D	Default queue of the port.
U	User defined queue of the port.
E	Outgoing hello packet's queue in the port.
I	Incoming hello packet's queue in the port.
Q	Hello packet's queue size in bytes.

Table 14-40 explain the fields in the command output.

Table 14-40: show interface counters queue-stats output details

Field	Description
Interface	A defined physical interface to which the queue is associated.
Queue/Class-map	Queues associated with a QoS class-map.
Q-Size	The size of a specified queue in bytes.
Output pkts	The number of out bound packets residing in the queues.
Output Bytes	The number of bytes in the outbound queue.
Dropped pkts	The number of packets dropped because of queue overflow.
Dropped bytes	The number of bytes dropped because of queue overflow.
Tx pkts	The number of transmit packets contained in the out bound queue.
Tx bytes	The number of transmit bytes contained in the out bound queue.

show interface counters rate

Use this command to display the average traffic rate over the load interval of the interface.

Command Syntax

```
show interface (IFNAME|) counters rate (kbps|mbps|gbps|)
show interface cpu counters rate (kbps|mbps|gbps|)
```

Parameter

IFNAME	Interface name.
kbps	Kilobits per second.
mbps	Megabits per second.
gbps	Gigabits per second.
cpu	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface counters rate
+-------------+--------------------------+-------------------------------+
|             |              Rx          |               Tx              |
|  Interface  |--------------------------+-------------------------------|
|             |      bps     |      pps  |      bps      |      pps      |
+-------------+--------------------------+-------------------------------+
 xe1/1         548439552       1008160     544400           1000

#show interface cpu counters rate
Load interval: 30 second
+------------------+-------------+-------------+-------------+-------------+
|    CPU Queue(%)  |    Rx bps   |    Rx pps   |    Tx bps   |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 isis          (  0%) -              -             742           0
 arp           (  0%) -              -             6             0
```

Table 14-41 explain the fields in the command output.

© 2021 IP Infusion Inc. Proprietary

Table 14-41: show interface counters rate output details

Field	Description
Interface	The particular interface.
RX	Number of hello packets received from the neighbor.
TX	Number hello packets transmitted to the neighbor.
bps	Bytes per second.
pps	Packets per second.
CPU Queue	CPU Queues used for various functions. In the example the CPU is maintaining queues for ARP and the IS-IS routing facilities.
Load interval	The length of time for which data is used to compute load statistics.
RX bps	Number of hello packets received from the neighbor in bytes per second.
RX pps	Number of hello packets received from the neighbor in packets per second.
TX bps	Number hello packets transmitted to the neighbor in bytes per second.
Tx pps	Number hello packets transmitted to the neighbor in packets per second.

show interface counters speed

Use this command to display the current average speed on the interface.

Command Syntax

```
show interface (IFNAME|) counters speed (kbps|mbps|gbps|)
```

Parameter

IFNAME	Interface name.
kbps	Kilobits per second.
mbps	Megabits per second.
gbps	Gigabits per second.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show interface counters speed
* indicates monitor is active
+-----------+-------------+--------------------+---------------------------
---------------+
|           |             |     Threshold(%)   |          Current average
speed           |
|  interface | configured   +--------------------+------------+-------+------
------+-------+
|           | speed ( bps) | Warning | Recovery |  Rx ( bps)  |   %   |  Tx (
bps)  |   %   |
+-----------+-------------+---------+----------+-------------+-------+------
------+-------+
  ce45       100000000000   90        80        0           0.00    0
0.00
  xe7        10000000000    90        80        0           0.00    0
0.00
  xe31       10000000000    90        80        0           0.00    0
0.00
  xe33       10000000000    90        80        0           0.00    0
0.00
  xe39       10000000000    90        80        0           0.00    0
0.00
  xe40       10000000000    90        80        0           0.00    0
0.00
#
```


© 2021 IP Infusion Inc. Proprietary

show interface counters summary

Use this command to display the summary of traffic counters on a specific interface or all interfaces.

Note: This command is supported for the out-of-band management (OOB) management interface.

Command Syntax

```
show interface (IFNAME|) counters summary
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 counters summary
+-----------+------------------------------+------------------------------+
|           |              Rx              |              Tx              |
| Interface |------------------------------+------------------------------|
|           |    packets    |     bytes    |    packets    |     bytes    |
+-----------+---------------+--------------+---------------+--------------+
 xe1/1       11032977        11032960000     61              3904


#show interface counters summary
+-------------+--------------------+--------------------+--------------------+--------------------+
|  Interface  |     Rx packets     |      Rx bytes      |     Tx packets     |      Tx bytes      |
+-------------+--------------------+--------------------+--------------------+--------------------+
 eth0          206222               13756391             235123               337010937
 po1           809121               72989094             825221               90605534
 xe1/1         0                    0                    1                    114
 xe3/1         43                   4730                 21                   2298
 xe5/1         29                   3178                 21                   2298
 xe8           10                   1076                 14                   1532
 xe9/1         16                   1760                 21                   2298
 xe11/1        0                    0                    7                    766
 xe19/1        12426292             1298526692           6                    620
 xe21/1        13                   1386                 14                   1532
 xe28/1        3144                 202370               21                   2298
 xe30/1        3161                 202304               7                    766
 xe32/1        694067               61687838             710274               79315093
 xe32/2        115054               11301256             114947               11290441
 xe32/3        603759               51208946             620502               68865557
 xe32/4        7                    766                  7                    766
```

Table 14-42 explain the fields in the command output.

Table 14-42: show interface counters summary output details

Field	Description
Interface	The particular interface.
RX	Number of hello packets received from the neighbor.
TX	Number hello packets transmitted to the neighbor.
bps	Bytes per second.
pps	Packets per second.
RX bps	Number of hello packets received from the neighbor in bytes per second.
RX pps	Number of hello packets received from the neighbor in packets per second.
TX bps	Number hello packets transmitted to the neighbor in bytes per second.
Tx pps	Number hello packets transmitted to the neighbor in packets per second.

© 2021 IP Infusion Inc. Proprietary

show interface fec

Use this command to display the FEC (forward error correction) statistics for an interface.

Note: You can only display FEC statistics for physical interfaces and not for management or logical interfaces.

Command Syntax

```
show interface (IFNAME|) fec
```

Parameters

IFNAME	Physical Interface name.

Default

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh int ce54 fec
+-------------+--------+-----------+-------------+----------------------+------------------------+
| Interface   | Config | HW Status | Oper Status | Corrected Block Count| Uncorrected Block Count|
+-------------+--------+-----------+-------------+----------------------|------------------------+
 ce54           on        cl91        cl91        0                     12


#sh int ce53 fec
+-------------+--------+-----------+-------------+----------------------+------------------------+
| Interface   | Config | HW Status | Oper Status | Corrected Block Count| Uncorrected Block Count|
+-------------+--------+-----------+-------------+----------------------|------------------------+
 ce53           auto      cl91        cl91        0                      0


#sh int ce52 fec
+-------------+--------+-----------+-------------+----------------------+------------------------+
| Interface   | Config | HW Status | Oper Status | Corrected Block Count| Uncorrected Block Count|
+-------------+--------+-----------+-------------+----------------------|------------------------+
 ce52           off       off         off         0                      0
```

Table 14-37 explain the fields in the command output.

Table 14-43: show interface fec

Field	Description
Interface	Name of the configured interface.
config	Configured value.
HW Status	FEC currently programmed in HW.
Oper Status	FEC currently operating over the link.

Table 14-43: show interface fec (Continued)

Corrected Block Count	Number of the corrected block count.
Uncorrected Block Count	Number of the uncorrected block count.

© 2021 IP Infusion Inc. Proprietary

show ip forwarding

Use this command to display the IP forwarding status.

Command Syntax

```
show ip forwarding
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ip forwarding` command displaying the IP forwarding status.

```
#show ip forwarding
vrf (management) :IP forwarding is on
vrf (default) :IP forwarding is on
#
```

Table 14-44 explain the fields in the command output.

Table 14-44: show ip forwarding

Field	Description
vrf (management)	Management VRF is for management purposes. IP forwarding packet is on.
vrf (default)	The default VRF uses the default routing context for ip forwarding. IP forwarding packet is on.

show ip interface

Use this command to display brief information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

Command Syntax

```
show ip interface brief
show ip interface IFNAME brief
```

Parameters

`IFNAME`	Interface name.
`brief`	Brief summary of IP status and configuration.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ip interface brief` command:

```
#show ip interface brief

'*' - address is assigned by dhcp client

Interface             IP-Address      Admin-Status          Link-Status
eth0                 *10.10.26.101    up                    up
lo                    127.0.0.1       up                    up
lo.management         127.0.0.1       up                    up
xe1/1                 10.1.1.1        up                    up
xe1/2                 unassigned      down                  down
xe1/3                 unassigned      down                  down
xe1/4                 unassigned      down                  down
xe2                   unassigned      up                    down
xe3/1                 unassigned      up                    up
xe3/2                 unassigned      down                  down
xe3/3                 unassigned      down                  down
```

Table 14-45 explain the fields in the command output.

Table 14-45: show ip interface output details

Field	Description
Interface	Interface name, also specifies interface type (eth0, lo, xe1/1, and xe1/2).
IP-Address	The IP address assigned to the interface. An asterisks indicates that the IP address was provided by DHCP.

© 2021 IP Infusion Inc. Proprietary

Table 14-45: show ip interface output details (Continued)

Field	Description
Admin-Status	Interface is up and functioning or down.
Link-Status	Interface is connected and passing traffic.

show ip prefix-list

Use this command to display the prefix list entries for IPv4 interfaces.

Syntax Description

```
show ip prefix-list
show ip prefix-list WORD
show ip prefix-list WORD seq <1-4294967295>
show ip prefix-list WORD A.B.C.D/M
show ip prefix-list WORD A.B.C.D/M longer
show ip prefix-list WORD A.B.C.D/M first-match
show ip prefix-list summary
show ip prefix-list summary WORD
show ip prefix-list detail
show ip prefix-list detail WORD
```

Parameters

`WORD`	Name of a prefix list.
`A.B.C.D/M`	IP prefix <network>/<length> (for example, 35.0.0.0/8).
`first-match`	First matched prefix.
`longer`	Lookup longer prefix.
`<1-4294967295>`	Sequence number.
`detail`	Detail of prefix lists.
`summary`	Summary of prefix lists.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ip prefix-list` command showing prefix-list entries.

```
#show ip prefix-list
ip prefix-list myPrefixList: 3 entries
   seq      5 permit 172.1.1.0/16
   seq     10 permit 173.1.1.0/16
   seq     15 permit 174.1.1.0/16
```


© 2021 IP Infusion Inc. Proprietary

show ip route

Use this command to display the IP routing table for a protocol or from a particular table.

When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. All best routes are entered into the FIB and can be viewed using this command. To display all routes (selected and not selected), use the `show ip route database` command.

Use this command to see all subnets of a specified network if they are present in the routing table. Please use this command with mask information.

Command Syntax

```
show ip route A.B.C.D
show ip route (database|)
show ip route (database|) (bgp|connected|database|isis|fast-
  reroute|interface|isis|kernel|mbgp|mstatic|next-hop|ospf|rip|static)
show ip route summary
show ip route vrf WORD (database|)
show ip route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)
```

Parameters

`A.B.C.D`	Network in the IP routing table.
`A.B.C.D/M`	IP prefix <network>/<length>, for example, 35.0.0.0/8.
`bgp`	Border Gateway Protocol.
`connected`	Connected.
`database`	Routing table database.
`fast-reroute`	Fast reroute repair paths.
`interface`	Interface.
`isis`	IS-IS.
`kernel`	Kernel.
`mbgp`	Multiprotocol BGP routes.
`mstatic`	Multicast static routes.
`next-hop`	Next hop address.
`ospf`	Open Shortest Path First.
`rip`	Routing Information Protocol.
`static`	Static routes.
`summary`	Summarize all routes.
`WORD`	Routes for a Virtual Routing/Forwarding instance.

Command Mode

Exec mode and Privileged Exec mode

© 2021 IP Infusion Inc. Proprietary

Applicability

This command was introduced before OcNOS version 1.3.

Example: Display FIB Routes

The following shows output for the best routes.

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       E - EVPN,
v - vrf leaked
       * - candidate default
```


© 2021 IP Infusion Inc. Proprietary

show ip route A.B.C.D/M longer-prefixes

Use this command to see all subnets of a specified network if they are present in the routing table. Please use this command with mask information.

Command Syntax

```
show ip route A.B.C.D/M longer-prefixes
```

Parameters

```
A.B.C.D/M
```

Command Mode

Exec-mode and Privileged exec-mode

Applicability

This command was introduced from OcNOS 1.3.6

Example

```
OcNOS#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN,
v - vrf leaked

    - candidate default

IP Route Table for VRF "default"
C     10.1.1.0/24 is directly connected, eth1, 00:00:23
C     10.12.41.0/24 is directly connected, eth0, 00:00:23
S     55.0.0.0/8 [1/0] is directly connected, eth1, 00:00:23
S     55.0.0.0/12 [1/0] is directly connected, eth1, 00:00:23
S     55.0.0.0/24 [1/0] is directly connected, eth1, 00:00:23
S     55.1.0.0/16 [1/0] is directly connected, eth1, 00:00:23
S     55.1.1.0/24 [1/0] is directly connected, eth1, 00:00:23
C     127.0.0.0/8 is directly connected, lo, 00:00:23

Gateway of last resort is 10.30.0.11 to network 0.0.0.0

K*      0.0.0.0/0 via 10.30.0.11, eth0
O       9.9.9.9/32 [110/31] via 10.10.31.16, eth2, 00:18:56
K       10.10.0.0/24 via 10.30.0.11, eth0
C       10.10.31.0/24 is directly connected, eth2
S       10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O       10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:20:54
C       10.30.0.0/24 is directly connected, eth0
```

```
S       11.22.11.0/24 [1/0] via 10.10.31.16, eth2
O E2    14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:18:56
S       16.16.16.16/32 [1/0] via 10.10.31.16, eth2
O       17.17.17.17/32 [110/31] via 10.10.31.16, eth2, 00:20:54
C       45.45.45.45/32 is directly connected, lo
O       55.55.55.55/32 [110/21] via 10.10.31.16, eth2, 00:20:54
C       127.0.0.0/8 is directly connected, lo

OcNOS#sh ip route 55.0.0.0/7 longer-prefixes
Routing entry for 55.0.0.0/8
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.0.0.0/12
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.0.0.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.0.0/16
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

OcNOS#sh ip route 55.0.0.0/8 longer-prefixes
Routing entry for 55.0.0.0/8
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.0.0.0/12
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.0.0.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1
```


© 2021 IP Infusion Inc. Proprietary

```
Routing entry for 55.1.0.0/16
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

OcNOS#
OcNOS#sh ip route 55.0.0.0/11 longer-prefixes
Routing entry for 55.0.0.0/12
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.0.0.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.0.0/16
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

OcNOS#
OcNOS#
OcNOS#
OcNOS#sh ip route 55.0.0.0/16 longer-prefixes
Routing entry for 55.0.0.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

OcNOS#sh ip route 55.1.0.0/16 longer-prefixes
Routing entry for 55.1.0.0/16
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best
```

```
    directly connected, eth1

OcNOS#sh ip route 55.1.0.0/20 longer-prefixes
Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

OcNOS#sh ip route 55.1.0.0/24 longer-prefixes
% Network not in table
OcNOS#
OcNOS#
OcNOS#
OcNOS#sh ip route 55.1.1.0/24 longer-prefixes
Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

OcNOS#
```

Header

Each entry in this table has a code preceding it, indicating the source of the routing entry. For example, O indicates OSPF as the origin of the route and K indicates that the route has been learned from the kernel. Table 14-46 shows these codes and modifiers.

Table 14-46 explain the fields in the command output.

Table 14-46: route codes and modifiers

Code	Meaning	Description
K	kernel	Routes added through means other than by using the CLI; for example by using the operating system route command. Static routes added using kernel commands and static routes added using OcNOS commands are different. The kernel static routes are not redistributed when you give the `redistribute static` command in a protocol. However, the kernel static routes can be redistributed using the `redistribute kernel` command.
C	connected	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from other routing protocols. Routes for connected networks always exist in the kernel routing table but as an exception are not marked as kernel routes because OcNOS always calculates entries for these routes upon learning interface information from the kernel.
S	static	Routes manually configured via CLI which are not updated dynamically by IGPs.
The codes below are for routes received and dynamically learned via IGP neighbors. These networks are not directly connected to this device and were announced by some other device on the network. IGPs update these routes as the network topology changes.		
R	RIP	RIP routing process and enter Router mode.

© 2021 IP Infusion Inc. Proprietary

Table 14-46: route codes and modifiers

Code	Meaning	Description
B	BGP	Route is from an Border Gateway Protocol.
O	OSPF	Modifiers for OSPF: IA - OSPF inter area N1 - OSPF NSSA external type 1 N2 - OSPF NSSA external type 2 E1 - OSPF external type 1 E2 - OSPF external type 2
i	IS-IS	Modifiers for IS-IS: L1 - IS-IS level-1 L2 - IS-IS level-2 ia - IS-IS inter area
Other modifiers:		
v	vrf leaked	The device has two or more VRFs configured and each has at least one interface bound to it. While each VRF will have its own routing table, the VRFs can learn each other's routes.
*	candidate default	Route has been added to the FIB. With equal cost paths to a destination, the router does per-packet or per-destination load sharing. An asterisk ("*") means that the route is being used at that instant for forwarding packets. If you run the same `show ip route x.x.x.x` command over and over, you might see the * moving between the route entries.
>	selected route	When multiple routes are available for the same prefix, the best route. When multiple entries are available for the same prefix, OcNOS uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. OcNOS populates the FIB with the *best* route to each destination
p	stale info	A route information that is marked stale due to graceful restart.

After the codes, the header has default gateway information:

```
Gateway of last resort is 10.12.4.1 to network 0.0.0.0
```

The "gateway of last resort", also called the default gateway, is a static route that routes IP address 0.0.0.0 (all destinations) through a single host (the gateway). The effect of setting a gateway is that if no routing table entry exists for a destination address, packets to that address will be forwarded to the gateway router.

Route Entry Fields

Table 14-47 explains the each route entry fields.

Table 14-47: route entry output details

Field	Description
Codes and modifiers	As explained in Table 14-46.
IP address	IP address of the remote network.

Table 14-47: route entry output details

Field	Description
Administrative distance and metric	The administrative distance determines how trustworthy this route is. If there is a similar route but with a smaller administrative distance, it is used instead, because it is more “trustworthy”. The smaller the administrative distance, the more trustworthy the route. Directly connected routes have an administrative distance of 0, which makes them the most trustworthy type of route.The metric varies from protocol to protocol, and for OSPF the metric is cost, which indicates the best quality path to use to forward packets. Other protocols, like RIP, use hop count as a metric. For neighboring routers, the metric value is 1.
Next hop router IP address	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Outgoing interface name	Interface used to get to the next-hop address for this route.
Duration	Length of time that this route has been present in the routing table. This is also the length of time this route has existed without an update. If the route were removed and then re-added (if the cable was disconnected, for instance), this timer would begin again at 00:00:00.

Route Entry Examples

```
O       10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:20:54
```

- This route in the network 10.10.37.0/24 was added by OSPF.
- This route has an administrative distance of 110 and metric/cost of 11.
- This route is reachable via nexthop 10.10.31.16.
- The outgoing local interface for this route is eth2.
- This route was added 20 minutes and 54 seconds ago.

```
O E2    14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:18:56
```

- This route is the same as the other OSPF route above; the only difference is that it is a Type 2 External OSPF route.

```
C       10.10.31.0/24 is directly connected, eth2
```

- This route is directly connected.
- Route entries for network 10.10.31.0/24 are derived from the IP address of local interface eth2.

```
K       10.10.0.0/24 via 10.30.0.11, eth0
```

- This route in the network 10.10.0.0/24 was learned from the kernel routing table (route was statically added using kernel commands).
- This route is reachable via nexthop 10.30.0.11.
- The outgoing local interface for this route is eth0.

```
K*      0.0.0.0/0 via 10.30.0.11, eth0
```

- This is a default route that was learned from the kernel (route was statically added using kernel commands).
- This route is reachable via nexthop 10.30.0.11.
- The local interface for this route is eth0.

Example: Display OSPF Routes

The following is the output with the `ospf` parameter:

```
#show ip route ospf
O       1.1.1.0/24 [110/20] via 2.2.2.1, eth2, 00:00:44
```


© 2021 IP Infusion Inc. Proprietary

```
    O IA    4.4.4.0/24 [110/21] via 2.2.2.1, eth2, 00:00:44
    #
```

Example: Display Route Summary

The following is the output with the `summary` parameter.

```
    #show ip route summary
    IP routing table name is Default-IP-Routing-Table(0)
    IP routing table maximum-paths is 4
    Route Source    Networks
    kernel          1
    connected       5
    ospf            2
    Total           8
    FIB             2
```

Example: Display RIB Routes

The following shows displaying database routes.

```
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

K    *> 0.0.0.0/0 via 10.30.0.11, eth0
O    *> 9.9.9.9/32 [110/31] via 10.10.31.16, eth2, 00:19:21
K    *> 10.10.0.0/24 via 10.30.0.11, eth0
O       10.10.31.0/24 [110/1] is directly connected, eth2, 00:28:20
C    *> 10.10.31.0/24 is directly connected, eth2
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O       10.10.34.0/24 [110/31] via 10.10.31.16, eth2, 00:21:19
O    *> 10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:21:19
K    *  10.30.0.0/24 is directly connected, eth0
C    *> 10.30.0.0/24 is directly connected, eth0
S    *> 11.22.11.0/24 [1/0] via 10.10.31.16, eth2
O E2 *> 14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:19:21
O       16.16.16.16/32 [110/11] via 10.10.31.16, eth2, 00:21:19
S    *> 16.16.16.16/32 [1/0] via 10.10.31.16, eth2
O    *> 17.17.17.17/32 [110/31] via 10.10.31.16, eth2, 00:21:19
C    *> 45.45.45.45/32 is directly connected, lo
O    *> 55.55.55.55/32 [110/21] via 10.10.31.16, eth2, 00:21:19
K    *  127.0.0.0/8 is directly connected, lo
C    *> 127.0.0.0/8 is directly connected, lo
```

The codes and modifier at the start of each route entry are explained in Table 14-46.

Routes in the FIB are marked with a `*`. When multiple routes are available for the same prefix, the best route is indicated with the > symbol. Unselected routes have neither the `*` nor the > symbol.

Route Database Entry Examples

This example shows 2 entries in the route database; one learned from the kernel and the other derived from interface information.

```
K    * 10.30.0.0/24 is directly connected, eth0
C    *> 10.30.0.0/24 is directly connected, eth0
```

- Both these routes are in the same network 10.30.0.0/24.
- The first route has originated from the kernel. The `*` indicates that it has been added to the FIB.
- The second route is derived from the IP address of local interface eth0. It is marked as a connected route. Since a connected route has the lowest administrative distance, it is the selected route.

```
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O       10.10.34.0/24 [110/31] via 10.10.31.16, eth2, 00:21:19
```

- The same prefix was learned from OSPF and from static route configuration.
- Static routes are preferred over OSPF routes, so the static route is selected and installed in the FIB.

  Note: If the static route becomes unavailable, OcNOS automatically selects the OSPF route and installs it in the FIB.

Example: Display VRF Routes

The following is the output with the `vrf` parameter:

```
#show ip route vrf vrf31
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN,
v - vrf leaked
* - candidate default

IP Route Table for VRF "vrf31"
O            2.2.2.2/32 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
O            10.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
O            20.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
C            21.1.1.0/24 is directly connected, vlan1.4, 00:02:54
C            31.31.1.1/32 is directly connected, lo.vrf31, 00:03:02
O            40.40.1.1/32 [110/3] via 21.1.1.2, vlan1.4, 00:00:43
C            127.0.0.0/8 is directly connected, lo.vrf31, 00:03:05

Gateway of last resort is not set
```

The following is the output with the `vrf database` parameter:

```
#show ip route vrf vrf31 database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN,
v - vrf leaked
> - selected route, * - FIB route, p - stale info
```


© 2021 IP Infusion Inc. Proprietary

```
IP Route Table for VRF "vrf31"
O    *>  2.2.2.2/32 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
O    *>  10.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
O    *>  20.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
C    *>  21.1.1.0/24 is directly connected, vlan1.4, 00:02:57
O        21.1.1.0/24 [110/1] is directly connected, vlan1.4, 00:02:57
C    *>  31.31.1.1/32 is directly connected, lo.vrf31, 00:03:05
O        31.31.1.1/32 [110/1] is directly connected, lo.vrf31, 00:03:00
O    *>  40.40.1.1/32 [110/3] via 21.1.1.2, vlan1.4, 00:00:46
B     >  50.1.1.0/24 [200/0] via 41.41.41.41, 00:00:18
C    *>  127.0.0.0/8 is directly connected, lo.vrf31, 00:03:08

Gateway of last resort is not set
```

show ip vrf

This command displays routing information about VRFs.

Command Syntax

```
show ip vrf
show ip vrf WORD
```

Parameter

WORD	Virtual Routing and Forwarding name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip forwarding
 vrf (management) :IP forwarding is on
 vrf (default) :IP forwarding is on
```


© 2021 IP Infusion Inc. Proprietary

show ipv6 forwarding

Use this command to display the IPv6 forwarding status.

Command Syntax

```
show ipv6 forwarding
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ipv6 forwarding` command displaying the IPv6 forwarding status.

```
#show ipv6 forwarding
 vrf (management) :IPv6 forwarding is on
 vrf (default) :IPv6 forwarding is on#
```

show ipv6 interface brief

Use this command to display information about interfaces. To display information about a specific interface, include the interface name.

Command Syntax

```
show ipv6 interface brief
show ipv6 interface IFNAME brief
```

Parameters

IFNAME	Name of the interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 interface brief
Interface           IPv6-Address                Admin-Status
lo                  ::1                         [up/up]

gre0                unassigned                  [admin down/down]

eth3                3ffe:abcd:104::1            [up/up]
                    3ffe:abcd:103::1
                    fe80::2e0:29ff:fe6f:cf0

eth1                fe80::260:97ff:fe20:f257    [up/up]

eth2                unassigned                  [admin down/down]

eth3                unassigned                  [admin down/down]

sit0                unassigned                  [admin down/down]

tun24               unassigned                  [admin down/down]

tunl0               unassigned                  [admin down/down]
```

Table 14-48 explains the each interface brief entry.

© 2021 IP Infusion Inc. Proprietary

Table 14-48: show interface brief output details

Field	Description
Interface	Name of the interface.
IPv6-Address	IPv6 address. An asterisk (“*”) means the address was assigned by the DHCPv6 client.
Admin-Status	Status of the interface: The first part of the field indicates if the interface is up. The second part indicates if the interface is running.

show ipv6 route

Use this command to display the IP routing table for a protocol or from a particular table, including database entries known by NSM. When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. The best routes in the FIB can be viewed using `show ipv6 route`.

Command Syntax

```
show ipv6 route vrf WORD (database|)
show ipv6 route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)
show ipv6 route (database)
show ipv6 route (database) (bgp|connected|isis|kernel|ospf|rip|static)
show ipv6 route X:X::X:X
show ipv6 route X:X::X:X/M
show ipv6 route summary
```

Parameters

`X:X::X:X`	Network in the IP routing table.
`X:X::X:X/M`	Prefix <network>/<length>, e.g., 35.0.0.0/8
`all`	All IPv6 routes
`bgp`	Border Gateway Protocol.
`connected`	Connected.
`database`	IPv6 routing table database.
`isis`	IS-IS.
`IFNAME`	Interface name
`kernel`	Kernel.
`ospf`	Open Shortest Path First.
`rip`	Routing Information Protocol.
`static`	Static routes.
`summary`	Summarize all routes
`WORD`	Routes from a Virtual Routing and Forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

See Table 14-46 and Table 14-47 for an explanation of the codes and fields in the output.

```
#show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng, O - OSPFv3,
```


© 2021 IP Infusion Inc. Proprietary

```
       I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info.
C> * ::1/128 is directly connected, lo
C> * 3ffe:1::/48 is directly connected, eth1
C> * 3ffe:2:2::/48 is directly connected, eth2
#
```

show ipv6 prefix-list

Use this command to display the prefix list entries for IPv6 interfaces.

Syntax Description

```
show ipv6 prefix-list
show ipv6 prefix-list WORD
show ipv6 prefix-list WORD seq <1-4294967295>
show ipv6 prefix-list WORD X:X::X:X/M
show ipv6 prefix-list WORD X:X::X:X/M longer
show ipv6 prefix-list WORD X:X::X:X/M first-match
show ipv6 prefix-list summary
show ipv6 prefix-list summary WORD
show ipv6 prefix-list detail
show ipv6 prefix-list detail WORD
```

Parameters

`WORD`	Name of prefix list.
`X:X::X:X/M`	IP prefix <network>/<length> (for example, 35.0.0.0/8).
`first-match`	First matched prefix.
`longer`	Look up longer prefix.
`<1-4294967295>`	Sequence number of an entry.
`detail`	Detail of prefix lists.
`summary`	Summary of prefix lists.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ip prefix-list` command showing prefix-list entries.

```
#show ip prefix-list
ip prefix-list myPrefixList: 3 entries
   seq      5 permit 172.1.1.0/16
   seq     10 permit 173.1.1.0/16
   seq     15 permit 174.1.1.0/16
```


© 2021 IP Infusion Inc. Proprietary

show hosts

Use this command to display the IP domain-name, lookup style and any name server.

Command Syntax

```
show hosts
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show hosts

       VRF: management

DNS lookup is enabled
 Default domain      : .com
 Additional Domain   : .in .ac
 Name Servers        : 10.12.3.23
Host                                                                    Address
----                                                                    -------
test                                                                    10.12.12.67
test                                                                    10::23

 * - Values assigned by DHCP Client.
```

Table 14-49 explains the output fields.

Table 14-49: show hosts fields

Entry	Description
VRF: management	DNS configuration of specified VRF
DNS lookup is enabled	DNS feature enabled or disabled
Default domain	Default domain name used to complete unqualified host names (names without a dotted decimal domain name).
Additional Domain	A list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.
Name Servers	DNS server addresses that are used to translate hostnames to IP addresses.

Table 14-49: show hosts fields

Entry	Description
Host Address test 10.12.12.67 test 10::23	Static hostname-to-address mappings in DNS.
* - Values assigned by DHCP Client.	* in name-server indicates it has been learned dynamically.

© 2021 IP Infusion Inc. Proprietary

show running-config interface

Use this command to show the running system status and configuration for a specified interface, or a specified interface for a specified protocol.

Command Syntax

```
show running-config interface IFNAME
show running-config interface IFNAME bridge
show running-config interface IFNAME ip igmp
show running-config interface IFNAME ip multicast
show running-config interface IFNAME ip pim
show running-config interface IFNAME ipv6 ospf
show running-config interface IFNAME ipv6 rip
show running-config interface IFNAME ipv6 pim
show running-config interface IFNAME isis
show running-config interface IFNAME lacp
show running-config interface IFNAME ldp
show running-config interface IFNAME mpls
show running-config interface IFNAME mstp
show running-config interface IFNAME ospf
show running-config interface IFNAME ptp
show running-config interface IFNAME rip
show running-config interface IFNAME rstp
show running-config interface IFNAME rsvp
show running-config interface IFNAME stp
show running-config interface IFNAME synce
```

Parameters

`bridge`	Bridge.
`ip`	IPv4 (see also show running-config interface ip).
`ipv6`	IPv6 (see also show running-config interface ipv6).
`isis`	Intermediate System to Intermediate System.
`lacp`	Link Aggregation Control Protocol.
`ldp`	Label Distribution Protocol.
`mpls`	Multi-Protocol Label Switching.
`mstp`	Multiple Spanning Tree Protocol.
`ospf`	Open Shortest Path First.
`ptp`	Precision Time Protocol.
`rip`	Routing Information Protocol.

`rstp`	Rapid Spanning Tree Protocol.
`rsvp`	Resource Reservation Protocol.
`stp`	Spanning Tree Protocol.
`synce`	Synchronous Ethernet.

Command Mode

Privileged Exec mode and Config Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 bridge
!
interface eth1
 switchport
 bridge-group 1
 switchport mode access
 user-priority 3
 traffic-class-table user-priority 2 num-traffic-classes 3 value 3 traffic-
class-table user-priority 7 num-traffic-classes 1 value 2 traffic-class-table
user-priority 7 num-traffic-classes 2 value 0 traffic-class-table user-
priority 7 num-traffic-classes 3 value 0 traffic-class-table user-priority 7
num-traffic-classes 4 value 0 traffic-class-table user-priority 7 num-traffic-
classes 5 value 0 traffic-class-table user-priority 7 num-traffic-classes 6
```


© 2021 IP Infusion Inc. Proprietary

show running-config interface ip

Use this command to show the running system status and configuration for a specified IP.

Command Syntax

```
show running-config interface IFNAME ip (igmp|multicast|pim|)
```

Parameters

`IFNAME`	Interface name.
`igmp`	Internet Group Management Protocol.
`multicast`	Multicast.
`pim`	Protocol Independent Multicast.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 ip igmp
!
interface eth1
 switchport
```

show running-config interface ipv6

Use this command to show the running system status and configuration for a specified IPv6 protocol.

Command Syntax

```
show running-config interface IFNAME ipv6 (mld|multicast|ospf|pim|rip|)
```

Parameters

`IFNAME`	Interface name.
`mld`	Multicast Listener Discovery
`multicast`	Multicast
`ospf`	Open Shortest Path First
`pim`	Protocol Independent Multicast
`rip`	Routing Information Protocol

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 ipv6 rip
!
interface eth1
 switchport
```


© 2021 IP Infusion Inc. Proprietary

show running-config ip

Use this command to show the running system of IP configurations.

Command Syntax

```
show running-config ip (dhcp|mroute|route)
```

Parameters

`dhcp`	Dynamic Host Configuration Protocol.
`mroute`	Static IP multicast route.
`route`	Static IP route.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config ip route
!
ip route 3.3.3.3/32 eth3
ip route 3.3.3.3/32 eth2
ip route 200.0.0.0/16 lo
!
```

show running-config ipv6

Use this command to show the running system status and configuration for IPv6.

Command Syntax

```
show running-config ipv6 (access-list|mroute|neighbor|prefix-list|route|)
```

Parameters

`access-list`	Access list.
`mroute`	Static IPv6 Multicast route.
`neighbor`	Static IPv6 neighbor entry.
`prefix-list`	IPv6 prefix-list.
`route`	Static IPv6 route.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config ipv6 access-list
!
ipv6 access-list abc permit any
!
#show running-config ipv6 prefix-list
!
ipv6 prefix-list sde
 seq 5 permit any
!
#show running-config ipv6 route
!
ipv6 route 3e11::/64 lo
ipv6 route 3e11::/64 eth2
ipv6 route fe80::/64 eth2
!
```


© 2021 IP Infusion Inc. Proprietary

show running-config prefix-list

Use this command to display the running system status and configuration details for prefix lists.

Command Syntax

```
show running-config prefix-list
```

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
(config)#show running-config prefix-list
!
ip prefix-list abc
 seq 5 permit any
!
ip prefix-list as
 description annai
!
ip prefix-list wer
 seq 45 permit any
!
(config)#
```

shutdown

Use this command to shut down an interface.

Use the `no` form of this command to bring up an interface.

Command Syntax

```
shutdown
no shutdown
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the use of the `shutdown` command to shut down the interface called `eth3`.

```
#configure terminal
(config)#interface eth3
(config-if)#shutdown
```


© 2021 IP Infusion Inc. Proprietary

speed

Use this command to set the link speed of the interface.

Use the `no` parameter to set the speed to its default value.

On copper ports, auto-negotiation is enabled by default and force speed is not supported.

On fiber optic ports, auto-negotiation is disabled by default. Auto-negotiation is not supported on fiber optic medium/ AOC for speeds 10g and beyond. IP Infusion Inc.does not recommend using auto speed on such transceivers. On DAC cables, both force and auto-negotiation are supported.

IP Infusion Inc. recommends configuring the same speed mode on both peers.

When an interface is configured with the speed auto option, the negotiated parameters are speed, duplex, flowcontrol, and fec, each of which is configured separately. Please see the respective command for details.

Note: For 10g DAC/AOC, setting speed auto negotiates with a maximum of 1G.

Table 14-50 shows the IP Infusion Inc. recommendations regarding front-panel port speed and transceivers.

Table 14-50: Recommendatons

Suported/ Recommended	Explanation
Not Supported	When front panel port capability is less than the transceiver's capability the behavior is undefined.
Not Recommended	When the transceiver's capability and front panel port capability is the same, reducing the speed is not recommended.
Recommended	When the transceiver's capability is less than the front panel port capability, the behavior is undefined and the link might even come up. So speed needs to be set to match the transceiver's capability.

Table 14-51 show examples with front-panel configurations:

Table 14-51: Front-panel configurations

Front Panel Port	Explanation
Front Panel Port 100g	When 40g transceivers are used, make sure to use the command `speed 40g`. IP Infusion Inc. does not recommend using 40g on 100g speed transceivers.
Front Panel Port 40g	100g transceivers should not be used.
Front Panel Port 25g	When 10g transceivers are used, make sure to use the `port-group` command to reduce the speed to 10g. IP Infusion Inc. does not recommend to use 10g on 25g speed transceivers. When using 1g transceivers, make sure to set the speed to 1g. Below 25g, port-speed can defer (10g or 1g) for ports under same port-group i.e. 1 port can have 1g & remaining 10g but 1 port 25g & remaining 10g not allowed. When "`no speed`" command is used at interface level it tries to set speed "25g" to one of the port of port-group while other may be at 10g or 1g speed which is not allowed. Use "`no port-group`" command in such case.

Table 14-51: Front-panel configurations (Continued)

Front Panel Port	Explanation
Front Panel Port 10g	25g transceivers should not be used. When using 1g transceivers, make sure to set the speed to 1g.
Front Panel Port 1g	10g/25g transceivers should not be used.

Command Syntax

```
speed (10m | 100m | 1g | 2.5g | 10g | 20g | 25g | 40g | 50g | 100g | auto )
no speed
```

Parameter

`10m`	10 megabits
`100m`	100 megabits
`1g`	1 gigabit
`2.5g`	2.5 gigabits
`10g`	10 gigabits
`20g`	20 gigabits
`25g`	25 gigabits
`40g`	40 gigabits
`50g`	50 gigabits
`100g`	100 gigabits
`auto`	Negotiate the speed with a connected port

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Enable auto-negotiation:

```
#configure terminal
(config)#interface xe0
(config-if)#speed auto
```


© 2021 IP Infusion Inc. Proprietary

switchport

Use this command to set the mode of an interface to switched.

All interfaces are configured `routed` by default. To change the behavior of an interface from switched to routed, you must explicitly give the `no switchport` command.

Note: When you change the mode of an interface from switched to routed and vice-versa, all configurations for that interface are erased.

User should be prompted for confirmation, while executing `switchport/no switchport` command. To support this requirement, please refer the command `enable/disable confirmation-dialog.`

Use the `no` form of this command to set the mode to routed.

Command Syntax

```
switchport
```

```
no switchport
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport

(config)#interface eth0
(config-if)#no switchport

#configure terminal
(config)#enable confirmation-dialog
(config)#interface xe5
(config-if)#switchport
Are you sure? (y/n): y
(config-if)#
(config-if)#exit

(config)#disable confirmation-dialog
(config)#
(config)#interface xe5
(config-if)#switchport
(config-if)#
```

switchport allowed ethertype

Use this command to indicate which types of traffic will be allowed on the switchport.

Note: A maximum of 5 Ethertype values can be assigned on an interface.

Command Syntax

```
switchport allowed ethertype {arp|ipv4|ipv6|mpls|ETHTYPE|log}
```

Parameters

`arp`	ARP traffic
`ipv4`	IPv4 traffic
`ipv6`	IPv6 traffic
`mpls`	MPLS traffic
`ETHTYPE`	Traffic of any Ethertype value (0x600 - 0xFFFF).
`log`	Log unwanted ethertype packets.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

Example

```
(config)#interface xe32/1

(config-if)#switchport
(config-if)#switchport allowed ethertype ipv4
(config-if)#switchport allowed ethertype 0x800
```


© 2021 IP Infusion Inc. Proprietary

switchport protected

Use this command to enable or disable the protected port feature on an interface.

Command Syntax

```
switchport protected (community | isolated | promiscuous)
no switchport protected
```

Parameter

`community`	Community mode
`isolated`	Isolated mode type
`promiscuous`	Protected mode type

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport protected isolated
(config-if)#no switchport protected

(config)#interface po1
(config-if)#switchport protected promiscuous
(config-if)#no switchport protected
```

transceiver

Use this command to set the type of Small Form-factor Pluggable (SFP) transceiver inserted in the physical port.

Use the `no` form of this command to remove the setting.

Command Syntax

```
transceiver (1000base-sx|1000base-lx|1000base-ex|1000base-cx|10gbase-sr|10gbase-
  lr|10gbase-er|10gbase-cr|25gbase-sr|25gbase-lr|25gbase-er|25gbase-cr|40gbase-
  sr4|40gbase-lr4|40gbase-er4|40gbase-cr4|100gbase-sr4|100gbase-lr4|100gbase-
  er4|100gbase-cr4)
no transceiver
```

Parameters

`1000base-cx`	SFP 1000base-cx
`1000base-ex`	SFP 1000base-ex
`1000base-lx`	SFP 1000base-lx
`1000base-sx`	SFP 1000base-sx
`100gbase-cr4`	QSFP28 100gbase-cr4
`100gbase-er4`	QSFP28 100gbase-er4
`100gbase-lr4`	QSFP28 100gbase-lr4
`100gbase-sr4`	QSFP28 100gbase-sr4
`10gbase-cr`	SFP+ 10gbase-cr
`10gbase-er`	SFP+ 10gbase-er
`10gbase-lr`	SFP+ 10gbase-lr
`10gbase-sr`	SFP+ 10gbase-sr
`25gbase-cr`	SFP+ 25gbase-cr
`25gbase-ers`	SFP+ 25gbase-er
`25gbase-lr`	SFP+ 25gbase-lr
`25gbase-sr`	SFP+ 25gbase-sr
`40gbase-cr4`	QSFP 40gbase-cr4
`40gbase-er4`	QSFP 40gbase-er4
`40gbase-lr4`	QSFP 40gbase-lr4
`40gbase-sr4`	QSFP 40gbase-sr4

Default

No default value is specified

Command Mode

Interface mode

© 2021 IP Infusion Inc. Proprietary

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
(config)#interface ce1/1
(config-if)#transceiver 40gbase-lr4
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 15 IP Service Level Agreements Commands

IP Service Level Agreements (SLAs) is a diagnostic method which generates and analyses the traffic between an OcNOS device and your network. IP SLA monitors and reports network performance data which helps you to identify the actual root cause of a problem when the performance level drops.

This chapter describes the commands used to manage the IP SLA for ICMP echo.

- clear ip sla statistics
- frequency
- icmp-echo
- ip sla
- ip sla schedule
- show ip sla statistics
- show ip sla summary
- show running-config ip sla
- threshold
- timeout

clear ip sla statistics

Use this command to clear the IP SLA statistics.

Command Syntax

```
clear ip sla statistics <1-65535>
```

Parameters

1-65535	IP SLA identifier

Default

N/A

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#clear ip sla statistics 1
```


© 2021 IP Infusion Inc. Proprietary

frequency

Use this command to configure the frequency/interval to send ICMP echo packets one by one.

Use the `no` form of this command to remove the configured ICMP echo frequency.

Command Syntax

```
frequency <1-60>
no frequency
```

Parameters

`1-60`	Frequency in seconds

Default

5 seconds

Command Mode

IP SLA ICMP Echo mode (config-ip-sla-echo)

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#frequency 3
```

icmp-echo

Use this command to select and configure the ICMP echo SLA operation. ICMP echo packets are constructed in the device and sent to the destination address that you specify. These packets are transferred on a specific interface by setting the `source-interface` parameter.

Use the `no` form of this command to un-configure or remove the configured ICMP echo measurement sessions.

Command Syntax

```
icmp-echo (ipv4 A.B.C.D|ipv6 X:X::X:X|HOSTNAME) (source-interface IFNAME|)
no icmp-echo (ipv4 A.B.C.D | ipv6 X:X::X:X | HOSTNAME)
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`HOSTNAME`	Host name
`IFNAME`	Source interface name

Default

N/A

Command Mode

IP SLA mode (config-ip-sla)

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#
```


© 2021 IP Infusion Inc. Proprietary

ip sla

Use this command to create an IP SLA instance. One instance maps to a single SLA operation. You can create multiple SLA operations to perform multiple similar or different SLA operations.

Use the `no` form of this command to remove a configured IP SLA configurations.

Command Syntax

```
ip sla <1-65535>
no ip sla <1-65535>
```

Parameters

`1-65535`	IP SLA identifier

Default

N/A

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#
```

ip sla schedule

Use this command to schedule an IP SLA operation by associating a time-range object with the IP SLA operation.

Use the `no` form of this command to stop the configured IP SLA measurement.

Command Syntax

```
ip sla schedule <1-65535> time-range WORD (vrf (NAME)|)
```

Parameters

`<1-65535>`	IP SLA identifier.
`time-range`	Time Range
`TR_NAME`	Time range name that you set with the time-range command.
`vrf`	VPN Routing/Forwarding instance
`NAME`	VPN Routing/Forwarding instance name. Maximum limit 32 characters

Default

N/A

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#ip sla schedule 1 time-range t1 vrf v1
```


© 2021 IP Infusion Inc. Proprietary

show ip sla statistics

Use this command to display the statistics of IP SLA measurement.

Command Syntax

```
show ip sla statistics (1-65535) detail
```

Parameters

1-65535	IP SLA identifier.

Default

N/A

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#show ip sla statistics 1 detail
========================================
            IP SLA Statistics
========================================
  IP SLA ID                : 1
  Start Time               : 2021 Aug 30 17:40:04
  Elapsed time(milli sec)  : 46015
  Packets Sent             : 23
  Packets Received         : 23
  Packet Loss(%)           : 0.0000
  Invalid Tests            : 0
  Round Trip Delay(usec)
      Minimum              : 1000
      Maximum              : 1000
      Average              : 1000
```

Table 15-52 explains the output fields.

Table 15-52: show ip sla statistics fields

Field	Description
IP SLA ID	IP SLA Identifier (1-65535)
Start Time	Measurement start time
Elapsed time(milli sec)	Time taken to complete the measurement in milliseconds
Packets Sent	Number of packet sent

Table 15-52: show ip sla statistics fields (Continued)

Field	Description
Packets Received	Number of packet received
Packet Loss(%)	Packet lost in percentage
Invalid Tests	Received ICMP echo reply packets after configured threshold limit will be marked as invalid tests
Round Trip Delay(usec)	Round trip delay between ICMP echo request and ICMP echo reply: minimum, maximum and average round trip delay in microseconds

© 2021 IP Infusion Inc. Proprietary

show ip sla summary

Use this command to display the summary of all IP SLA measurements.

Command Syntax

```
show ip sla summary
```

Parameters

None

Default

N/A

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive

ID       Type        Destination       Stats       Return      Last
                                       (usec)        Code        Run
---------------------------------------------------------------------
^1      icmp-echo    20.2.2.3           0           OK        2021 Aug 23 13:53:37
```

Table 15-53 explains the output fields.

Table 15-53: show ip sla summary fields

Field	Description
ID	IP SLA Identifier (1-65535)
Type	Measurement type
Destination	Destination address
Stats (usec)	Round trip time in microseconds for the measurement
Return Code	Measurement status
Last Run	Measurement last run date and time

show running-config ip sla

Use this command to display the IP SLA running configuration alone.

Command Syntax

```
show running-config ip sla
```

Parameters

None

Default

N/A

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#show running-config ip sla
ip sla 1
 icmp-echo ipv4 20.2.2.3
  frequency 2
  threshold 2000
  timeout 5000
ip sla schedule 1 time-range t1 vrf v1
```


© 2021 IP Infusion Inc. Proprietary

threshold

Use this command to configure the threshold for every ICMP echo packet.

Use the `no` form of this command to remove the configured ICMP echo threshold.

Command Syntax

```
threshold <1000-60000>
no threshold
```

Parameters

`1000-60000`	Threshold in milliseconds.

Default

10000 milliseconds

Command Mode

IP SLA ICMP Echo mode (config-ip-sla-echo)

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#threshold 5000
```

timeout

Use this command to configure the timeout for every ICMP echo packet. Any packet arriving beyond this interval is considered to be lost.

Use the `no` form of this command to remove the configured ICMP echo timeout.

Command Syntax

```
timeout <1000-60000>
no timeout
```

Parameters

`1000-60000`	Timeout in milliseconds.

Default

10000 milliseconds

Command Mode

IP SLA ICMP Echo mode (config-ip-sla-echo)

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#timeout 5000
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 16 Linux Shell Commands

This chapter is a reference for Linux shell commands that you can run at the OcNOS prompt.

Table 16-54 describes the commands. Note the following:

- You must be in privileged exec mode to run these commands.
- You cannot use the pipe (“|”) or redirect (">") operators.

Table 16-54: Linux shell commands

Command	Description
`cat` *file*	Display contents of *file*
`cd`	Change to home directory
`cd` *dir*	Change directory to *dir*
`cp` *file1 file2*	Copy *file1* to *file2*
`cp -r` *dir1 dir2*	Copy *dir1* to *dir2*; create *dir2* if it does not exist
`dir`	Display contents of current directory
`less` *file*	Display the contents of file
`ls` *options*	Display contents of current directory
`mkdir` *dir*	Create a directory *dir*
`more` *file*	Display the contents of *file*
`mv` *file1 file2*	Rename *file1* to *file2*
`mv` *file dir*	Move *file* to directory *dir*
`pwd`	Display current directory
`rmdir` *dir*	Remove a directory *dir* (only if empty)

© 2021 IP Infusion Inc. Proprietary

CHAPTER 17 Network Time Protocol

This chapter is a reference for Network Time Protocol (NTP) commands.

NTP synchronizes clocks between computer systems over packet-switched networks. NTP can synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).

NTP uses a hierarchical, layered system of time sources. Each level of this hierarchy is called a “stratum” and is assigned a number starting with zero at the top. The number represents the distance from the reference clock and is used to prevent cyclical dependencies in the hierarchy.

Note: The default time-to-live value for the unicast packets is 64.

This chapter contains these commands:

- clear ntp statistics
- debug ntp
- feature ntp
- ntp acl
- ntp authenticate
- ntp authentication-key
- ntp discard
- ntp enable
- ntp logging
- ntp master
- ntp master stratum
- ntp peer
- ntp server
- ntp source-interface
- ntp sync-retry
- ntp trusted-key
- show ntp authentication-keys
- show ntp authentication-status
- show ntp logging-status
- show ntp peer-status
- show ntp peers
- show ntp statistics
- show ntp trusted-keys
- show running-config ntp

© 2021 IP Infusion Inc. Proprietary

clear ntp statistics

Use this command to reset NTP statistics.

Command Syntax

```
clear ntp statistics (all-peers | io | local | memory)
```

Parameters

`all-peers`	Counters associated with all peers
`io`	Counters maintained in the input-output module
`local`	Counters maintained in the local protocol module
`memory`	Counters related to memory allocation

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ntp statistics all-peers
```


© 2021 IP Infusion Inc. Proprietary

debug ntp

Use this command to display NTP debugging messages.

Use the `no` form of this command to stop displaying NTP debugging messages.

Command Syntax

```
debug ntp
```

```
no debug ntp
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug ntp

(config)#no debug ntp
```

feature ntp

Use this command to enable NTP.

Use the `no` form of this command to disable NTP.

Command Syntax

```
feature ntp (vrf management|)
no feature ntp (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

By default, feature ntp is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature ntp vrf management

(config)#no feature ntp vrf management
```


© 2021 IP Infusion Inc. Proprietary

ntp acl

Use this command to allow paticular client to communicate with NTP server.

Use the `no` form of this command to remove the particular client from NTP server.

Note: ntp discard option and limited rate flag are required for sending the KOD packet.

Command Syntax

```
ntp allow (A.B.C.D | X:X::X:X) (mask (A.B.C.D| <1-128>)|)
({nopeer|noserve|noquery|nomodify|kod|limited|notrap}|) (vrf management|)
no ntp allow (A.B.C.D | X:X::X:X) (mask (A.B.C.D| <1-128>)|)
({nopeer|noserve|noquery|nomodify|kod|limited|notrap}|) (vrf management|)
```

Parameters

`A.B.C.D`	IPV4 address of the client
`X:X::X:X`	IPV6 address of the client
`A.B.C.D`	Mask for the IPv4 address
`1-128`	Mask for the IPv6 address
`nopeer`	Prevent the client from establishing a peer association
`noserve`	Prevent the client from performing time queries
`noquery`	Prevent the client from performing NTPq and NTPdc queries, but not time queries
`nomodify`	Restrict the client from making any changes to the NTP configurations
`kod`	Send a kiss-of-death packet if the client limit has exceeded
`limited`	Deny time service if the packet violates the rate limits established by the discard command
`notrap`	Prevent the client from configuring control message traps
`vrf`	Virtual Router and Forwarding
`management`	Virtual Routing and Forwarding name

Default

By default, only local host is permitted.

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS DC version 4.2.

Example

```
#configure terminal
(config)#ntp allow 1.1.1.1 mask 255.255.255.0 nopeer kod notrap noserve vrf
management
```

ntp authenticate

Use this command to enable NTP authentication.

Use the `no` form of this command to disable authentication.

Command Syntax

```
ntp authenticate (vrf management|)
no ntp authenticate (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

By default, ntp authenticate is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ntp authenticate vrf management
```


© 2021 IP Infusion Inc. Proprietary

ntp authentication-key

Use this command to set an NTP Message Digest Algorithm 5 (MD5) authentication key.

Use the `no` form of this command to delete an authentication key.

Command Syntax

```
ntp authentication-key <1-65535> md5 WORD (vrf management|)
ntp authentication-key <1-65535> md5 WORD 7 (vrf management|)
no ntp authentication-key <1-65535> md5 WORD (vrf management|)
```

Parameters

`<1-65535>`	Authentication key
`WORD`	MD5 string (maximum 8 characters)
`7`	Encrypt using weak algorithm
`management`	Virtual Routing and Forwarding name

Default

The default authentication key is 65535.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ntp authentication-key 535 md5 J@u-b;l2 vrf management
```

ntp discard

Use this command to enable rate limiting access to the NTP service running on a system.

Use the no form of this command to disable rate limiting access to the NTP service running on a system.

This NTP discard option and limited rate flag are required for sending the KOD packet. KOD (Kiss of Death) packets have the leap bits set unsynchronized and stratum set to zero and the reference identifier field set to a four-byte ASCII code. If the noserve or notrust flag of the matching restrict list entry is set, the code is "DENY"; if the limited flag is set and the rate limit is exceeded, the code is "RATE".

Command Syntax

```
ntp discard minimum <1-65535> (vrf management|)
no ntp discard minimum (vrf management|)
```

Parameters

`minimum`	Specify the minimum interpacket spacing <default 2>
`<0-65535>`	Minimum value

Default

By default, the minimum value is 2.

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS DC version 4.2.

Example

```
#configure terminal
(config)#ntp discard minimum 50 vrf management
```


© 2021 IP Infusion Inc. Proprietary

ntp enable

Use this command to enable NTP.

Use the `no` form of this command to disable NTP.

Command Syntax

```
ntp enable (vrf management|)
no ntp enable (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

By default, ntp is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ntp enable vrf management
```

ntp logging

Use this command to log NTP events.

Use the `no` form of this command to disable NTP logging.

Command Syntax

```
ntp logging (vrf management|)
no ntp logging (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

By default, ntp logging message is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ntp logging vrf management
```


© 2021 IP Infusion Inc. Proprietary

ntp master

Use this command to run OcNOS device as NTP server.

Use the `no` command to disable NTP server.

Command Syntax

```
ntp master (vrf management|)
no ntp master (vrf management|)
```

Parameters

`vrf`	Virtual Router and Forwarding
`management`	Virtual Routing and Forwarding name

Default

By default, NTP master is disabled

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS DC version 4.2.

Example

```
#configure terminal
(config)#ntp master vrf management
```

ntp master stratum

Use this command to set stratum value for NTP server.

Use the `no` command to remove stratum value.

The NTP Stratum model is a representation of the hierarchy of time servers in an NTP network, where the Stratum level (0-15) indicates the device's distance to the reference clock.

Command Syntax

```
ntp master stratum <1-15> (vrf management|)
no ntp master stratum (vrf management|)
```

Parameters

`<1-15>`	Stratum value for NTP server
`vrf`	Virtual Router and Forwarding
`management`	Virtual Routing and Forwarding name

Default

By default, NTP startum value is 16.

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS DC version 4.2.

Example

```
#configure terminal
(config)#ntp master stratum 2 vrf management
```


© 2021 IP Infusion Inc. Proprietary

ntp peer

Use this command to configure a peer association. In a peer association, this system can synchronize with the other system or the other system can synchronize with this system.

Use the `no` command to remove a peer association.

Command Syntax

```
ntp peer (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp peer (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp peer (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) (vrf management|)
no ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) (vrf management|)
```

Parameters

`A.B.C.D`	IPv4 address of peer
`HOSTNAME`	Host name of peer
`X:X::X:X`	IPv6 address of peer
`prefer`	Prefer this peer; preferred peer responses are discarded only if they vary dramatically from other time sources
`key`	Peer authentication key
`<1-65534>`	Peer authentication key value
`minpoll`	Minimum poll interval
`<4-16>`	Minimum poll interval value in seconds raised to a power of 2 (default 4 = 16 seconds)
`maxpoll`	Maximum poll interval
`<4-16>`	Maximum poll interval value in seconds raised to a power of 2 (default 6 = 64 seconds)
`management`	Virtual Routing and Forwarding name

Default

By default, value of `minpoll` is 4 and `maxpoll` is 6.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ntp peer 10.10.0.23 vrf management
(config)#ntp peer 10.10.0.23 prefer key 12345 vrf management

(config)#no ntp peer 10.10.0.23 vrf management
```


© 2021 IP Infusion Inc. Proprietary

ntp server

Use this command to configure an NTP server so that this system synchronizes with the server, but not vice versa.

Use the `no` option with this command to remove an NTP server.

Command Syntax

```
ntp server (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
ntp server (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp server (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp server (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) (vrf management|)
no ntp server (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf management|)
no ntp server (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) (vrf management|)
```

Parameters

`A.B.C.D`	IPv4 address of the server
`HOSTNAME`	Host name of the server
`X:X::X:X`	IPv6 address of the server
`prefer`	Prefer this server; preferred server responses are discarded only if they vary dramatically from other time sources
`key`	Server authentication key
`<1-65534>`	Server authentication key
`minpoll`	Minimum poll interval
`<4-16>`	Minimum poll interval value in seconds raised to a power of 2 (default 4 = 16 seconds)
`maxpoll`	Maximum poll interval
`<4-16>`	Maximum poll interval value in seconds raised to a power of 2 (default 6 = 64 seconds)
`management`	Virtual Routing and Forwarding name

Default

By default, `minpoll` is 4 and `maxpoll` is 6.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ntp server 10.10.0.23 vrf management
(config)#ntp server 10.10.0.23 prefer key 12345 vrf management

(config)#no ntp server 10.10.0.23 vrf management
```


© 2021 IP Infusion Inc. Proprietary

ntp source-interface

Use this command to configure an NTP source-interface. NTP sets the source IP address for all NTP packets based on the address of the interface through which the NTP packet are sent.

Use the `no` option with this command to remove an NTP server.

Command Syntax

```
ntp source-interface  IFNAME
```

Parameter

`IFNAME`	Interface name

Default

No default value is specified.

Command Mode

Configure mode

Applicability

This command was introduced in a version before OcNOS 1.3.

Examples

```
#configure terminal
(config)#ntp source-interface xe7/1
(config)#no ntp source-interface xe7/1
```

ntp sync-retry

Use this command to retry NTP synchronization with configured servers.

Command Syntax

```
ntp sync-retry (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#ntp sync-retry vrf management
```


© 2021 IP Infusion Inc. Proprietary

ntp trusted-key

Use this command to define a “trusted” authentication key. If a key is trusted, the device will synchronize with a system that specifies this key in its NTP packets.

Use the `no` option with this command to remove a trusted key.

Command Syntax

```
ntp trusted-key <1-65534> (vrf management|)
no ntp trusted-key <1-65534> (vrf management|)
```

Parameter

`<1-65534>`	Authentication key number
`management`	Virtual Routing and Forwarding name

Default

By default, ntp trusted key is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ntp trusted-key 234676 vrf management
```

show ntp authentication-keys

Use this command to display authentication keys.

Command Syntax

```
show ntp authentication-keys
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp authentication-keys
--------------------------
 Auth Key       MD5 String
--------------------------
123             0xa2cb891442844220
```

Table 17-55 explains the output fields.

Table 17-55: show ntp authentication-key fields

Entry	Description
Auth key	Authentication key (password). Use the password to verify the authenticity of packets sent from this interface or peer interface.
MD5 String	One or more MD5 key strings. The MD5 key values can be from 1 through 16 characters long. You can specify more than one key value within the list.

© 2021 IP Infusion Inc. Proprietary

show ntp authentication-status

Use this command to display whether authentication is enabled or disabled.

Command Syntax

```
show ntp authentication-status
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp authentication-status
Authentication enabled
```

show ntp logging-status

Use this command to display the NTP logging status.

Command Syntax

```
show ntp logging-status
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp logging-status
NTP logging enabled
```


© 2021 IP Infusion Inc. Proprietary

show ntp peer-status

Use this command to display the peers for which the server is maintaining state along with a summary of that state.

Command Syntax

```
show ntp peer-status
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*216.239.35.4    .GOOG.           1 u   24   64  377   38.485    0.149   0.053
```

Table 17-56 explains the output fields.

Table 17-56: show ntp peer-status fields

Entry	Description
Total peers	Number of servers and peers configured.
* - selected for sync, + - peer mode (active), - - peer mode (passive), = - polled in client mode x - source false ticker	Fate of this peer in the clock selection process.
Remote	Address of the remote peer.
refid	Reference ID (0.0.0.0 for an unknown reference ID).
st	The stratum of the remote peer (a stratum of 16 indicated remote peer is unsynchronized).
t	Type of peer (local, unicast, multicast and broadcast).
when	Time the last packet was received.
poll	The polling interval (seconds).

Table 17-56: show ntp peer-status fields

Entry	Description
reach	The reachability register (octal).
delay	Current estimated delay in seconds.
offset	Current estimated offset in seconds.
jitter	Current dispersion of the peer in seconds.

© 2021 IP Infusion Inc. Proprietary

show ntp peers

Use this command to display NTP peers.

Command Syntax

```
show ntp peers
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp peers

------------------------------------------------------------
Peer IP Address                          Serv/Peer
------------------------------------------------------------
216.239.35.4                             Server (configured)
```

Table 17-57 explains the output fields.

Table 17-57: show ntp peers fields

Entry	Description
Peer IP Address	Address of the neighbor protocol.
Serv/Peer	List of NTP peers and servers configured or dynamically learned.

show ntp statistics

Use this command to display NTP statistics.

Command Syntax

```
show ntp statistics (io | local | memory | peer ( ipaddr (A.B.C.D | X:X::X:X ) |
  name (HOSTNAME)) )
```

Parameters

`io`	Counters maintained in the input-output module
`local`	Counters maintained in the local protocol module
`memory`	Counters related to memory allocation
`peer`	Counters associated with the specified peer
`A.B.C.D`	Peer IPv4 address
`X:X::X:X`	Peer IPv6 address
`HOSTNAME`	Peer host name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp statistics local
time since restart:     1685
time since reset:       1685
packets received:       4
packets processed:      0
current version:        0
previous version:       0
declined:               0
access denied:          0
bad length or format:   0
bad authentication:     0
rate exceeded:          0
#show ntp statistics memory
time since reset:     1698
total peer memory:    15
free peer memory:     15
calls to findpeer:    0
new peer allocations: 0
peer demobilizations: 0
hash table counts:      0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
```


© 2021 IP Infusion Inc. Proprietary

Table 17-58 explains the output fields.

Table 17-58: show ntp statisticsfields

Entry	Description
Time since restart	Time when the ntp protocols were last started and how long they have been running.
Time since reset	Time when the ntp protocols were last reset and how long they have been running.
Packets received	Number of packets received from the peers.
Packets processed	Number of packets processed to the peers.
Current version	Current version of the protocol that is being used.
Previous version	Previous version of the protocol that has been used.
Declined	Access to the protocol declined
Access denied	Number of attempts denied to access protocol
Bad length or format	Number of messages received with length or format errors so severe that further classification could not occur.
Bad authentication	Number of messages received with incorrect authentication.
Rate exceeded	Exceed the configured rate if additional bandwidth is available from other queues
Total peer memory	Actual memory available to the peer system.
Free peer memory	Free memory available to the peer system.
Calls to find peer	Number of calls to find peer.
New peer allocations	Number of allocations from the free peer list.
Peer demobilizations	Number of structures freed to free peer list.
Hash table counts	Peer hash table’s each bucket count.

© 2021 IP Infusion Inc. Proprietary

show ntp trusted-keys

Use this command to display keys that are valid for authentication.

Command Syntax

```
show ntp trusted-keys
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp trusted-keys

Trusted Keys:
333
#
```

Table 17-59 explains the output fields.

Table 17-59: show ntp trusted-keys fields

Entry	Description
Trusted Keys	Keys that are valid for authentication.

© 2021 IP Infusion Inc. Proprietary

show running-config ntp

Use this command to display the NTP running configuration.

Command Syntax

```
show running-config ntp (|all)
```

Parameters

`all`	Reserved for future use

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config ntp
feature ntp vrf management
ntp enable vrf management
ntp authenticate vrf management
ntp logging vrf management
ntp authentication-key 123 md5 0xa2cb891442844220 7 vrf management
ntp trusted-key 123 vrf management
ntp server 216.239.35.4 vrf management
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 18 RADIUS

This chapter is a reference for Remote Authentication Dial In User Service (RADIUS) commands, RADIUS provides centralized Authentication, Authorization management for users that connect to and use a network service. RADIUS is specified in RFC 2865.

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF.

- clear radius-server
- debug radius
- radius-server login host
- radius-server login host acct-port
- radius-server login host auth-port
- radius-server login host key
- radius-server login key
- radius-server login timeout
- show debug radius
- show radius-server
- show running-config radius

clear radius-server

Use this command to clear radius-server statistics.

Command Syntax

```
clear radius-server ((HOSTNAME | X:X::X:X | A.B.C.D)|) counters (vrf (management |
  all)|)
```

Parameters

`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`vrf management`	To clear radius server counters for Virtual Routing and Forwarding management
`all`	To clear radius server counters for both management an default vrf
`counters`	To clear radius server counters for default vrf

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS version 1.3.7.

Examples

```
#clear radius-server counters vrf management
```


© 2021 IP Infusion Inc. Proprietary

debug radius

Use this command to display RADIUS debugging information.

Use the `no` form of this command stop displaying RADIUS debugging information.

Command Syntax

```
debug radius
no debug radius
```

Parameters

None

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug radius
```

radius-server login host

Use this command to configure a RADIUS server for both accounting and authentication.

Use the `no` form of this command to remove a RADIUS server.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|)
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|) timeout <1-60>
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|)
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|)
  timeout
```

Parameters

`login`	Remote login
`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`seq-num`	seq-num Sequence Number / Priority index for radius-servers
`<1-8>`	sequence number for servers
`timeout`	How long to wait for a response from the RADIUS server before declaring a timeout failure
`<1-60>`	Range of time out period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management
```


© 2021 IP Infusion Inc. Proprietary

radius-server login host acct-port

Use this command to configure a RADIUS server and specify a UDP port to use for RADIUS accounting messages.

Use the `no` form of this command to remove a RADIUS server.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|) acctport <0-65535> |) | timeout <1-60> |)
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) acct-
  port |) | timeout <1-60> |)
```

Parameters

`login`	Remote login
`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`acct-port`	UDP port to use for RADIUS accounting messages
`<0-65535>`	Range of UDP port numbers
`seq-num`	seq-num Sequence Number / Priority index for radius-servers
`<1-8>`	sequence number for servers
`timeout`	How long to wait for a response from the RADIUS server before declaring a timeout failure
`<1-60>`	Range of timeout period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

By default, radius-server login host acct-port is 1813

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 192.168.2.3 vrf management acct-port 23255
```

radius-server login host auth-port

Use this command to configure a RADIUS server and specify a UDP port to use for RADIUS authentication messages.

Use the `no` form of this command to remove a RADIUS server.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|) (|(authport <0-65535> (|(acct-port <0-65535> (|(timeout <1-60>))))))
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|)
  (auth-port (|(acct-port (|timeout))))
```

Parameters

`login`	Remote login
`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`seq-num`	seq-num Sequence Number / Priority index for radius-servers
`<1-8>`	sequence number for servers
`auth-port`	UDP port to use for RADIUS accounting messages
`<0-65535>`	Range of UDP port numbers
`acct-port`	UDP port to use for RADIUS accounting messages
`<0-65535>`	Range of UDP port numbers
`timeout`	How long to wait for a response from the RADIUS server before declaring a timeout failure
`<1-60>`	Range of timeout period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

By default, radius-server login host acct-port is 1812

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management auth-port 23255
```


© 2021 IP Infusion Inc. Proprietary

radius-server login host key

Use this command to set per-server shared key (“shared secret”) which is a text string shared between the device and RADIUS servers.

Use the no form of this command to remove a server shared key.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|) (|(key ((0 WORD) | (7 WORD) | (WORD)) (|(auth-port <0-65535> (|(acct-
  port <0-65535>
(|(timeout <1-60>))))))))
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (key
  ((0 WORD) | (7 WORD) | (WORD)) (|(auth-port <0-65535> (|(acct-port
  (|(timeout)))))))
```

Parameters

login	Remote login
A.B.C.D	IPv4 address of RADIUS server
X:X::X:X	IPv6 address of RADIUS server
HOSTNAME	DNS host name of RADIUS server
seq-num	seq-num Sequence Number / Priority index for radius-servers
<1-8>	sequence number for servers
0	Unencrypted (clear text) shared key
WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 63 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
auth-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
acct-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
timeout	How long to wait for a response from the RADIUS server before declaring a timeout failure
<1-60>	Range of timeout period in seconds
vrf	Virtual Routing and Forwarding
management	Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management key 0 testing
auth-port 23255
```


© 2021 IP Infusion Inc. Proprietary

radius-server login key

Use this command to set a global preshared key (“shared secret”) which is a text string shared between the device and RADIUS servers.

Use the `no` form of this command to remove a global preshared key.

Command Syntax

```
radius-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
no radius-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
```

Parameters

`login`	Remote login
`0`	Unencrypted (clear text) shared key
`WORD`	Unencrypted key value; maximum length 63 characters
`7`	Hidden shared key
`WORD`	Hidden key value; maximum length 63 characters
`WORD`	Unencrypted (clear text) shared key value; maximum length 63 characters
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login key 7 p2AcxlQA vrf management

#configure terminal
(config)#no radius-server login key 7 p2AcxlQA vrf management
```

radius-server login timeout

Use this command to set the global timeout which is how long the device waits for a response from a RADIUS server before declaring a timeout failure.

Use the `no` form of this command to set the global timeout to its default (1 second).

Note: TELNET client session's default timeout is 60 seconds, so configuring timeout of 60 seconds timeout impacts TELNET client applications, because it cannot be fallback to use the other configured server/group. Hence it is recommended to configure 57 seconds or lesser timeout while using TELNET. This timeout doesn't have an impact on SSH connections.

Command Syntax

```
radius-server login timeout <1-60> (vrf management|)
no radius-server login timeout (vrf management|)
```

Parameters

`login`	Remote login
`<1-60>`	Range of timeout period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Note: The system takes minimum 3 secs to timeout even though the configured timeout value is less than 3 seconds. Hence do not configure timeout value less than 3 secs. The timeout range value is mentioned as 1-60 secs for backward compatibility.

Default

By default, radius-server login timeout is 5 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login timeout 15 vrf management

#configure terminal
(config)#no radius-server login timeout 15 vrf management
```


© 2021 IP Infusion Inc. Proprietary

show debug radius

Use this command to display debugging information.

Command Syntax

```
show debug radius
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug radius
RADIUS client debugging is on
```

show radius-server

Use this command to display the RADIUS server configuration.

Command Syntax

```
show radius-server (|vrf(management|all))((WORD)|(groups (GROUP|))|)|sorted
```

Parameters

WORD	DNS host name or IP address
groups	RADIUS server group
GROUP	Group name; if this parameter is not specified, display all groups
sorted	Sort by RADIUS server name
vrf	management or all VRFs

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show radius-server vrf management
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:
Radius Server                          : 10.12.12.39
   Sequence Number                     : 1
   available for authentication on port : 1812
   available for accounting on port     : 1813
   RADIUS shared secret                 : ********
   Failed Authentication count          : 0
   Successful Authentication count      : 0
   Failed Connection Request            : 0
   Last Successful authentication       :

Radius Server                          : 1.1.1.1
   Sequence Number                     : 2
   available for authentication on port : 1234
   available for accounting on port     : 1234
   timeout                             : 5
   Failed Authentication count          : 0
   Successful Authentication count      : 0
   Failed Connection Request            : 0
   Last Successful authentication       :
```

Table 18-60 explains the output fields.

© 2021 IP Infusion Inc. Proprietary

Table 18-60: show radius-server fields

Entry	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Timeout Value	Period the local router waits to receive a response from a RADIUS accounting server before retransmitting the message
Total number of servers	Number of authentication requests received by the authentication server.

show running-config radius

Use this command to display RADIUS configuration settings in the running configuration.

Command Syntax

```
show running-config radius
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config radius
radius-server login key 7 0x67efdb4ad9d771c3ed8312b2bc74cedb vrf management
radius-server login host 10.12.12.39 vrf management seq-num 1 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 19 Secure Shell

This chapter describes Secure Shell (SSH) commands.

SSH is a cryptographic protocol for secure data communication, remote login, remote command execution, and other secure network services between two networked computers.

Note: In OcNOS, the default Linux terminal type is "export TERM=xterm"

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

- clear ssh host-key
- clear ssh hosts
- debug ssh server
- feature ssh
- show debug ssh-server
- show running-config ssh server
- show ssh host-key
- show ssh server
- show username
- ssh
- ssh6
- ssh server algorithm encryption
- ssh keygen host
- ssh login-attempts
- ssh server port
- ssh server session-limit
- username sshkey
- username keypair

clear ssh host-key

Use these commands to remove SSH server host key.

Command syntax

```
clear ssh host-key  ((dsa|rsa|ecdsa|ed25519)|) (vrf management|)
```

Parameters

`dsa`	dsa keys
`rsa`	rsa keys
`ecdsa`	ecdsa keys
`ed25519`	ed25519 keys
`management`	Management VRF

Default

If no keys are specified, all the host keys will be removed

Command Mode

Privilege exec mode

Applicability

This command was introduced in OcNOS version 5.0

Examples

```
OcNOS#clear ssh host-key vrf management
OcNOS#
OcNOS#clear ssh host-key rsa
OcNOS#
```


© 2021 IP Infusion Inc. Proprietary

clear ssh hosts

Use this command to clear the `known_hosts` file.

This command clears all trusted relationships established with SSH servers during previous connections. When a client downloads a file from an external server the first time, the client stores the server keys in the `known_hosts` file. After that, other connections to the same server will use the server keys stored in the `known_hosts` file. In other words, a trusted relationship is created when a client accepts the server keys the first time.

An example of when you need to clear a trusted relationship is when SSH server keys are changed.

Command Syntax

```
clear ssh hosts
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ssh hosts
```

debug ssh server

Use this command to display SSH server debugging information.

Use the `no` form of this command to stop displaying SSH server debugging information.

Command Syntax

```
debug ssh server
no debug ssh server
```

Parameters

None

Default

By default, disabled.

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ssh server
```


© 2021 IP Infusion Inc. Proprietary

feature ssh

Use this command to enable the SSH server.

Use the `no` form of this command to disable the SSH server.

Command Syntax

```
feature ssh (vrf management|)
no feature ssh (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)feature ssh
```

show debug ssh-server

Use this command to display whether SSH debugging is enabled.

Command Syntax

```
show debug ssh-server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug ssh-server
ssh server debugging is on
```


© 2021 IP Infusion Inc. Proprietary

show running-config ssh server

Use this command to display SSH settings in the running configuration.

Command Syntax

```
show running-config ssh server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config ssh server
feature ssh vrf management
ssh server port 1024 vrf management
ssh login-attempts 2 vrf management
ssh server algorithm encryption 3des-cbc
```

show ssh host-key

Use this command to display the SSH server key.

By default, ssh feature is enabled in "management" vrf. Until and unless the same feature is explicitly enabled in "default" vrf, respective show command output will be empty.

Command syntax

```
show ssh host-key  ((dsa|rsa|ecdsa|ed25519)|) (vrf management|)
```

Parameters

`dsa`	dsa keys
`rsa`	rsa keys
`ecdsa`	ecdsa keys
`ed25519`	ed25519 keys
`management`	Management VRF

Default

If no keys are specified, all host keys will be displayed

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0

Examples

```
#sh ssh host-key
************************************************
dsa public key :

ssh-dss AAAAB3NzaC1kc3MAAACBANgq+TZPkmKOn7ot7PBO9TOCV/
+GPyHCz9Wq39+6veigQ2CWmLNo
uqZb1B05LfeU2MuRz4rtO6mcX81nAygqDLNZaRsirYdWTsJ40HAOZYr9765w+M8TAcKmBYbuWSIkqn
YQ
J1h5bj6UrJ7dW4LgaSxmVmrkXoYrr5gnxfEVgw8HAAAAFQC//
BVHnTWh8Iizbk0mvOyNzqtfMwAAAIBQ
Ca9X0qbL66Js0ul+7LMmLvWkC4Fy1Y/3igZORZ+NsNP4CJIJ1JCLwj7nj/NeUfUuyG1/
dnDVdki4FngL
LjbVa5XrK5VbsEj4sZBfebkLVZKd8h880FqNhfc3iZjCGqdYrWWlRYdNqNvq7zVa6YC7Vvo0sEC5/
rDm
aNygbx0iCAAAAIEAoZHk+5cqaYptqYBPGPMRynpWyWJPJQjoiy+p1BRNk7E/kwInQaqmtFQuM/
YaTOoN
nz5skwQ1dJmdJGq+h7bfmab0atzaaVjkcTjz0rtSBO3JID2G6KqG55yhr03bC8BY+A6g9Qm8TuWZU6
8D
NIZGj28GZSbkIpQgqSD9VUAxEHs=

dsa fingerprint :
```


© 2021 IP Infusion Inc. Proprietary

```
1024 SHA256:Qzd8n4RjsxeW9+AnUP+zc59oPRTl2FBwdwDfVBq0DdQ
**************************************************
**************************************************
rsa public key :

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC706mz0GQvdEaqK/2zUUtCOh/
kEUkZpQ7d8gie4jf1
yV4nV2g1u7oIbdnoBBI0a5bIwbUGDHPUvfTpoJntpryY7G/
QIWuBJVDiu6QteoB4u5byNVbSqA3fljbF
MISYfLxK3i3S07htadDfUIpYTyx/
D5PCf8DDxmdf7UkhOM4Quj8GgGW3PacE2YyJASBq5x7MaWEUiStu
NgtemWqR/DTw+OO8l3gZzHhWBcmHLzo3jdkH/
8ffLGEWqEb78wR4lxckVlja4suFB0GEa7vFLucYO3Tp
GzZARf7iY5A0bB0fi7Zi1yQ3RN7+di28lSNWsFCzZm8vWS7GyLUFn1xttlqJ

rsa fingerprint :

2048 SHA256:YVX+zlrDk8bqzF+HPKpFW0BttbLoiQ5IBDVI/VMYhbs
**************************************************
**************************************************
ecdsa public key :

ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBCN/
XoG
uZGwNfKCE+cuQOULrSHomRSmkDp0u6MsoNIVLhtRe9+r8Ak7G8taE55D7NgugnEDzdLKBmeCZWcww6
4=

ecdsa fingerprint :

256 SHA256:T7KOgXyrU/38EvO6z/apgYDANf+q9YhqCiYoocD5Ajg
**************************************************
**************************************************
ed25519 public key :

ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAII/jNFIYKbUk/ePbp4wu/
AjhP5gERqn6F+4tH39idbh7

ed25519 fingerprint :

256 SHA256:1MU6iy03eEQBj099GERLjkMCPDoUwkdCwGh8bgYZbeo
**************************************************
#
```

show ssh server

Use this command to display the SSH server status.

Command Syntax

```
show ssh server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ssh server
VRF MANAGEMENT:
ssh server enabled port: 22
authentication-retries 3
VRF DEFAULT:
ssh server enabled port: 22
authentication-retries 3
#
```


© 2021 IP Infusion Inc. Proprietary

show username

Use this command to display the RSA or DSA key pair for a user.

Command Syntax

```
show username USERNAME keypair
```

Parameters

USERNAME	User identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3

Examples

```
#show username kedar keypair
***************RSA KEY*******************
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDCnWo/3Y7LlVkw/Z43dbVIm+I3o25JlgUTmwa9ll
T35+2gNvDbIPfYAqUKYgrmXKDc9vg7f4SAsmXS+4ZwrrQSTTsHk8PNLA+4lEcufFNl3jpfXTuhphN9
N9
i+uFHGYIIviWZksiRqpMZmDlALyzAIOzyCfG44hlRm3/
pYfhBNhHruvxYVhbP4wHsmrWfcFb+HZCWQGM
CJupxu8bouGd2UW5/BlVy1yuYNIhdo2NHjUI+ameETV+Wroki8+OLVA6eXp5/
KY3Bj9x2+AxOCiKcpU0
axwFSoCbP3+29wrp4JJhl4ssSqM+19+VbUtpuXAM0cR7VQ7mJ0JDZ9tBvK4l8/
bitcount: 2048 fingerprint: 2b:ac:17:a4:ef:1d:79:4e:2d:17:af:72:4c:c7:e4:2f
***********************************
***************DSA KEY*******************
ssh-dss AAAAB3NzaC1kc3MAAACBAP0npAm+Pw8t7OpO+KQ0Vx3ayXavHHVPPAKOo8RTmquE8zUSjn
/XiZ+vP2343RpXu9/
jLwAcCUMfNBZyE8NbmGKxMMk2PqMz10VtfvDOn5LSNurXL4lypZLG2hR2PNva4w
6b4Adpd+E1fEoUncIgOun2i4SO8N5TCMYVyusKjYzDAAAAFQCWeAzeahZeoIzBlnSo87madxfL3QAA
AI
EA4b86l/
nHoWobRoYBrkeOGtjyWLRKk1P2T+rGH+j0rqqJiD0sh2PVfppylliNvqLtYSmXyMCxzEEeFd
HH1cVXgrgQjtUOeCPhF+2We2ummmlCwg4v71Z358FRjsi9VgJ/vQUpOq1hRDhwjJHtEHSA+NkX/
ccW9J
ww8YOoNhCI7DcAAACANuYiP6tKGSU9LeClF1F65Tq1blVHfLp3TSeZYPldqonDoZ1qo3NNvOOH5KN8
Lj
MRtTCN1GaXow1QccS941XFy3efuWXxC00HZ64FhmjCyOYYv2Wsvn4UGCAG3ikiu6M1xjOLl6b53H4m
B3
w7O6bkcjH1GnytwrgR0D/nlsZ/9fs=
bitcount: 1024 fingerprint: c1:0a:e5:e1:a1:78:ae:c2:4a:07:4a:50:07:4b:d5:84
***********************************
```

ssh

Use this command to open an ssh session to a IPv4 address or host name resolved to an IPv4 address.

Command Syntax

```
ssh WORD (vrf (NAME | management))
ssh WORD <1-65535> (vrf (NAME | management))
ssh (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc|
aes256-cbc | 3des-cbc)) WORD  (vrf (NAME | management))
ssh (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc |
aes256-cbc | 3des-cbc)) WORD <1-65535> (vrf (NAME | management))
```

Parameters

`WORD`	User and destination host name to resolve into IPv4 address to open a SSH session as user@ipv4-address/hostname
`1-65535`	Destination Port to open a SSH session. Default is 22.
`cipher`	Specify algorithm to encrypt SSH session
`aes128-ctr`	Advanced Encryption Standard 128 bit Counter Mode
`aes192-ctr`	Advanced Encryption Standard 192 bit Counter Mode
`aes256-ctr`	Advanced Encryption Standard 256 bit Counter Mode
`aes128-cbc`	Advanced Encryption 128 bit Standard Cipher Block Chaining
`aes192-cbc`	Advanced Encryption Standard 192 bit Cipher Block Chaining
`aes256-cbc`	Advanced Encryption Standard 256 bit Cipher Block Chaining
`3des-cbc`	Triple Data Encryption Standard Cipher Block Chaining
`vrf`	VPN routing/forwarding instance.
`NAME`	Name of the VPN routing/forwarding instance.
`management`	Management VPN routing/forwarding instance.

Default

The default destination port is 22.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#ssh cipher aes128-ctr 10.12.16.17 22 vrf management
The authenticity of host '10.12.16.17 (10.12.16.17)' can't be established.
RSA key fingerprint is 93:82:98:ce:b7:20:1a:85:a5:9a:2e:93:13:84:ea:9e.
Are you sure you want to continue connecting (yes/no)?
```


© 2021 IP Infusion Inc. Proprietary

ssh6

Use this command to open an ssh session to an IPv6 address or host name resolved to an IPv6 address.

Command Syntax

```
ssh6 (X:X::X:X | HOSTNAME) (vrf (NAME | management))
ssh6 (X:X::X:X | HOSTNAME) <1-65535> (vrf (NAME | management))
ssh6 (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc |
aes256-cbc | 3des-cbc)) (X:X::X:X | HOSTNAME) (vrf (NAME | management))
ssh6 (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc |
aes256-cbc | 3des-cbc))  (X:X::X:X | HOSTNAME) <1-65535> (vrf (NAME |
management))
```

Parameters

`X:XX::X:X`	User and destination IPv6 address to open an SSH session as user@ipv6-address
`HOSTNAME`	User and destination host name to resolve into IPv6 address to open an SSH session as user@ipv4-address/hostname
`1-65535`	Destination Port to open a SSH session. Default is 22.
`cipher`	Algorithm to encrypt SSH session
`aes128-ctr`	Advanced Encryption Standard 128 bit Counter Mode
`aes192-ctr`	Advanced Encryption Standard 192 bit Counter Mode
`aes256-ctr`	Advanced Encryption Standard 256 bit Counter Mode
`aes128-cbc`	Advanced Encryption 128 bit Standard Cipher Block Chaining
`aes192-cbc`	Advanced Encryption Standard 192 bit Cipher Block Chaining
`aes256-cbc`	Advanced Encryption Standard 256 bit Cipher Block Chaining
`3des-cbc`	Triple Data Encryption Standard Cipher Block Chaining
`vrf`	VPN routing/forwarding instance.
`NAME`	Name if the VPN routing/forwarding instance.
`management`	Management VPN routing/forwarding instance.

Default

The default destination port is 22.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#ssh6 cipher aes128-ctr 2:2::2:2 22 vrf management
The authenticity of host '2:2::2:2 (2:2::2:2)' can't be established.
RSA key fingerprint is 93:82:98:ce:b7:20:1a:85:a5:9a:2e:93:13:84:ea:9e.
```

```
Are you sure you want to continue connecting (yes/no)?
```


© 2021 IP Infusion Inc. Proprietary

ssh server algorithm encryption

Use this command to set an encryption algorithm for SSH sessions.

An SSH server authorizes connection of only those algorithms from the list below. If a client tries to establish a connection to the server with the algorithm encryption not in the list, the connection fails.

SSH supports these encryption algorithms:

- Advanced Encryption Standard Counter:
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - aes128-cbc
- Advanced Encryption Standard Cipher Block Chaining:
  - aes192-cbc
  - aes256-cbc
- Triple Data Encryption Standard Cipher Block Chaining:
  - 3des-cbc

Use the `no` form of this command to not encrypt SSH sessions.

Command Syntax:

```
ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc
  |aes192-cbc | aes256-cbc | 3des-cbc} (vrf management|)
no ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-
  cbc |aes192-cbc | aes256-cbc | 3des-cbc} (vrf management|)
```

Parameters

`aes18-ctr`	AES 128 bit Counter Mode
`aes192-ctr`	AES 192 bit Counter Mode
`aes256-ctr`	AES 256 bit Counter Mode
`aes128-cbc`	AES 128 bit Cipher block chaining
`aes192-cbc`	AES 192 bit Cipher block chaining
`aes256-cbc`	AES 256 bit Cipher block chaining
`3des-cbc`	Triple DES Cipher block chaining
`vrf management`	Management VPN routing/forwarding instance.

Default

No encryption.

By default, all the ciphers are supported for a new SSH client to connect to the SSH server.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ssh server algorithm encryption aes128-ctr
```


© 2021 IP Infusion Inc. Proprietary

ssh keygen host

Use these commands to create SSH server host, and public keys. These host keys are added in the SSH clients known_hosts file after user's acceptance.

Once entry is added in known_hosts, for the subsequent attempt login to the server will be validated against the host key and if there is key mismatch user will be prompted about the change in server identity.

Command syntax

```
ssh keygen host dsa (vrf management|) (force|)
ssh keygen host rsa (length <1024-4096>|) (vrf management|) (force|)
ssh keygen host ecdsa (length (256|384|521)|) (vrf management|) (force|)
ssh keygen host ed25519 (vrf management|) (force|)
```

Parameters

`dsa`	dsa keys
`rsa`	rsa keys
`ecdsa`	ecdsa keys
`ed25519`	ed25519 keys
`management`	Management VRF
`force`	Replace the old host-key with newly generated host-key
`<1024-4096>`	Number of bits to use when creating the SSH server key; this parameter is only valid for RSA keys (DSA keys have a default length of 1024)

Default

DSA key has length of 1024 bits

RSA key has default length of 2048 bits

ECDSA key has default length of 521 bits

ED25519 key has length of 256 bits

Command Mode

Privilege exec mode

Applicability

This command was introduced in OcNOS version 5.0

Examples

```
OcNOS#ssh keygen host rsa vrf management
OcNOS#
OcNOS#ssh keygen host ecdsa vrf management
OcNOS#
OcNOS#ssh keygen host ecdsa
%% ssh host key exists, use force option to overwrite
OcNOS#
OcNOS#ssh keygen host ecdsa force
```

ssh login-attempts

Use this command to set the number of times that a user can try to log in to a SSH session.

Use the `no` form of this command to set the number of login attempts to its default (3).

Enable the feature ssh command to configure this command on default vrf port.

You can only give this command when the SSH server is enabled for default vrf. See the feature ssh command.

Command Syntax

```
ssh login-attempts RETRIES (vrf management|)
no ssh login-attempts (vrf management|)
```

Parameters

`RETRIES`	Number of retries <1-3>
`management`	Management VPN routing/forwarding instance.

Default

By default, the device attempts to negotiate a connection with the connecting host three times.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ssh login-attempts 3
```


© 2021 IP Infusion Inc. Proprietary

ssh server port

Use this command to set the port number on which the SSH server listens for connections. The default port on which the SSH server listens is 22.

Use the `no` form of this command to set the default port number (22).

Command Syntax

```
ssh server port <1024-65535> (vrf management|)
no ssh server port (vrf management|)
```

Parameters

`<1024-65535>`	Port number
`management`	Management VPN routing/forwarding instance.

Default

By default, the SSH server port is 22.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ssh server port 1720
```

ssh server session-limit

Use this command to limit number of SSH sessions. Only 40 sessions allowed including Telnet and SSH.

Use `no` form of this command to set to default value.

Command Syntax

```
ssh server session-limit <1-40> (vrf management|)
no ssh server session-limit (vrf management|)
```

Parameters

`<1-40>`	Number of sessions
`management`	Virtual Routing and Forwarding name

Default

By default, 40 sessions are allowed.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.2

Examples

```
#configure terminal
(config)#ssh server session-limit 4 vrf management
```


© 2021 IP Infusion Inc. Proprietary

username sshkey

Use this command to create a user account.

Command Syntax

```
username USERNAME sshkey LINE
```

Parameters

`USERNAME`	User identifier
`LINE`	Digital System Algorithm (DSA) key or Rivest, Shamir, and Adelman (RSA) key in OpenSSH format; this key is written to the `authorized_keys` file

Default

By default, SSHKEY is 1024.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#username fred sshkey ssh-rsa
AAAAB3NzaC1kc3MAAAEBAIirweZzCdyITqbMWB8Wly9ivGxY1JBVnWTVtcWKi6uc
CPZyw3I6J6/+69LEkPUSAyO+SK8zj0NF2f25FFc2YDMh1KKHi5gK7iXF3/ran54j
nP2byyLeo8rnuVqfEDLaBI1qQaWBcDQvsZc14t5SEJfsOQSfR03PDqPYAisrZRvM
5pWfzo486Rh33J3+17OuARQtZFDP4wA5zZoFxhl4U3RK42JzKNUiYBDrH3lSgfkv
XLWLXz9WcxY6zuKvXFwUpOA9PRXwUsKQqWuyywZQLNavENqFyoQ8oZnNKLCYE0h8
QnUe62NGxb3jQXKLflOL04JFNiii9sACG1Y/ut4ANysAAAAVAJbM7Z4chRgiVahN
iwXFJNkBmWGZAAABAAuF1FlI6xy0L/pBaIlFw34uUL/mh4SR2Di2X52eK70VNj+m
y5eQdRC6cxpaVqpS3Q4xTN+W/kaBbIlX40xJP5lcjMvfn/nqiuIeEodmVIJMWxOD
fh3egeGuSW614Vzd1RGrxpYInIOygMULRcxhmbX+rPliuUIvhg36iH0UR7XBln6h
uyKFvEmaL7bGlRvELjqaj0y6iiCfP1yGBc5vavH5X+jOWqdsJHsCgcIzPF5D1Ybp
w0nZmGsqO+P55mjMuj0O2uI7Ns1sxyirbnGhd+ZZ1u03QDy6MBcUspai8U5CIe6X
WqvXY+yJjpuvlW9GTHowCcGd6Z/e9IC6VE/kNEAAAAEAFIe6kLGTALR0F3AfapYY
/M+bvkmkkhOJUZVdLiwMjcvtJb9fQpPxqXElS3ZvUNIEElUPS/V7KgSsj8eg3FKN
iUGICkTwHIK7RTLC8k4IE6U3V3866JtxW+Znv1DB7uwnbZgoIZuVt3r1+h8O0ah8
UKwDUMJT0fwu9cuuS3G8Ss/gKi1HgByrcxXoK51/r4Bc4QmR2VQ8sXOREv/SHJeY
JGbEX3OxjRgXC7GlpbrdPiL8zs0dPiZ0ovAswsBOYlKYhd7JvfCcvWRjgP5h55aw
GNSmNs3STKufbIqYGeDAISYNYY4F2JzR593KIBnWgyhokyYybyEBh8NwTTO4J5rT
ZA==
```

username keypair

Use this command to generate the key for users.

Command Syntax

```
username USERNAME keypair rsa
username USERNAME keypair dsa
username USERNAME keypair rsa length <1024-4096>
username USERNAME keypair rsa length <1024-4096> force
username USERNAME keypair rsa force
username USERNAME keypair dsa force
```

Parameters

`USERNAME`	User identifier
`rsa`	Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key
`dsa`	Digital System Algorithm (DSA) SSH key
`<1024-4096>`	Number of bits to use when creating the SSH server key; this parameter is only valid for RSA keys (DSA keys have a default length of 1024)
`force`	Forces the replacement of an SSH key

Default

DSA keys have a default value of 1024.

RSA keys have a minimum key length of 1024 bits and the default length is 4096.

By default the system has RSA/DSA public/private key pair placed in /etc/ssh/. The force option is used if the user wants to regenerate the ssh rsa keys. The same thing applies for dsa also.

Command Mode

Execute mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
    #configure terminal
(config)#username fred keypair rsa
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 20 sFlow Commands

This chapter describes the Sampled Flow (sFlow) commands.

- clear sflow statistics
- debug sflow
- feature sflow
- sflow agent-ip
- sflow collector
- sflow poll-interval
- sflow sampling enable
- sflow sampling-rate
- show sflow
- show sflow interface
- show sflow statistics

clear sflow statistics

Use this command to clear sFlow sampling-related counters such as the number of packets sampled and the number of counters sampled.

Command Syntax

```
clear sflow statistics (interface IFNAME|)
```

Parameters

IFNAME	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear sflow statistics
```


© 2021 IP Infusion Inc. Proprietary

debug sflow

Use this command to display sFlow debugging messages.

Command Syntax

```
debug sflow (all|agent|sampling|polling|)
```

Parameters

`all`	Debug all (agent,sampling,polling)
`agent`	Debug sFlow agent
`sampling`	Debug sFlow sampling
`polling`	Debug sFlow polling

Default

By default, debug command is disabled.

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug sflow all
#debug sflow agent

#configure terminal
(config)#debug sflow agent
```

feature sflow

Use this command to enable the sFlow feature.

Use the no form to disable the sFlow feature.

Command Syntax

```
feature sflow
no feature sflow
```

Parameters

None

Default

By default, sFlow feature is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#feature sflow
```


© 2021 IP Infusion Inc. Proprietary

sflow agent-ip

Use this command to manually configure the agent IP address when there the eth0 IP address is down. The sflow is enabled only when the eth0 ip address available. The switch sends th sflow packets to the sflow collecter via agent IP address.

Command Syntax

```
sflow agent-ip A.B.C.D
no sflow agent-ip
```

Parameters

`agent-ip`	sFlow Agent
`A.B.C.D`	Ipv4 address type

Default

By default, disabled.

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.9

Example

```
OcNOS(config)#sflow agent-ip 10.10.10.1
OcNOS(config)#no sflow agent-ip
```

sflow collector

Use this command to configure the collector details such as the collector IPv4 address, port number, receiver time-out and datagram size.

Use the `no` form of this command to disable the sFlow collector.

Command Syntax

```
sflow collector A.B.C.D port <1024-65535> receiver-time-out <0-2147483647>
  max-datagram-size <200-9000>
no sflow collector (A.B.C.D port <1024-65535>|)
```

Parameter

`A.B.C.D`	Collector IPv4 address
`<1024-65535>`	Collector UDP Port number. The standard sFlow UDP Port : 6343
`<0-2147483647>`	Receiver time out value in seconds. Zero means no timeout. Upon timeout, value collector information is removed, stopping any ongoing sampling.
`<200-9000>`	Maximum datagram size in bytes that can be sent Collector

Default

By default, sFlow collector is disabled. Default port number is 6343.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#sflow collector 2.2.2.2 port 1111 receiver time-out 30 max-datagram-
size 500

(config)#no sflow collector
```


© 2021 IP Infusion Inc. Proprietary

sflow poll-interval

Use this command to configure the sFlow counter polling interval. Any change in the polling interval restarts ongoing polling of existing data source interfaces, if any.

Use the `no` form of this command to disable the sFlow counter polling interval.

Command Syntax

```
sflow poll-interval <5-60>
no sflow poll-interval
```

Parameters

`<5-60>`	Interface counter. Polling interval in seconds

Default

By default, sFlow counter polling interval is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#sflow poll-interval 25
(config-if)#no sflow poll-interval
```

sflow sampling enable

Use this command to enable or disable sampling on an interface after giving the sflow sampling-rate command on the same interface.

Note: sFlow egress sampling for multicast, broadcast, or unknown unicast packets is not supported.

Command Syntax

```
sflow enable
no sflow enable
```

Default

By default, sFlow sampling is disabled.

Command Mode

Interface mode

Parameters

None

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface xe1
(config-if)#sflow sampling-rate 1024 direction ingress max-datagram-size 200
(config-if)#sflow enable
(config-if)#no sflow enable
```


© 2021 IP Infusion Inc. Proprietary

sflow sampling-rate

Use this command to set the sampling rate on an interface. Any change in the sampling rate restarts the ongoing sampling of existing data-source interfaces, if any.

Use the `no` form of this command to disable the sFlow sampling rate.

Note: Packets to CPU is rate limited. In case of unknown unicast, rate limit is applied to such packets as well as sampled data packets.

Command Syntax

```
sflow sampling-rate <1024-16777215> direction (ingress | egress) max-header-size
  <128-256>
no sflow sampling-rate direction (ingress | egress)
```

Parameters

`<1024-16777215>`	Sampling rate
`direction`	The direction of sampling an interface:
`ingress`	Ingress traffic
`egress`	Egress traffic
`<128-256>`	Maximum header size in bytes

Default

By default, sFlow sampling rate is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#sflow sampling-rate 1024 direction ingress max-header-size 200
(config-if)#no sflow sampling-rate direction ingress
```

show sflow

Use this command to display sFlow agent configuration along with statistics for all interfaces.

Command Syntax

```
show sflow (brief | detail)
```

Parameters

`brief`	Display configuration parameters on interfaces along with sampling rate and poll interval.
`detail`	Same as `brief` along with configured and default attributes and values of sFlow agent, sFlow collector, and sampling information.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show sflow
sFlow Feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 10.12.16.38
Collector IP: 10.12.16.17      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface  Packet-Sampling           Packet-Sampling            Counter-Polling         Maximum Header
                 Rate                     Count               Interval       Count        Size(bytes)
           Ingress      Egress       Ingress      Egress       (sec)                     Ingress     Egress
---------  -----------------------   -----------------------  -----------------------   --------------------
xe1            1024            0           0            0           6            3     128            0

#
#show sflow brief
sFlow Feature: Enabled
Collector IP: 10.12.16.17      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Configuration:
Interface   Status               Sample Rate               Counter-Polling
            Ingress    Egress    Ingress      Egress       Interval(sec)
---------   ------------------   ----------------------    ---------------
xe1       Enabled    Disabled         1024            0      6
```


© 2021 IP Infusion Inc. Proprietary

Table 20-61: Show sflow output

Entry	Description
sFlow feature	Shows whether sFlow is enabled or disabled.
sFlow Version	Displays the sFlow version. Version 5 is the current global standard.
sFlow Global Information	Global Information consists of the Agent IP address, Collector IP, Port number, Maximum Datagram Size, and the Receiver timeout.
Agent IP	IPv4 address of this switch/router.
Collector IP	IPv4 address of the sFlow collector server.
Port	Port number on the sFlow collector server. Standard is port 6343.
Maximum Datagram Size	The maximum size of the datagrams sent by the agent
Receiver timeout	The number of seconds between each sampling – zero means sample continuously.
sFlow Port Interface	The interface of this switch/router on which sFlow is running (e.g. xe1/1).
Packet-Sampling Rate	the number of packets received or transmitted before a sample is taken.
Packet-Sampling Count	The number of sample packets that have been sampled on both the ingress and egress of the interface.
Counter-Polling	Shows the amount of time between polling samples and the count of the total number of polling samples taken.
Maximum Header Size	The maximum header size for both the ingress and egress of the interface.

© 2021 IP Infusion Inc. Proprietary

show sflow interface

Use this command to display the sFlow configuration for the input interface.

Command Syntax

```
show sflow interface IFNAME
```

Parameters

IFNAME	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Note: For information about the output of this command, see the show sflow command.

```
#show sflow interface xe1
sFlow feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 10.10.26.104
Collector IP: 10.12.16.18      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface  Packet-Sampling           Counter-Polling           Maximum Header
           Rate         Count        Interval(sec) Count       Size(bytes)
---------  -----------------------   ------------------------  --------------
xe1              1024            0           6           41      128
```


© 2021 IP Infusion Inc. Proprietary

show sflow statistics

Use this command to display sFlow counter information.

Command Syntax

```
show sflow statistics (interface IFNAME|)
```

Parameters

IFNAME	Interface name.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Note: For information about the output of this command, see the show sflow command.

```
#show sflow statistics

sFlow Port Statistics:
Interface  Packet-Sampling   Counter-Polling
                Count              Count
---------  ---------------   ---------------
xe1                      0                19
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 21 Simple Network Management Protocol

This chapter is a reference for Simple Network Management Protocol (SNMP) commands.

SNMP provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- An SNMP manager: The system used to control and monitor the activities of network devices. This is sometimes called a Network Management System (NMS).
- An SNMP agent: The component within a managed device that maintains the data for the device and reports these data SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables which describe the system configuration. These variables can be queried (and sometimes set) by SNMP managers.

In SNMP, administration groups are known as *communities*. SNMP communities consist of one agent and one or more SNMP managers. You can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The security levels are:

- noAuthNoPriv: No authentication or encryption
- authNoPriv: Authentication but no encryption
- authPriv: Both authentication and encryption.

SNMP is defined in RFCs 3411-3418.

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

- clear snmp hostconfig
- debug snmp
- debug snmp-server
- show running-config snmp
- show snmp
- show snmp community
- show snmp engine-id
- show snmp group
- show snmp host
- show snmp user
- show snmp view
- snmp-server community
- snmp-server contact
- snmp-server enable snmp

© 2021 IP Infusion Inc. Proprietary

- snmp-server enable traps
- snmp-server host
- snmp-server location
- snmp-server tcp-session
- snmp-server user
- snmp-server view

© 2021 IP Infusion Inc. Proprietary

clear snmp hostconfig

Use this command to remove all SNMP trap hosts.

Command Syntax

```
clear snmp hostconfig
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear snmp hostconfig
```

debug snmp

Use this command to enable debugging for SNMP Agentx.

Use the `no` parameter with this command to disable SNMP Agentx debugging.

Command Syntax

```
debug snmp (all | detail | error-string | process | receive | send | xdump |)
no debug snmp (all | detail | error-string | process | receive | send | xdump |)
```

Parameters

`all`	All debugging (included hexa-dump and error-string)
`detail`	Detail debugging
`error-string`	Error string display
`process`	Packet process
`receive`	Packet receive
`send`	Packet send
`xdump`	Packet hexa dump

Command Mode

Exec mode

Applicability

This command was introduced in a version before OcNOS version 1.3.

Example

```
#debug snmp all
```


© 2021 IP Infusion Inc. Proprietary

debug snmp-server

Use this command to display SNMP debugging information.

Use the `no` form of this command to stop displaying SNMP debugging information.

Command Syntax

```
debug snmp-server
no debug snmp-server
```

Parameters

None

Default

By default, disabled.

Command Mode

Exec and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug snmp-server
```

show running-config snmp

Use this command to display the SNMP running configuration.

Command Syntax

```
show running-config snmp
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config snmp
snmp-server view all .1 included
snmp-server community abc group network-admin
snmp-server enable snmp
```


© 2021 IP Infusion Inc. Proprietary

show snmp

Use this command to display the SNMP configuration, including session status, system contact, system location, statistics, communities, and users.

Command Syntax

```
show snmp
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp
SNMP Protocol:Enabled
sys Contact:
sys Location:

--------------------------------------------------------------------------------
Community Group/Access Context acl_filter
--------------------------------------------------------------------------------
public network-admin
_____________________________________________________________________________

                        SNMP USERS
_____________________________________________________________________________
User Auth Priv(enforce) Groups
_____________________________________________________________________________

SNMP Tcp-session :Disabled
```

show snmp community

Use this command to display SNMP communities.

Command Syntax

```
show snmp community
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp community

-------------------------------------------------------------------------------
-------------------------
Community                    Group/Access        view-name
version
-------------------------------------------------------------------------------
-------------------------
test                                  network-operator
testing                     network-operator          ipi
2c
```

Table 21-62 explains the output fields.

Table 21-62: show snmp community fields

Entry	Description
Community	SNMP Community string.
Group/Access	Community group name.
View-name	Community view name.
Version	Community version.

© 2021 IP Infusion Inc. Proprietary

show snmp engine-id

Use this command to display the SNMP engine identifier.

The SNMP engine identifier is a unique string used to identify the device for administration purposes. You do not specify an engine identifier for a device; OcNOS generates a default string. For more about the SNMP engine identifier, see RFC 2571.

Command Syntax

```
show snmp engine-id
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp engine-id
SNMP ENGINE-ID : 80 00 8f 41 03 00 00 00 00 00 00
```

Table 21-63 explains the output fields.

Table 21-63: show snmp engine-ip fields

Entry	Description
SNMP ENGINE-ID : 80 00 8f 41 03 00 00 00 00 00 00	The SNMP engine identifier is a unique string used to identify the device for administration purposes. You do not specify an engine identifier for a device; OcNOS generates a default string.

show snmp group

Use this command to display SNMP server groups and associated views.

Command Syntax

```
show snmp group
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp group
--------------------------------------------------------------------------------
------------------------------
community/user    group         version   Read-View   Write-view   Notify-view
--------------------------------------------------------------------------------
------------------------------

test          network-operator    2c/1      all          all          all
kedar         network-operator    3         all          none         all
tamil         network-operator    3         all          none         all
```

Table 21-64 explains the output fields.

Table 21-64: show snmp group output

Entry	Description
Community/User	Displays the access type of the user for which the notification is generated.
Group	The name of the SNMP group, or collection of users that have a common access policy.
Version	SNMP version number.
Read-View	A string identifying the read view of the group. For further information on the SNMP views, use the show snmp view command.
Write-View	A string identifying the write view of the group.
Notify-View	A string identifying the notify view of the group. The notify view indicates the group for SNMP notifications, and corresponds to the setting of the snmp-server group group-name version notify notify-view command.

© 2021 IP Infusion Inc. Proprietary

show snmp host

Use this command to display the SNMP trap hosts.

Command Syntax

```
show snmp host
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp host
-------------------------------------------------------------------------
Host            Port    Version    Level       Type      SecName
-------------------------------------------------------------------------

10.10.26.123    162     2c         noauth      trap      test
```

Table 21-65 explains the output fields.

Table 21-65: Show snmp host output

Entry	Description
Host	The IP address of the SNMP host server.
Port	The port being used for SNMP traffic.
Version	SNMP version number.
Level	The security level being used.
Type	The type of SNMP object being sent.
SecName	Secure Name for this SNMP session.

show snmp user

Use this command to display SNMP users and associated authentication, encryption, and group.

Command Syntax

```
show snmp user
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp user

SNMP USERS
_____________________________________________________________________
User            Auth    Priv(enforce)     Groups
_____________________________________________________________________
ntwadmin        MD5     AES               network-admin

#
```

Table 21-66 explains the output fields.

Table 21-66: Show snmp user output

Entry	Description
User	The person attempting to use the SMNMP agent.
Auth	The secure encryption scheme being used.
Priv(enforce)	What enforcement privilege is being used (in this case, it is the Advance Encryption Standard).
Group	The group to which the user belongs.

© 2021 IP Infusion Inc. Proprietary

show snmp view

Use this command to display SNMP views.

Command Syntax

```
show snmp view
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp view

View : all
  OID : .1
  View-type : included
```

snmp-server community

Use this command to create an SNMP community string and access privileges.

Use the `no` form of this command to remove an SNMP community string.

Command Syntax

```
snmp-server community WORD (| (view VIEW-NAME version (v1 | v2c ) ( ro )) | (group
  WORD) |( ro ) | (use-acl WORD) ) (vrf management|)
no snmp-server community COMMUNITY-NAME (vrf management|)
```

Parameters

`WORD`	Name of the community (Maximum 32 alphanumeric characters)
`VIEW-NAME`	Name of the snmp view (Maximum 32 alphanumeric characters)
`v1`	SNMP v1
`v2c`	SNMP v2c
`ro`	Read-only access
`group`	Community group
`WORD`	Community group name; maximum length 32 characters
`ro`	Read-only access
`use-acl`	Access control list (ACL) to filter SNMP requests
`WORD`	ACL name; maximum length 32 characters
`management`	Virtual Routing and Forwarding name

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server community MyComm view MyView1 version v2c ro vrf management
```


© 2021 IP Infusion Inc. Proprietary

snmp-server contact

Use this command to set the system contact information for the device (`sysContact` object).

Use the `no` form of this command to remove the system contact information.

Command Syntax

```
snmp-server contact (vrf management|) (TEXT|)
no snmp-server contact (vrf management|) (TEXT|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`TEXT`	System contact information; maximum length 1024 characters without spaces

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server contact vrf management Irving@555-0150
```

snmp-server enable snmp

Use this command to start the SNMP agent daemon over UDP.

Use the `no` form of this command to stop the SNMP agent daemon over UDP.

Command Syntax

```
snmp-server enable snmp  (vrf management|)
no snmp-server enable snmp  (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server enable snmp vrf management
```


© 2021 IP Infusion Inc. Proprietary

snmp-server enable traps

Use this command to enable SNMP traps and inform requests.

Use no form of this command to disable SNMP traps and inform requests.

Command Syntax

```
snmp-server enable traps (link(|linkDown|linkUp)|snmp authentication|
  mpls|pw|pwdelete|rsvp|ospf|bgp|isis)
no snmp-server enable traps (link(|linkDown|linkUp)|snmp
  authentication|mpls|pw|pwdelete|rsvp|ospf|bgp|isis)
```

Parameters

`link`	Module notifications enable
`linkDown`	IETF link state down notification
`linkUp`	IETF link state up notification
`snmp`	Enable RFC 1157 notifications
`authentication`	Send SNMP authentication failure notifications
`mpls`	Enable notification trap for MPLS
`pw`	Enable notification trap for pseudowire
`pwdelete`	Enable notification trap for pseudowire delete
`rsvp`	Enable notification trap for RSVP
`ospf`	Enable notification trap for OSPF
`bgp`	Enable notification trap for BGP
`isis`	Enable notification trap for ISIS

Default

By default, SNMP server traps are enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.6 and changed in OcNOS DC Version 5.0.

Examples

```
(config)#snmp-server enable traps snmp authentication
(config)#sh running-config snmp
snmp-server view all .1 included vrf management
snmp-server enable snmp vrf management
snmp-server enable traps snmp authentication
```

snmp-server host

Use this command to configure an SNMP trap host. An SNMP trap host is usually a network management station (NMS) or an SNMP manager.

Use the `no` form of this command to remove an SNMP trap host.

Note: The maximum number of SNMP trap hosts is limited to 8.

Command Syntax

```
snmp-server host (A.B.C.D | X:X::X:X | HOSTNAME) ((traps version(( (1 | 2c) WORD )
  | (3 (noauth | auth | priv) WORD))) |(informs version ((2c WORD ) | (3 (noauth |
  auth | priv) WORD))))(|udp-port <1-65535>) (vrf management|)
snmp-server host (A.B.C.D | X:X::X:X | HOSTNAME) WORD (|udp-port <1-65535>) (vrf
  management|)
snmp-server host (A.B.C.D | X:X::X:X | HOSTNAME) (version(( (1 | 2c) WORD ) | (3
  (noauth | auth | priv) WORD)))(|udp-port <1-65535>) (vrf management|)
```

Parameters

`A.B.C.D`		IPv4 address
`X:X::X:X`		IPv6 address
`HOSTNAME`		DNS host name
`WORD`		SNMP community string or SNMPv3 user name (Maximum 32 alphanumeric characters)
`informs`		Send notifications as informs
`version`		SNMP Version. Default notification is traps
`<1-65535>`		Host UDP port number; the default is 162
`management`		Virtual Routing and Forwarding name
`traps`		Send notifications as traps
`version`		Version
	`1`	SNMP v1
	`2c`	SNMP v2c
		`WORD` SNMP community string (Maximum 32 alphanumeric characters)
	`3`	SNMP v3 security level
		`noauth` No authentication and no privacy (noAuthNoPriv) security model: messages transmitted as clear text providing backwards compatibility with earlier versions of SNMP
		`auth` Authentication and no privacy (authNoPriv) security model: use message digest algorithm 5 (MD5) or Secure Hash Algorithm (SHA) for packet authentication; messages transmitted in clear text
		`priv` Authentication and privacy (authPriv) security model: use authNoPriv packet authentication with Data Encryption Standard (DES) Advanced Encryption Standard (AES) for packet encryption
		`WORD` SNMPv3 user name

© 2021 IP Infusion Inc. Proprietary

Default

The default SNMP version is v2c and the default UDP port is 162.Simple Network Management Protocol.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server host 10.10.10.10 traps version 3 auth MyUser udp-port 512
vrf management
```

snmp-server location

Use this command to set the physical location information of the device (`sysLocation` object).

Use the `no` form of this command to remove the system location information.

Command Syntax

```
snmp-server location (vrf management|) (LINE|)
no snmp-server location (vrf management|) (LINE|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`LINE`	Physical location information; maximum length 1024 characters

Default

No system location string is set.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server location vrf management Bldg. 5, 3rd floor, northeast
```


© 2021 IP Infusion Inc. Proprietary

snmp-server tcp-session

Use this command to start the SNMP agent daemon over TCP.

Use the `no` form of this command to close the SNMP agent daemon over TCP.

Command Syntax

```
snmp-server tcp-session (vrf management|)
no snmp-server tcp-session (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

By default, snmp server tcp session is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server tcp-session vrf management
```

snmp-server user

Use this command to create an SNMP server user.

Use the `no` form of this command to remove an SNMP server user.

Command Syntax

```
snmp-server user WORD (|WORD) ((auth (md5 | sha ) AUTH-PASSWORD) ((priv (des | aes)
  PRIV-PASSWORD) |) |) (vrf management|)
no snmp-server user USER-NAME (vrf management|)
```

Parameters

`WORD`	Specify the snmp user name (Min 5 to Max 32 alphanumeric characters)
`WORD`	Name of the group to which the user belongs; maximum length 35 characters
`auth`	Packet authentication type
`md5`	Message Digest Algorithm 5 (MD5)
`sha`	Secure Hash Algorithm (SHA)
`AUTH-PASSWORD`	Authentication password; length 8-32 characters
`priv`	Packet encryption type (“privacy”)
`des`	Data Encryption Standard (DES)
`aes`	Advanced Encryption Standard (AES)
`PRIV-PASSWORD`	Encryption password; length 8-33 characters
`management`	Virtual Routing and Forwarding name

Default

By default, snmp server user word is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp-server user Fred auth md5 J@u-b;l2e`n,9p_ priv des t41VVb99i8He{Jt
vrf management
```


© 2021 IP Infusion Inc. Proprietary

snmp-server view

Use this command to create or update a view entry

Use the `no` from of this command to remove a view entry.

Command Syntax

```
snmp-server view VIEW-NAME OID-TREE (included | excluded) (vrf management|)
no snmp-server view VIEW-NAME (vrf management|)
```

Parameters

`VIEW-NAME`	Name of the snmp view (Maximum 32 alphanumeric characters)
`OID-TREE`	Object identifier of a subtree to include or exclude from the view; specify a text string consisting of numbers and periods, such as 1.3.6.2.4
`included`	Include `OID-TREE` in the SNMP view
`excluded`	Exclude `OID-TREE` from the SNMP view
`management`	Virtual Routing and Forwarding name

Default

By default, snmp-server view VIEW-NAME OID-TREE `is` disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example creates a view named `myView3` that excludes the `snmpCommunityMIB` object (1.3.6.1.6.3.18).

```
#configure terminal
(config)#snmp-server view myView3 1.3.6.1.6.3.18 excluded vrf management
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 22 Software Monitoring and Reporting

This document describes software watchdog and reporting related commands.

- copy techsupport
- feature software-watchdog
- show bootup-parameters
- show cores
- show software-watchdog status
- show system log
- show system login
- show system reboot-history
- show system resources
- show system uptime
- show techsupport
- show techsupport status
- software-watchdog
- software-watchdog keep-alive-time

copy techsupport

Use this command to copy the contents of a compressed techsupport file (`tar.gz`) to another file.

The default filename is in the form: `tech_support_YYYY_MMM_DD_HH_MM_SS.tar.gz`.

Syntax

```
copy (log|techsupport) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL)
  (vrf (NAME|management)|)
```

Parameters

`log`	Log file storage; on Linux this refers to `/var/log/`
`techsupport`	Tech support file storage; on Linux this refers to `/var/log/`
`FILE`	Source file name
`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Default

NA

Command Mode

Privileged EXEC

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#copy techsupport tech_support_23_Feb_2019_18_27_00.tar.gz scp scp://10.12.16.17/home/
tech_support_23_Feb_2019_18_27_00.tar.gz vrf management

Enter Username:root
Enter Password:
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 72368 0 0 0 72368 0 147k -::- -::- -::- 147k
100 72368 0 0 0 72368 0 147k -::- -::- -::- 147k
Copy Success
#
```


© 2021 IP Infusion Inc. Proprietary

feature software-watchdog

Use this command to enable software watchdog functionality for all OcNOS modules. This feature is enabled by default.

Use the `no` form of this command to disable software watchdog functionality.

Command Syntax

```
feature software-watchdog
```

```
no feature software-watchdog
```

Parameter

None

Default

By default, software watchdog is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
#(config)feature software-watchdog
```

show bootup-parameters

Use this command to show OcNOS kernel bootup parameters.

Command Syntax

```
show bootup-parameters
```

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bootup-parameters
BOOT_IMAGE=/boot/vmlinuz-3.16.7-g490411a-ec-as7712-32x root=UUID=317567fc-
b69e-4

5d9-ab4e-fa1d9e57b

703 console=ttyS1,115200n8 ro
```


© 2021 IP Infusion Inc. Proprietary

show cores

Use this command to list core files in the system or to display information about a given core file.

Command Syntax

```
show cores (|WORD details)
```

Parameter

WORD	Core file name

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh cores
Core location :/var/log/crash/cores
Core-File-Name
--------------
core_nsm.683_20191110_103611_signal_5.gz
core_nsm.712_20191107_171803_signal_11.gz
core_nsm.684_20191112_054937_signal_5.gz
core_yangcli.5695_20191107_171715_signal_11.gz
#
```

Table 22-67 explains the output fields.

Table 22-67: show cores fields

Entry	Description
Core-File-Name	Core dump file name.

show software-watchdog status

Use this command to display the software watchdog status for each OcNOS module.

Command Syntax

```
show software-watchdog status
show software-watchdog status detail
```

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.4.

Examples

```
#show software-watchdog status
Software Watchdog timeout in seconds : 60
Process name         Watchdog status
============         ===============
nsm                  Enabled
ripd                 Enabled
ripngd               Enabled
ospfd                Enabled
ospf6d               Enabled
isisd                Enabled
hostpd               Enabled
ldpd                 Enabled
rsvpd                Enabled
mribd                Enabled
pimd                 Enabled
authd                Enabled
mstpd                Enabled
imi                  Enabled
onmd                 Enabled
HSL                  Enabled
oamd                 Enabled
vlogd                Enabled
vrrpd                Enabled
ndd                  Enabled
ribd                 Enabled
bgpd                 Enabled
l2mribd              Enabled
lagd                 Enabled
sflow                Enabled
```


© 2021 IP Infusion Inc. Proprietary

```
cmld                  Enabled
cmmd                  Enabled

#show software-watchdog status detail
Software Watchdog timeout in seconds : 60

Process Watchdog   Process   Disconnect Connect         Last Restart
 Name    Status     Status     Count     Count             Reason
======= ======== =========== ========== ======= ==============================
nsm     Enabled  Running     0          1       Fresh bootup
ripd    Enabled  Running     0          1       Fresh bootup
ripngd  Enabled  Running     0          1       Fresh bootup
ospfd   Enabled  Running     0          1       Fresh bootup
ospf6d  Enabled  Running     0          1       Fresh bootup
isisd   Enabled  Running     0          1       Fresh bootup
hostpd  Enabled  Running     0          1       Fresh bootup
ldpd    Enabled  Running     0          1       Fresh bootup
rsvpd   Enabled  Running     0          1       Fresh bootup
mribd   Enabled  Running     0          1       Fresh bootup
pimd    Enabled  Running     0          1       Fresh bootup
authd   Enabled  Running     0          1       Fresh bootup
mstpd   Enabled  Running     0          1       Fresh bootup
imi     Enabled  Running     0          1       Fresh bootup
onmd    Enabled  Running     0          1       Fresh bootup
HSL     Enabled  Running     0          1       Fresh bootup
oamd    Enabled  Running     0          1       Fresh bootup
vlogd   Enabled  Running     0          1       Fresh bootup
vrrpd   Enabled  Running     0          1       Fresh bootup
ndd     Enabled  Running     0          1       Fresh bootup
ribd    Enabled  Running     0          1       Fresh bootup
bgpd    Enabled  Running     0          1       Fresh bootup
l2mribd Enabled  Running     0          1       Fresh bootup
lagd    Enabled  Running     0          1       Fresh bootup
sflow   Enabled  Running     0          1       Fresh bootup
cmld    Enabled  Running     0          1       Fresh bootup
cmmd    Enabled  Running     0          1       Fresh bootup
```

Table 22-68 explains the output fields.

Table 22-68: show software-watchdog status output fields

Field	Description
Process Name	The name of a protocol module.
Watchdog Status	Status of a protocol module (Enabled or Disabled).
Process Status	Status of the protocol module Running/Not-running).
Disconnect Count	Number of times the protocol module disconnected from monitoring module.

Table 22-68: show software-watchdog status output fields (Continued)

Field	Description
Connect Count	Number of times the protocol module connected to monitoring module.
Last Restart Reason	Reason why a module disconnected from monitoring module.

© 2021 IP Infusion Inc. Proprietary

show system log

Use this command to display the system's log file.

Command Syntax

```
show system log
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show system log
Syslog              : enabled      File Name   : /var/log/messages
Oct 18 18:10:18 localhost rsyslogd: [origin software="rsyslogd"
swVersion="8.4.2
" x-pid="541" x-info="http://www.rsyslog.com"] start
Oct 18 18:10:18 localhost systemd[1]: Started Apply Kernel Variables.
Oct 18 18:10:18 localhost systemd[1]: Started Create Static Device Nodes in /
dev
.
Oct 18 18:10:18 localhost systemd[1]: Starting udev Kernel Device Manager...
Oct 18 18:10:18 localhost systemd[1]: Started udev Kernel Device Manager.
Oct 18 18:10:18 localhost systemd[1]: Starting Copy rules generated while the
ro
ot was ro...
Oct 18 18:10:18 localhost systemd[1]: Starting LSB: Set preliminary keymap...
Oct 18 18:10:18 localhost systemd[1]: Started Copy rules generated while the
roo
t was ro.
Oct 18 18:10:18 localhost nfs-common[163]: Starting NFS common utilities:.
Oct 18 18:10:18 localhost systemd[1]: Found device /dev/ttyS0.
Oct 18 18:10:18 localhost systemd[1]: Found device 16GB_SATA_Flash_Drive
OcNOS-CONFIG.
Oct 18 18:10:18 localhost systemd[1]: Starting File System Check on /dev/disk/
by
-label/OcNOS-CONFIG...
Oct 18 18:10:18 localhost systemd[1]: Starting system-ifup.slice.
Oct 18 18:10:18 localhost systemd-fsck[217]: OcNOS-CONFIG: clean, 85/128016
file
s, 27057/512000 blocks
Oct 18 18:10:18 localhost systemd[1]: Created slice system-ifup.slice.
--More--
```

Table 22-69 explains the output fields.

Table 22-69: show system log fields

Entry	Description
Syslog	Status of the protocol (enabled or disabled).
File Name	Specifies the name of the system log files that you configured.

© 2021 IP Infusion Inc. Proprietary

show system login

Use this command to display the system's login history.

Command Syntax

```
show system login
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show system login
eric      ttyS0                        Wed Oct 19 18:31   still logged in
takayuki  ttyS0                        Wed Oct 19 18:14 - 18:25  (00:10)
girish    ttyS0                        Wed Oct 19 16:46 - 17:01  (00:14)

wtmp begins Wed Oct 19 16:46:18 2016
```

show system reboot-history

Use this command to show the OcNOS reboot history.

Command Syntax

```
show system reboot-history
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show system reboot-history
#) On Thu Jun 6 06:16:03 2013
Reason: Reset Requested by Active User
Service: NONE
#) On Thu Jun 6 06:21:30 2015
Reason: Reset Requested due to Process Crash
Service: nsm
#
```

Table 22-69 explains the output fields.

Table 22-70: show system reboot-history fields

Entry	Description
Reason	Displays the reason, why the fields are reset.
Service	Name of the service in this protocol.

© 2021 IP Infusion Inc. Proprietary

show system resources

Use this command to display the system's current resources.

Command Syntax

```
show system resources (iteration <1-5>|)
```

Parameters

<1-5>	The number of times to check the resources before they are displayed.

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
DELL-6K3#show system resources
load average: 0.11, 0.08, 0.05
Tasks: 113 total,   1 running, 112 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.1 us,  0.4 sy,  0.0 ni, 98.5 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0
st
KiB Mem:   8181040 total,   736124 used,  7444916 free,   133012 buffers


#show system resources iteration 5
load average: 0.03, 0.06, 0.05
Tasks: 112 total,   3 running, 109 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.0 us,  0.6 sy,  0.0 ni, 98.4 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0
st
KiB Mem:   8181040 total,   736608 used,  7444432 free,   132976 buffers
KiB Swap:        0 total,        0 used,        0 free.   252416 cached Mem
```

Table 22-71 explains the output fields.

Table 22-71: show system resource fields

Entry	Description
Load Average	Number of processes that are running. The average reflects the system load the past 1, 5, and 15 minutes.
Tasks	Number of processes in the system and how many processes are actually running when the command is issued.
CPU	Displays the CPU utilization information for processes on the device.

Table 22-71: show system resource fields

Entry	Description
KiB Mem	The memory field (Mem) shows the virtual memory used by processes. The value in the memory field is in KB and MB, and is broken down as follows: Total: The total amount of available virtual memory, in kibibytes (KiBs). Used:The total amount of used virtual memory, in kibibytes (KiBs). Free: The total amount of free virtual memory, in kibibytes (KiBs) Buffers: The size of the memory buffer used to hold data recently called from disk.
KiB Swap	The Swap field shows the total swap space available and how much is unused and is broken down as follows: Total: The total amount of available swap memory, in kibibytes (KiBs). Used: The total amount of used swap memory, in kibibytes (KiBs). Free: The total amount of free swap memory, in kibibytes (KiBs). Cache Memory: Memory that is not associated with any program and does not need to be swapped before being reused.

© 2021 IP Infusion Inc. Proprietary

show system uptime

Use this command to display how lone the system has been up and running.

Command Syntax

```
show system uptime
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
DELL-6K3#show system uptime
 19:10:22 up 1 day,  1:01,  1 user,  load average: 0.08, 0.05, 0.05
```

Table 22-72 explains the output fields.

Table 22-72: show system uptime fields

Entry	Description
Time and up	Current time, in the local time zone, and how long the router or switch has been operational.
Users	Number of users logged in to the router or switch.
Load Average	Number of processes that are running. The average reflects the system load the past 1, 5, and 15 minutes.

show techsupport

Use this command to collect system data for technical support to save support information in a compressed (.gz) file.

The default file path is `/var/log/` and the filename is `tech_support_YYYY_MMM_DD_HH_MM_SS.tar.gz`.

The filename given can be the same as another file; to distinguish them, each of the filenames are appended with a date and timestamp.

If a `show techsupport` command execution is in progress, any newly issued `show techsupport` commands are ignored.

If a `show techsupport` command is executing, and the `show running-config` command is given, the displayed information is copied from the `show techsupport` command.

Command Syntax

```
show techsupport
  ({all|authd|bgp|cmmd|hostpd|hsl|imi|isis|l2mribd|lag|ldp|mribd|mstp|nd|nsm|oam|o
  nm|ospf|ospf6|pcep|pim|ptp|rib|rip|ripng|rsvp|sflow|synce|vrrp})
```

Parameters:

`all`	ALL Related Information
`authd`	AUTHD Related Information
`bgp`	BGP Related Information
`cmmd`	CMMD Related Information
`hostpd`	HOSTP Related Information
`hsl`	HSL Related Information
`imi`	IMI Related Information
`isis`	ISIS Related Information
`l2mribd`	L2MRIB Related Information
`lag`	LAG/LACP Related Information
`ldp`	LDP Related Information
`mribd`	MRIB Related Information
`mstp`	MSTP Related Information
`nd`	NDD Related Information
`nsm`	NSM Related Information
`oam`	BFD Related Information
`onm`	ONM/LLDP Related Information
`ospf`	OSPF Related Information
`ospf6`	OSPF6 Related Information
`pcep`	PCEP Related Information
`pim`	PIM Related Information
`ptp`	PTP Related Information
`rib`	RIB Related Information

© 2021 IP Infusion Inc. Proprietary

`rip`	RIP Related Information
`ripng`	RIPNG Related Information
`rsvp`	RSVP Related Information
`sflow`	SFLOW Related Information
`synce`	SYNCE Related Information
`vrrp`	VRRP Related Information

Default

The default file path for show techsupport is /var/log/.

Command Mode

Privileged EXEC

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show techsupport all
#show techsupport bgp
#show techsupport bgp isis
```

show techsupport status

Use this cli to view the status of `show techsupport` CLI to generate techsupport archive.

Command Syntax

```
show techsupport status
```

Parameters

None

Command Mode

Privileged EXEC

Applicability

This command was introduced before OcNOS-SP version 4.2.

Example

```
#show techsupport status
 Tech Support Command Execution Is Complete
 ##Generated Tech Support File-list
 /var/log/OcNOS_tech_support_18_Jun_2021_10_01_38.tar.gz
 Tar File is generated at /var/log and file name begins with
'OcNOS_tech_support'
```


© 2021 IP Infusion Inc. Proprietary

software-watchdog

Use this command to enable the software watchdog feature for an OcNOS module.

Use the `no` form of this command to disable the software watchdog feature.

Command Syntax

```
software-watchdog (nsm|authd|bgpd|cmld|hostpd|imi|isisd|lagd|l2mribd|
  mstpd|mribd|ndd|oamd|onmd|ospfd|ospf6d|pimd|ribd|ripd|ripngd|sflow|vlogd|vrrpd||
  ldpd|rsvpd||hsl|cmmd)
no software-watchdog (nsm|authd|bgpd|cmld|hostpd|imi|isisd|lagd|l2mribd|
  mstpd|mribd|ndd|oamd|onmd|ospfd|ospf6d|pimd|ribd|ripd|ripngd|sflow|vlogd|vrrpd||
  ldpd|rsvpd||hsl|cmmd)
```

Parameters

`nsm`	NSM module
`authd`	AUTH module
`bgpd`	BGP module
`cmld`	CML module
`hostpd`	HOSTP module
`imi`	IMI module
`isisd`	ISIS module
`lagd`	LAG module
`l2mribd`	L2MRIB module
`mstpd`	MSTP module
`mribd`	MRIB module
`ndd`	NDD module
`oamd`	OAM module
`onmd`	ONM module
`ospfd`	OSPF module
`ospf6d`	OSPF6 module
`pimd`	PIM module
`ribd`	RIB module
`ripd`	RIP module
`ripngd`	RIPNG module
`sflow`	SFLOW module
`vlogd`	VLOG module
`vrrpd`	VRRP module
`ldpd`	LDP module
`rsvpd`	RSVP module
`hsl`	HSL module

`cmmd`	CMM module

Default

By default, software watchdog is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
#(config)no software-watchdog imi
#(config)software-watchdog nsm
```


© 2021 IP Infusion Inc. Proprietary

software-watchdog keep-alive-time

Use this command to set the software watchdog keep-alive time interval in seconds. The default keep-alive time interval is 60 seconds.

Use the `no` form of this command to set default keep-alive time interval.

Command Syntax

```
software-watchdog keep-alive-time <30-1800>
no software-watchdog keep-alive-time
```

Parameters

`<30-1800>`	Keep-alive time interval in seconds

Default

By default, software watchdog is enabled and the keep-alive time interval is 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
#(config)software-watchdog keep-alive-time 100
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 23 Syslog

This chapter is a reference for the `syslog` commands.

Linux applications use the `syslog` utility to collect, identify, time-stamp, filter, store, alert, and forward logging data. The `syslog` utility can track and log all manner of system messages from informational to extremely critical. Each system message sent to a `syslog` server has two descriptive labels associated with it:

- The function (facility) of the application that generated it. For example, an application such as `mail` and `cron` generates messages with a facility names “mail” and “cron”.
- Eight degrees of severity (numbered 0-7) of the message which are explained in Table 23-73.

This chapter contains these commands:

- clear logging logfile
- feature rsyslog
- debug logging
- log syslog
- logging console
- logging level
- logging logfile
- logging monitor
- logging remote facility
- logging remote server
- logging timestamp
- show logging
- show logging last
- show logging logfile
- show logging logfile last-index
- show logging logfile start-seqn end-seqn
- show logging logfile start-time end-time
- show running-config logging

Syslog Severities

In the example log entries in Table 23-73, the prefixes are removed. For example. this is a complete log entry with the prefix:

```
2020 Apr 12 11:20:27.612 : 17U-18U : PSERV : MERG : !!! hsl Module crashed, System reboot halted as it rebooted continuosly 2 times
```

This is the same log entry without the prefix:

```
hsl Module crashed,System reboot halted as it rebooted continuosly 2 times
```

Table 23-73: Syslog severities (Sheet 1 of 2)

Severity Level	Keyword	Description

0	emergency	The whole system is unusable and needs operator intervention to recover. If only a particular port or component is unusable, but the system as a whole is still usable it is not categorized at an emergency level.
		Examples of this type of message:
		`Output Power of PSU XX (psu_no) XX Watt] has exceeded Maximum Output Power Limit[XX Watt]`
		`OSPF Initialization failed.`

1	alert	The operator needs to act immediately or the system might go into emergency state. The system or one of its component's functionality might be critically affected.
		Examples of this type of message:
		`Temperature of sensor is (curr_temp)C. It is nearing Emergency Condition.`
		`OSPF has exceed lsdb limit`
		`OSPF Detected router with duplicate router ID [ID]`

2	critical	A critical system event happened which requires the operator's attention. The event might not require immediate action, but this event can affect functionality or behavior of a system component.
		Examples of this type of message:
		`OSPF Neighbor session went down.`
		`Interface %s changed state to down`

3	error	An error event happened which does not require immediate attention. This log message provides details about error conditions in the system or its components which you can use to troubleshoot problems.
		These events are not logged directly even if the logging level is set to include this level. You also need to enable the protocol debug filters (such as `debug ospf all`).
		Examples of this type of message:
		`Device i2c bus open error.!!!`
		`[DECODE] Attr ASPATH: Invalid AS Path value.`
		`OSPF MD5 authentication error`

© 2021 IP Infusion Inc. Proprietary

Table 23-73: Syslog severities (Sheet 2 of 2)

Severity Level	Keyword	Description

4	notification	Notifications about important system and protocol events to assure the operator that the system is running properly. If a critical/alert condition has happened and has been corrected, that is also logged at this level.
		Examples of this type of message:
		`OSPF Received link up for interface: xe1`
		`OSPF neighbour [10.1.1.1] Status change Exstart -> Exchange`
		`Interface %s changed state to UP`

5	informational	Detailed informational events happening across the system and protocol modules. These events are not necessarily important and are useful only to find details about the functionality being executed in the system and its components. Some of these events might be periodic events like hello or keep alive messages along with packet dumps. Also, this level includes logs for control packets that are ignored and do not impact the protocol states.
		IP Infusion Inc. recommends to use proper debug filters to log only relevant events and switch off other events; otherwise the logs can get verbose. For example:
		`debug ospf all`
		`no debug ospf packet hello`
		The above enables all OSPF debugging, but disables the periodic hello messages.
		Examples of this type of message:
		`Successfully added dynamic neighbour`
		`[DECODE] KAlive: Received!`
		`[FSM] Ignoring Unsupported event <EVENT> in state <STATE>`
		`Unknown ICMP packet type"`
		`OSPF RECV[%s]: From %r via %s: Version number mismatch`
		`OSPF RECV[%s]: From %r via %s: Network address mismatch`

6	debug informational	Developer notification events that might not be readable by an operator. However these logs are useful for debugging by a developer and if required, this level needs to be enabled and provided to technical support for analysis.
7	debug detailed	Developer notification events that might not be readable by an operator. However these logs are useful for debugging by a developer and if required, this level needs to be enabled and provided to technical support for analysis.

Log File Rotation

Log rotation is important to maintain the stability of the device, because the larger log files are difficult to manipulate and file system would run out of space. The solution to this common problem is log file rotation.

Log rotation is scheduled to happen for every 5 minutes, here the log file size is used as the condition to perform rotation.

Log rotate operation creates a backup of the current log file, and clears the current log file content. Also these rotated log files are compressed to save disk space. Excluding the current log file, four backup files are maintained in the system, and the older logs are removed as part of the rotation operation.

Default log file `/var/log/messages` rotated, if the size is greater than 100 MB. The following are the rotated log files generated in the path `/var/log`

```
root@host:/var/log# ls messages*
messages  messages.1  messages.2.gz  messages.3.gz  messages.4.gz
```

Manually configured log file `/log/LOG1` gets rotated, if its size is greater than configured size. Here `LOG1` is the manually configured using the command `logging logfile <filename>` and the log file size in bytes can be configured using the command `logging logfile LOG1 <severity> size <4096-419430400>`

```
(config)#logging logfile LOG1 7 size 4096
```

Here configured logging file `/log/LOG1` is rotated if the size is greater than 4096 bytes. The following are the rotated log files generated in the path `/log`

```
root@host:/log# ls LOG*
LOG1  LOG1.1  LOG1.2.gz  LOG1.3.gz  LOG1.4.gz
```


© 2021 IP Infusion Inc. Proprietary

clear logging logfile

Use this command to clear the existing contents of the configured logging logfile.

Note: If the name of the configured logging log file is “mylogfile”, this command clears only the log file mylogfile. But the other rotated or compressed log files are untouched.

Command Syntax

```
clear logging logfile
```

Parameters

None

Default

No default value is specified

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS-SP version 3.0.

Example

```
#clear logging logfile
```

feature rsyslog

Use this command to enable the rsyslog server.

Use the `no` form of this command to disable the rsyslog server.

Command Syntax

```
feature rsyslog vrf (management|)
no feauture rsyslog vrf (management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#feature rsyslog vrf management
```


© 2021 IP Infusion Inc. Proprietary

debug logging

Use this command to display logging debugging information.

Use the `no` form of this command stop displaying logging debugging information.

Command Syntax

```
debug logging host
no debug logging host
```

Parameters

None

Command Mode

Exec and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug logging host
```

log syslog

Use this command to begin logging to the system log and set the level to debug.

Syslog enables centrally logging and analyzing of configuration events and system error messages. This helps monitor interface status, security alerts, and CPU process overloads. It also allows real-time capturing of client debug sessions. The command instructs the `VLOGD` daemon to forward all PVR debug output from all active `terminal monitor` sessions to the syslog file.

Use the `no` parameter to disable logging to the system log.

Command Syntax

```
log syslog
no log syslog
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
```


© 2021 IP Infusion Inc. Proprietary

logging console

Use this command to set the severity level that a message must reach before the messages is sent to the console. The severity levels are from 0 to 7 as shown in Table 23-73.

Use the `no` form of this command to disable logging console messages.

Note: Below message will be displayed if console severity is set to 6 or 7:

% Warning : If debug volume is huge it can degrade system performance and makes console to be non-responsive

Note: For CMMD, Critical logs in the console are equivalent to Alert traps & Alert logs on the console is equivalent to critical trap in SNMP.

Command Syntax

```
logging console (<0-7>|)
no logging console
```

Parameters

`<0-7>` Maximum logging level for console messages as shown in Table 23-73.

Note: Setting the level above 5 might affect performance and is not recommended in a production network.

Default

If not specified, the default logging level is 2 (Critical).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#logging console 6

(config)#2015 Dec 23 03:13:26 OcNOS BGP-6: [RIB] Scanning BGP Network Route
s...
2015 Dec 23 03:13:41 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:13:56 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:00 OcNOS BGP-6: [RIB] Scanning BGP RIB...
2015 Dec 23 03:14:11 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:26 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:41 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:56 OcNOS BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:15:00 OcNOS BGP-6: [RIB] Scanning BGP RIB...

(config)#no logging console
```

logging level

Use this command to set the severity level that a message for a specific process must reach before the messages is logged. The severity levels are from 0 to 7 as shown in Table 23-73. Logging happens for the messages less than or equal to the configured severity level.

Use the `no` form of this command to disable logging messages.

Note: Default log level is 2 to report Emergency-0, Alert-1 and Critical-2 level events.

Command Syntax

```
logging level (all|auth|bgp|dvmrp|hostp|hsl|isis|l2mrib|lacp|lagd|ldp|mrib|
  mstp|ndd|nsm|onm|oam|ospf|ospf6|pim|pon|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow
  |vrrp) <0-7>
no logging level (all|auth|bgp|dvmrp|hostp|hsl|isis|l2mrib|lacp|lagd|ldp|mrib|
  mstp|ndd|nsm|oam|onm|ospf|ospf6|pim|pon|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow
  |vrrp)
```

Parameters

`all`	All messages
`auth`	Auth messages
`bgp`	BGP messages
`dvmrp`	DVMRP messages
`hostp`	Hostp messages
`hsl`	HSL messages
`isis`	ISIS messages
`l2mrib`	L2MRIB messages
`lacp`	LACP messages
`lagd`	LAGD messages
`ldp`	LDP messages
`mrib`	MRIB messages
`mstp`	MSTP messages
`ndd`	NDD messages
`nsm`	NSM messages
`oam`	OAM messages
`onm`	ONM messages
`ospf`	OSPF messages
`ospf6`	OSPF6 messages
`pim`	PIM messages
`pon`	PON messages
`pservd`	PSERVD messages
`ptp`	PTP messages
`rib`	RIB messages

© 2021 IP Infusion Inc. Proprietary

`rip`	RIP messages
`ripng`	RIPNG messages
`rmon`	RMON messages
`rsvp`	RSVP messages
`sflow`	Sflow messages
`vrrp`	VRRP messages
`<0-7>`	Severity level as shown in Table 23-73.

Default

By default, the logging level is 2 (critical).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#logging level all 5

#configure terminal
(config)#logging level bgp 6

(config)#no logging monitor
```

logging logfile

Use this command to specify the log file controls and where to save the logs in a configuration file. This command enables writing debug output and command history to the disk file in the directory `/log/`.

When logging logfile is enabled, OcNOS log information is stored in user configured logging file which is present in "/log" directory. The log is spread across four files total of these files size is the user configured size.

For example, if the name of the logging log file is “mylogFile” and logging file size configured is 4 MB then each file will be maximum size of 1MB. The logging file names will be "mylogFile", "mylogfile.0", "mylogfile.1" and "mylogfile.2".

"mylogFile" will have the latest log information. As soon as it’s size becomes 1 MB this file is renamed as mylogFile.0 and newlog information is written to new "mylogFile". As a result oldest log information stored in mylogfile.2 and is lost in order to accommodate new set of logs in mylogFile.

Use option no to cancel writing to a specific log file.

Note: Changing logfile paramenters (name/size/severity) will be taken into effect for the next OcNOS session.

Command Syntax

```
logging logfile LOGFILENAME <0-7> ((size <4096-419430400>)|)
no logging logfile
```

Parameter

`LOGFILENAME`	Enter the logfile name (Maximum 200 alphanumeric characters)
`<0-7>`	Severity level as shown in Table 23-73.
`<4096-419430400>`	Log file size in bytes.

Default

By default, log file size is 419430400 bytes.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This command is used to log the debug messages of a particular protocol daemon to the specified file.

```
#configure terminal
(config)#logging logfile test123 7
```


© 2021 IP Infusion Inc. Proprietary

logging monitor

Use this command to set the severity level that a message must reach before a monitor message is logged. The severity levels are shown in Table 23-73.

Use the `no` parameter to disable logging monitor messages.

Command Syntax

```
logging monitor (<0-7>|)
no logging monitor
```

Parameters

`<0-7>`	Maximum logging level for monitor messages as shown in Table 23-73.

Note: Setting the level above 5 might affect performance and is not recommended in a production network.

Default

If not specified, the default logging level is 7 (debug-details).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#logging monitor 6

(config)#no logging monitor
```

logging remote facility

Use this command to set a syslog servers facility.

OcNOS supports logging messages to one or more remote syslog servers. but the same facility is used for all the servers.

Use the `no` form of this command to use the default facility value, which is `local7`.

Note: Only one facility is supported for all protocol modules across all the configured logging servers.

Command Syntax

```
logging remote facility
  (local0|local1|local2|local3|local4|local5|local6|local7|user)
no logging remote facility
```

Parameters

`facility`	Entity logging the message (user defined); if not specified, the default is local7
`local0`	Local0 entity
`local1`	Local1 entity
`local2`	Local2 entity
`local3`	Local3 entity
`local4`	Local4 entity
`local5`	Local5 entity
`local6`	Local6 entity
`local7`	Local7 entity (default)
`user`	User entity

Default

If not specified, the default `facility` is `local7`.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.1.

Examples

```
#configure terminal
(config)#logging remote facility local 6
(config)#no logging remote facility
```


© 2021 IP Infusion Inc. Proprietary

logging remote server

Use this command to set a syslog server.

OcNOS supports logging messages to a syslog server in addition to logging to a file or the console (local or SSH/telnet console). OcNOS messages can be logged to a local syslog server (the machine on which OcNOS executes) as well as to one or more remote syslog servers.

Use the `no` form of this command to remove a syslog server.

Note: Maximum 8 remote log servers can be configured.

Command Syntax

```
logging remote server (A.B.C.D|X:X::X:X|HOSTNAME) ((0|1|2|3|4|5|6|7)|) (vrf
  management|)
no logging remote server (A.B.C.D|X:X::X:X|HOSTNAME) (vrf management|)
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`HOSTNAME`	Host name; specify `localhost` to log locally
`0`	Emergency
`1`	Alert
`2`	Critical
`3`	Error
`4`	Notification
`5`	Informational
`6`	Debug informational
`7`	Debug detailed
`vrf management`	Virtual Routing and Forwarding name

Note: Severity at which messages are logged as shown in Table 23-73. If not specified, the default is 7.

Default

If not specified, the default severity at which messages are logged is 7 (debug detailed).

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.1.

Examples

```
#configure terminal
(config)#logging remote server MyLogHost vrf management
(config)#no feature rsyslog vrf management
(config)# (config)#feature rsyslog
```

```
(config)#logging remote server 10.10.10.10 7
```

Note: In the latter configuration, the default VRF does not need not to be specified in the command.

© 2021 IP Infusion Inc. Proprietary

logging timestamp

Use this command to set the logging timestamp granularity.

Use the `no` form of this command to reset the logging timestamp granularity to its default (milliseconds).

Note: Any change in timestamp configurations will result in timestamp configured for event logged by protocol modules except for CLI history for the current and active sessions. The timestamp configuration is reflected in CLI history for new CLI sessions.

Changing logging timestamp will be taken into effect for the next OcNOS session.

Command Syntax

```
logging timestamp (microseconds|milliseconds|seconds|none)
no logging timestamp
```

Parameters

`microseconds`	Microseconds granularity
`milliseconds`	Milliseconds granularity
`seconds`	Seconds granularity
`none`	no timestamp in log message

Default

By default, logging time stamp granularity is milliseconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#logging timestamp milliseconds
```

© 2021 IP Infusion Inc. Proprietary

show logging

Use this command to display the logging configuration.

Command Syntax

```
show logging (info|level|server|console|timestamp|monitor)
```

Parameters

`info`	Show server logging configuration
`level`	Show facility logging configuration
`server`	Syslog server configuration
`console`	Console configuration
`timestamp`	Timestamp configuration
`monitor`	Monitor configuration

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging console
Console logging     : enabled Severity: Operator (critical) Level : 2


#show logging monitor
Logging monitor     : enabled Severity: Operator (debugging) Level: 7


#show logging server
  Remote Servers:
               1.1.1.1
               severity: Operator (informational)
               facility: local7
               VRF : management

#sh logging info
  Remote Servers:
               1.1.1.1
               severity: Operator (informational)
               facility: local7
               VRF : management
Logging console     : enabled Severity: operator (critical) Level : 2
Logging monitor     : enabled Severity: Operator (debugging) Level : 7
Logging timestamp   : seconds
File logging        : enabled  File Name   : /log/abc  Severity   : Operator (de
```


© 2021 IP Infusion Inc. Proprietary

```
bugging)  Level   : 7  Size   : 4194304
Cli logging         : enabled

Facility        Default Severity        Current Session Severity
nsm                     2                       2
ripd                    2                       2
ripngd                  2                       2
ospfd                   2                       2
ospf6d                  2                       2
isisd                   2                       2
hostpd                  2                       2
mribd                   2                       2
pimd                    2                       2
authd                   2                       2
mstpd                   2                       2
onmd                    2                       2
HSL                     2                       2
oamd                    2                       2
vlogd                   2                       2
vrrpd                   2                       2
ndd                     2                       2
ribd                    2                       2
bgpd                    2                       2
l2mribd                 2                       2
hslrasmgr               2                       2
lagd                    2                       2
pservd                  2                       2
cmmd                    2                       2
```

show logging last

Use this command to display lines from the end of the log file.

Command Syntax

```
show logging last (<1-9999>)
```

Parameters

<1-9999>	Number of lines to display from end of the log file

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging last 100
2016 Mar 03 00:02:32 x86_64-debian NSM-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian OSPF-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian OSPFv3-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian IS-IS-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian BGP-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian RIP-3: AgentX: failed to send open message:
Connection refused
```


© 2021 IP Infusion Inc. Proprietary

show logging logfile

Use this command to display whether logging is enabled, the log file name, and the logging severity.

Command Syntax

```
show logging logfile
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh logging logfile
File logging        : enabled  File Name   : /log/abc  Severity   : (7)
2017 Sep 25 17:18:14 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
logging remote server 1.1.1.1 5 vrf management '

2017 Sep 25 17:18:14 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
ex'

2017 Sep 25 17:18:17 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging info '

2017 Sep 25 17:19:15 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging console '

2017 Sep 25 17:19:20 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging monitor '

2017 Sep 25 17:19:32 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging logfile '

2017 Sep 25 17:19:44 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging server '

2017 Sep 25 17:28:26 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging info '

2017 Sep 25 17:29:02 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging console
```

show logging logfile last-index

Use this command to display the number of line in the log file.

Command Syntax

```
show logging logfile last-index
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging logfile last-index
logfile last-index : 10
```

Table 23-74 explains the output fields.

Table 23-74: show logging logfile last-index fields

Entry	Description
logfile last-index	Number of line in the logfile.

© 2021 IP Infusion Inc. Proprietary

show logging logfile start-seqn end-seqn

Use this command to display a range of lines in the log file.

Command Syntax

```
show logging logfile start-seqn (<0-2147483647>) (|(end-seqn <0-2147483647>))
```

Parameters

start-seqn	Starting line number
end-seqn	Ending line number

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging logfile start-seqn 2 end-seqn 7
2
3 2019 Jan 04 06:20:49.611 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : sh logging logfile
4
5 2019 Jan 04 06:21:08.512 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
6
7 2019 Jan 04 06:21:16.246 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
NE4-router#
```

Table 23-75 explains the output fields.

Table 23-75: show logging logfile start-seqn end-seqn fields

Entry	Description
start-seqn	Starting line number
end-seqn	Ending line number

show logging logfile start-time end-time

Use this command to display lines from the log file within a given date-time range.

Command Syntax

```
show logging logfile start-time (<2000-2030> WORD <1-31> WORD) (|(end-time <2000-
  2030> WORD <1-31> WORD))
```

Parameters

`start-time`	Starting date and time:
`<2000-2030>`	Year in YYYY format
`WORD`	Month as `jan`, `feb`, `mar`,..., `oct`, `nov`, or `dec` (maximum length 3 characters)
`<1-31>`	Day of month in DD format
`WORD`	Hour, minutes, seconds in HH:MM:SS format (maximum length 8 characters); range <0-23>:<0-59>:<0-59>
`end-time`	Ending date and time:
`<2000-2030>`	Year in YYYY format
`WORD`	Month as `jan`, `feb`, `mar`,..., `oct`, `nov`, or `dec` (maximum length 3 characters)
`<1-31>`	Day of month in DD format
`WORD`	Hour, minutes, seconds in HH:MM:SS format (maximum length 8 characters); range <0-23>:<0-59>:<0-59>

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh logging logfile start-time 2019 Jan 04 06:20:49 end-time 2019 Jan 04
06:21:16
2019 Jan 04 06:20:49.611 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : sh logging logfile

2019 Jan 04 06:21:08.512 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index

2019 Jan 04 06:21:16.246 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
#
```


© 2021 IP Infusion Inc. Proprietary

show running-config logging

Use this command to display the logging configuration.

Command Syntax

```
show running-config logging
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config logging
no Logging console
no Logging monitor
logging timestamp milliseconds
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 24 System Configure Mode Commands

This chapter provides a reference for system-level configure mode commands.

- forwarding custom-profile
- forwarding profile
- hardware-profile filter (XGS)
- hardware-profile filter (Qumran)
- hardware-profile flowcontrol (Qumran)
- hardware-profile statistics (Qumran)
- load-balance rtag7
- load-balance rtag7 hash
- load-balance rtag7 macro-flow
- show forwarding profile limit
- show hardware-profile filters
- snmp restart

© 2021 IP Infusion Inc. Proprietary

forwarding custom-profile

Use this command to configure forwarding table sizes.

Note: You must reboot after any profile change, except a change to the default profile. The configuration is applied only after a reboot.

Use `show-running configuration` or show forwarding profile limit to verify the selected profile.

Use the `forwarding custom-profile default` command (with no parameters) to set the forwarding table size to its default.

Command Syntax

Tomahawk platform:

```
forwarding custom-profile {l2-banks <1-4>|l3-banks <1-4>|lpm-banks 2}
```

Helix4 platform:

```
forwarding custom-profile {l2-banks <1-24>|l3-banks <1-23>|vlan-xlate-banks <1-
  23>|ep-vlan-xlate-banks <1-23>}
```

Tomahawk and Helix4 platforms:

```
forwarding custom-profile default
```

Parameters

`l2-banks`	L2 banks. Unspecified banks are used as L2 banks.
`<1-4>`	Number of L2 banks. Each bank size is 32k entries and each entry is 105 bits.
`<1-24>`	Number of L2 banks. Each bank size is 1k entries and each entry is 420 bits.
`l3-banks`	L3 banks. Unspecified banks are used as L2 banks.
`<1-4>`	Number of L3 banks. Each bank size is 32k entries and each entry is 105 bits.
`<1-23>`	Number of L3 banks. Each bank size is 1k entries and each entry is 420 bits.
`lpm-banks`	Longest-prefix match banks. Unspecified banks are used as L2 banks.
`2`	Two LPM banks per entry. The remaining banks can be used by any.
`vlan-xlate-banks`	VLAN translate banks. Unspecified banks are used as L2 banks.
`<1-23>`	Number of VLAN translate banks. Each bank size is 1k entries and each entry is 420 bits.
`ep-vlan-xlate-banks`	Egress VLAN translate banks. Unspecified banks are used as L2 banks.
`<1-23>`	Number of EP VLAN translate banks. Each bank size is 1k entries and each entry is 420 bits.
`default`	Use L2 profile Three; the size of the l2 table (MAC address table) and L3 table (host table) is almost equal.

Default

By default, the forwarding table size is L2 profile three: the sizes of the L2 table (MAC address table) and L3 table (host table) are almost equal.

© 2021 IP Infusion Inc. Proprietary

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

This command only applies to Tomahawk and Helix4 platforms.

Examples

```
#configure terminal
(config)#forwarding custom-profile l3-banks 4
```

forwarding profile

Use this command to configure forwarding table sizes.

Note: You must reboot after any profile change, except a change to the default profile. The configuration is applied only after a reboot.

Note: The use of `k` for “kilo” (as in 1k) does not equal 1,000. In all cases, `k` equals the Boolean value: 1,024.

Use `show-running configuration` or show forwarding profile limit to verify the selected profile.

Use this `no` command to set the forwarding table size to the default.

Command Syntax

```
forwarding profile (l2-profile-one | l2-profile-two | l2-profile-three | l3-profile
  | l3-128bit-profile | lpm-profile | lpm-128bit-profile)
no forwarding profile
```

Parameters

For details about these profiles, see show forwarding profile limit.

`l2-profile-one`	L2 profile One
`l2-profile-two`	L2 profile Two
`l2-profile-three`	L2 profile Three (default); the sizes of the L2 table (MAC address table) and L3 table (host table) are almost equal
`l3-profile`	L3 profile
`l3-128bit-profile`	L3 profile with IPv6 prefix >64 support
`lpm-profile`	Longest-prefix match profile
`lpm-128bit-profile`	LPM profile with IPv6 prefix >64 support

Default

The default forwarding table size is `l2-profile-three`.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#forwarding profile l2-profile-one
```


© 2021 IP Infusion Inc. Proprietary

hardware-profile filter (XGS)

Use this command to enable or disable ingress IPv4 or IPv6 and egress IPv6 filter groups. Disabling filter groups increases the configurable filter entries.

Use the no command to remove explicit enable/disable config for the filter group and switch to default behavior for that filter group.

Command Syntax

```
hardware-profile filter (ingress-ipv4|ingress-ipv6|egress-ipv6|ingress-arp)
  (enable|disable)
no hardware-profile filter (ingress-ipv4|ingress-ipv6|egress-ipv6)
```

Note: 'no' command is provided only for ingress-ipv4, ingress-ipv6 and egress-ipv6. By default, group is enabled. To increase scalability for other groups disable the group.

Parameter

`ingress-ipv4`	IPv4 filter ingress group.
`ingress-ipv6`	IPv6 filter ingress group.
`egress-ipv6`	IPv6 filter egress group.
`enable`	Enable filter group.
`disable`	Disable filter group.
`ingress-arp`	ARP filter ingress group
`no`	Reset the group to as it was during init

Default

By default, all filter groups are enabled except the `ingress-arp` filter group.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

The `no` command is introduced in OcNOS DC version 4.2.

This form of the `hardware-profile filter` command is *not* available on Qumran platforms. See hardware-profile filter (Qumran).

Examples

```
#configure terminal
(config)#hardware-profile filter ingress-ipv4 disable
(config)#hardware-profile filter ingress-ipv4 enable
(config)#no hardware-profile filter ingress-ipv4
```

© 2021 IP Infusion Inc. Proprietary

hardware-profile filter (Qumran)

Use this command to enable or disable ingress and egress filter groups. Disabling filter groups increases the configurable filter entries.

Command Syntax

```
hardware-profile filter (ingress-l2-group|ingress-ipv4|qos-group|egress-
  ipv4|egress-ipv6|egress-l2-group) (enable|disable)
```

Parameter

`ingress-l2-group`
: Layer 2 (MAC) filter ingress group.

`ingress-ipv4`
: IPv4 filter ingress group.

`qos-group`
: QoS filter group.

`egress-ipv4`
: IPv4 filter egress group.

`egress-ipv6`
: IPv6 filter egress group.

`egress-l2-group`
: Layer 2 (MAC) filter egress group.

`enable`
: Enable filter group.

`disable`
: Disable filter group.

Default

By default, all filter groups are enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is only available on Qumran platforms. For other platforms, see hardware-profile filter (XGS).

Examples

```
#configure terminal
(config)#hardware-profile filter ingress-ipv4 disable
(config)#hardware-profile filter ingress-ipv4 enable
```


© 2021 IP Infusion Inc. Proprietary

hardware-profile flowcontrol (Qumran)

Use this command to globally enable or disable hardware-based flow control.

Syntax

```
hardware-profile flowcontrol (disable|enable)
```

Parameters

`disable`	Disable flow control globally
`enable`	Enable flow control globally

Default

By default flow control is disabled on Qumran platforms.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

This command is only available on Qumran platforms.

Examples

```
#configure terminal
(config)#hardware-profile flowcontrol enable
```

hardware-profile statistics (Qumran)

Use this command to enable or disable filter statistics in hardware.

Note: You must reboot the switch after giving this command for the changes to take effect.

Command Syntax

```
hardware-profile statistics (ingress-acl|mpls-ac|mpls-lsp|mpls-pwe)
  (enable|disable)
```

Parameter

`ingress-acl`	Ingress ACL statistics.
`mpls-ac`	Attachment circuit statistics.
`mpls-lsp`	LSP statistics.
`mpls-pwe`	Pseudowire logical interfaces statistics.
`enable`	Enable statistics.
`disable`	Disable statistics.

Default

By default, filter statistics are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is only available on Qumran platforms.

Examples

```
#configure terminal
(config)#hardware-profile statistics mpls-lsp enable
```


© 2021 IP Infusion Inc. Proprietary

load-balance rtag7

Use this command to configure rtag7 load balancing.

Use the `no` option to disable the rtag7 load balancing.

Command Syntax

This form enables or disables rtag7 load balancing globally:

```
load-balance rtag7
no load-balance rtag7
```

By default, load balancing is enabled for ECMP, and LAG.

This form sets rtag7 hashing for ECMP and L3 LAG based on IPv4 fields:

```
load-balance rtag7 (ipv4 {src-ipv4|dest-ipv4|srcl4-port|destl4-port|protocol-id})
no load-balance rtag7 (ipv4 {src-ipv4|dest-ipv4|srcl4-port|destl4-port|protocol-
  id})
```

By default, IPv4 ECMP is configured with the fields `src-ipv4`, `dest-ipv4`, `srcl4-port`, and `dest-l4port`.

By default, L3 LAG is configured with the fields `src-ipv4` and `dest-ipv4`.

This form sets rtag7 hashing for ECMP based on IPv6 fields:

```
load-balance rtag7 (ipv6 {src-ipv6|dest-ipv6|srcl4-port|destl4-port|next-hdr})
no load-balance rtag7 (ipv6 {src-ipv6|dest-ipv6|srcl4-port|destl4-port|next-hdr})
```

By default, IPv6 ECMP is configured with the fields `src-ipv6`, `dest-ipv6`, `srcl4-port`, and `dest-l4port`.

This form sets rtag7 hashing for L2 LAG based on L2 fields:

```
load-balance rtag7 (l2 {dest-mac|src-mac|ether-type|vlan})
no load-balance rtag7 (l2 {dest-mac|src-mac|ether-type|vlan})
```

By default, L2 LAG is configured with the fields `src-mac` and `dest-mac`.

This form sets rtag7 hashing on an MPLS egress LER node based on L2/L3 fields:

```
load-balance rtag7 (mpls-ler ((inner-l2 ({dest-mac|src-mac|ether-type|vlan})) |
  (inner-l3 ({src-ip|dest-ip|srcl4-port|destl4-port|protocol-id}))))
no load-balance rtag7 (mpls-ler ((inner-l2 ({dest-mac|src-mac|ether-type|vlan})) |
  (inner-l3 ({src-ip|dest-ip|srcl4-port|destl4-port|protocol-id}))))
```

Please note the following:

- For ingress LER nodes, hashing is done on L2 fields, L3 fields (outer IPx), or inner IP fields (only for IPx-over-IPx or IPx-over-GRE-IPx).
- For egress LER nodes, hashing is done based on only L2 and L3 fields immediately after the MPLS header which is popped. Any other fields are not supported.

This form sets rtag7 hashing based on the outer IP address:

```
load-balance rtag7 (tunnel outer-l3-header)
no load-balance rtag7 (tunnel outer-l3-header)
```

Parameters

`ipv4`	Load balance IPv4 packets
`src-ipv4`	Source IPv4 based load balancing
`dest-ipv4`	Destination IPv4 based load balancing
`srcl4-port`	Source L4 port based load balancing
`destl4-port`	Destination L4 port based load balancing
`protocol-id`	Protocol ID based load balancing
`ipv6`	Load balance IPv6 packets
`src-ipv6`	Source IPV6 based load balancing
`dest-ipv6`	Destination IPv6 based load balancing
`srcl4-port`	Source L4 port based load balancing
`destl4-port`	Destination L4 port based load balancing
`next-hdr`	Next header field for IPv6
`l2`	Load balance L2 packets
`dest-mac`	Destination MAC address based load balancing
`src-mac`	Source MAC address based load balancing
`ether-type`	Ether-type based load balancing
`vlan`	VLAN-based load balancing
`tunnel`	Load balance tunneled packets based on outer header (default uses the inner-header)
`outer-l3-header`	Use outer header for hashing (ip-over-ip, ipv6-over-ip, ip-over-gre-ip, ipv6-over-gre-ip, ipv6-over-ipv6, ip-over-ipv6, ip-over-gre-ipv6, ipv6-over-gre-ipv6)
`mpls-ler`	Load balance LER packets
`inner-l2`	Load balance Inner l2 header
`dest-mac`	Destination MAC address load balancing
`src-mac`	Source MAC address
`ether-type`	Ether-type based load balancing
`vlan`	VLAN tag id
`inner-l3`	Inner l3 header
`dest-ip`	Destination IP address
`src-ip`	Source IP address
`srcl4-port`	Source L4 port based load balancing
`protocol ID`	Protocol (IPv4), nxt-hdr (IPv6)

Command Mode

Configure mode

© 2021 IP Infusion Inc. Proprietary

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#load-balance rtag7
(config)#load-balance rtag7 ipv4 src-ipv4
```

load-balance rtag7 hash

Use this command to set the rtag7 hash computation method.

Use the `no` parameter to set the rtag7 hash computation method to its default.

Command Syntax

```
load-balance rtag7 hash (crc16-bisync|crc16-ccitt|crc32-lo|crc32-hi)
no load-balance rtag7 hash
```

Parameters

`crc16-bisync`	16-bit CRC16 using the binary synchronous polynomial.
`crc16-ccitt`	16-bit CRC16 using the CCITT polynomial.
`crc16-hi`	16 most significant bits of computed CRC32.
`crc16-lo`	16 least significant bits of computed CRC32

Default

The default rtag7 hash computation method is 16-bit CRC16 using the binary synchronous polynomial `(crc16-bisync)`.

Command Mode

Configure mode

Default settings

```
load-balance rtag7 hash crc16-bisync
```

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#load-balance rtag7
(config)#load-balance rtag7 hash crc16-ccit
(config)#show running-config | inc rtag7
!
load-balance rtag7
load-balance rtag7 hash crc16-ccitt
!
(config)#no load-balance rtag7 hash
(config)#
```


© 2021 IP Infusion Inc. Proprietary

load-balance rtag7 macro-flow

Use this command to enable rtag7 macro-flow based hashing.

When macro-flow is enabled, a hash function is chosen dynamically based on corresponding macro flow. It is useful when hash polarization is observed in the topology.

Note: In case of topology having multiple level of split paths, macro-flow improves the distribution but can still have variation in traffic distribution. It is observed that when 2 level of hashing is present in topology (LAG after ECMP split traffic to half), 6% of variation was observed.

Use the `no` parameter to disable rtag7 macro-flow based hashing.

Command Syntax

```
load-balance rtag7 macro-flow
```

```
no load-balance rtag7 macro-flow
```

Parameters

None

Default

By default, rtag7 macro-flow based hashing is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#load-balance rtag7
(config)#load-balance rtag7 macro-flow
(config)#show running-config | inc rtag7
!
load-balance rtag7
load-balance rtag7 macro-flow
!
(config)#no load-balance rtag7 macro-flow
```

show forwarding profile limit

Use this command to show all the forwarding table sizes.

Note: The use of `k` for “kilo” (as in 1k) does not equal 1,000. In all cases, `k` equals 2 ^10: 1,024.

Command Syntax

```
show forwarding profile limit
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show forwarding profile limit

 Configured profile : custom-profile
 Forwarding profile : custom-profile(Active in hardware)

 ------------------------------------------------------------------------
|                     Forwarding Profile Table Size                      |
|------------------------------------------------------------------------|
|Profile Name    |MAC    |Host-Table   |Prefix-     |Vlan-   |Egress-    |
|                |ADDR   |Table(UC)    |Table(UC)   |xlate-  |Vlan-xlate |
|                |Table  |IPV4  |IPv6  |IPV4  |IPV6 |Table   |Table      |
 ------------------------------------------------------------------------
  l2-profile-one      96k     0k     0k     8k    4k       0k        0k
  l2-profile-two      64k     8k     4k     8k    4k       8k        8k
l2-profile-three      32k    16k     8k     8k    4k      16k       16k
      l3-profile       4k    92k    46k     8k    4k       0k        0k
  custom-profile     576k    60k    30k     8k    4k       0k        0k#
```

Table 24-76 explains the show command output fields.

© 2021 IP Infusion Inc. Proprietary

Table 24-76: show forwarding profile limit output

Field	Description
Profile Name	Names of the forwarding profiles
MAC ADDR Table	MAC address table sizes
Host-Table (UC) IPv4	IPv4 unicast host table sizes
Host-Table (UC) IPv6	IPv6 unicast host table sizes
Prefix-Table (UC) IPv4	IPv4 unicast prefix table sizes
Prefix-Table (UC) IPv6	IPv6 unicast prefix table sizes
Vlan-xlate-Table	Number of VLAN translate banks
Egress-Vlan-xlate-Table	Number of egress VLAN translate banks

show hardware-profile filters

Use this command to check the status of hardware filter groups. Status is not shown for filter groups which are disabled.

Command Syntax

```
show hardware-profile filters
```

Parameters

None

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is *not* available on Qumran platforms.

Examples

```
#show hardware-profile filters

INGRESS:
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
QOS                  244       5     12        256     256         0
L2-ACL               253       1     3         256     256         0
IPV4-ACL             256       0     0         256     256         0
ARP-ACL              242       5     14        256     256         0

EGRESS:
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
L2-ACL/IPV4-ACL/QOS  512       0     0         512     256         256
```

Table 24-77 explains the output fields.

© 2021 IP Infusion Inc. Proprietary

Table 24-77: show hardware-profile filters

Field	Description
EGRESS	Egress filtering is a process in which outbound data is monitored or restricted, usually by means of a firewall that blocks packets that fail to meet certain security requirements.
INGRESS	Ingress filtering is a method used to prevent suspicious traffic from entering a network.
TCAMS	Number of ternary content addressable memory (TCAM) entries a particular firewall filter.
Free Entries	Number of TCAM filter entries available for use by the filter group.
Used Entries	Number of TCAM filter entries used by the filter group.
Total Entries	Number of TCAM total filter entries to the filter group.
Dedicated Entries	Number of TCAM filter entries dedicated to the filter group.
Shared Entries	Number of TCAM filter entries shared to the filter group.

snmp restart

Use this command to restart SNMP for a given process.

Command Syntax

```
snmp restart (auth | bfd | bgp | cfm | efm | isis | ldp | lldp | mrib | mstp | nsm
  | ospf | ospf6 | pim | rib| rmon | rsvp | vrrp)
```

Parameters

None

Default

By default, SNMP resart is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart nsm
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 25 TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+, usually pronounced like tack-axe) is an access control network protocol for network devices.

The differences between RADIUS and TACACS+ can be summarized as follows:

- RADIUS combines authentication and authorization in a user profile, while TACACS+ provides separate authentication.
- RADIUS encrypts only the password in the access-request packet sent from the client to the server. The remainder of the packet is unencrypted. TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.
- RADIUS uses UDP, while TACACS+ uses TCP.
- RADIUS is based on an open standard (RFC 2865). TACACS+ is proprietary to Cisco, although it is an open, publicly documented protocol (there is no RFC protocol specification for TACACS+).

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

- add policy
- clear tacacs-server counters
- debug tacacs+
- default
- deny
- feature dynamic-rbac enable
- feature tacacs+
- permit
- policy
- role
- show debug tacacs+
- show rbac-policy
- show rbac-role
- show running-config tacacs+
- show tacacs-server
- tacacs-server login host
- tacacs-server login key
- tacacs-server login timeout

add policy

Use this command to add a policy to a TACACS+ role-based authorization (RBAC) role.

Use the `no` form of this command to remove a policy from an RBAC role.

Command Syntax

```
add policy POLICY-NAME
no add policy POLICY-NAME
```

Parameters

`POLICY-NAME`	Name of the policy

Default

None

Command Mode

RBAC role mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#no add policy myPolicy2
```


© 2021 IP Infusion Inc. Proprietary

clear tacacs-server counters

Use this command to clear the counter on a specified TACACS server.

Syntax

```
clear tacacs-server ((HOSTNAME | X:X::X:X | A.B.C.D)|) counters (vrf (management |
  all)|)
```

Parameters

`HOSTNAME`	The name of the server
`X:X::X:X`	IPv6 address of the server
`A.B.C.D`	IPv4 address of the server
`vrf`	VRF of the sever
`management`	The management VRF
`all`	All VRFs

Default

NA

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear tacacs-server 10.1.1.1 counters
```

debug tacacs+

Use this command to display TACACS+ debugging information.

Use the `no` form of this command stop displaying TACACS+ debugging information.

Command Syntax

```
debug tacacs+
no debug tacacs+
```

Parameters

None

Default

Disabled

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug tacacs+
```


© 2021 IP Infusion Inc. Proprietary

default

Use this command to set the default rule for a TACACS+ role-based authorization (RBAC) role.

Command Syntax

```
default (permit-all | deny-all)
```

Parameters

`permit-all`	Permit all commands
`deny-all`	Deny all commands

Default

Unless you explicitly give this command, the default rule for a role is `deny-all`.

Command Mode

RBAC role mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#add policy myPolicy2
```

deny

Use this command to add a deny rule to a TACACS+ role-based authorization (RBAC) policy.

Use the `no` form of this command to remove a deny rule from an RBAC policy.

Command Syntax

```
deny RULE-STRING (mode MODE-NAME |)
no deny RULE-STRING (mode MODE-NAME |)
```

Parameters

`RULE-STRING`	Command string
`MODE-NAME`	Command prompt string such as “(config-router)” or “(config-if)’. Deny access to the command only in this mode.

Default

None

Command Mode

RBAC policy mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#configure terminal
(config)#policy myPolicy
(config-policy)#deny “ip address” mode config-if
```


© 2021 IP Infusion Inc. Proprietary

feature dynamic-rbac enable

Use this command to enable the TACACS+ role-based authorization (RBAC) feature.

Use the `no` form of this command to disable the RBAC feature.

Command Syntax

```
feature dynamic-rbac enable
no feature dynamic-rbac enable
```

Parameters

None

Default

By default, feature TACACS+ RBAC is disabled

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#configure terminal
(config)#feature dynamic-rbac enable
```

feature tacacs+

Use this command to enable the TACACS+ feature.

Use the `no` form of this command to disable the TACACS+ feature.

Command Syntax

```
feature tacacs+ (vrf management|)
no feature tacacs+ (vrf management|)
```

Parameters

`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

By default, feature tacacs+ is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature tacacs+ vrf management
```


© 2021 IP Infusion Inc. Proprietary

permit

Use this command to add a permit rule to a TACACS+ role-based authorization (RBAC) policy.

Use the `no` form of this command to remove a permit rule in an RBAC policy.

Command Syntax

```
permit RULE-STRING (mode MODE-NAME |)
no permit RULE-STRING (mode MODE-NAME |)
```

Parameters

`RULE-STRING`	Command string
`MODE-NAME`	Command prompt string such as “(config-router)” or “(config-if)”. Permit access to the command only in this mode.

Default

None

Command Mode

RBAC policy mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#configure terminal
(config)#policy myPolicy
(config-policy)#permit “ip address” mode config-if
```

policy

Use this command to create a TACACS+ role-based authorization (RBAC) policy and enter RBAC policy mode.

Use the `no` form of this command to remove an RBAC policy.

Command Syntax

```
policy POLICY-NAME
no policy POLICY-NAME
```

Parameters

`POLICY-NAME`	Policy name

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#configure terminal
(config)#policy myPolicy
(config-policy)#permit "ip address" mode config-if
```


© 2021 IP Infusion Inc. Proprietary

role

Use this command to create a TACACS+ role-based authorization (RBAC) role and enter RBAC role mode.

Use the `no` form of this command to remove an RBAC role.

Command Syntax

```
role ROLE-NAME
no role ROLE-NAME
```

Parameters

`ROLE-NAME`	Role name.
	You *cannot* specify one of these roles already defined in OcNOS:
	`network-admin`
	`network-user`
	`network-operator`
	`network-engineer`
	For more about these built-in roles, see username.

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#add policy myPolicy2
```

show debug tacacs+

Use this command to display whether TACACS+ debugging is enabled.

Command Syntax

```
show debug tacacs+
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug tacacs+
TACACS client debugging is on
```


© 2021 IP Infusion Inc. Proprietary

show rbac-policy

Use this command to display TACACS+ role-based authorization (RBAC) policies.

Command Syntax

```
show rbac-policy (POLICY-NAME |)
```

Parameters

POLICY-NAME	Policy name

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#show rbac-policy myPolicy
-------------------------------------------------------------------------
Policy Name     : myPolicy
permit "ip address" mode config-if
```

show rbac-role

Use this command to display information about TACACS+ role-based authorization (RBAC) roles.

Command Syntax

```
show rbac-role (ROLE-NAME |)
```

Parameters

ROLE-NAME	Role name

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced in OcNOS version 1.3.5.

Examples

```
#show rbac-role myRole
------------------------------------------------------------------------
Role Name           : myRole
Default rule        : permit-all
Attached Policies   : myPolicy1
                    : myPolicy2

------------------------------------------------------------------------
```

Table 25-78 explains the output fields.

Table 25-78: show rbac-role fields

Entry	Description
Role Name	Role name
Default rule	permit-all or deny-all
Attached Policies	Name of policies attached to this role

© 2021 IP Infusion Inc. Proprietary

show running-config tacacs+

Use this command to display TACACS+ settings in the running configuration.

Command Syntax

```
show running-config tacacs+
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config tacacs+
feature tacacs+ vrf management
tacacs-server login host 10.16.19.2 vrf management seq-num 1 key 7
0x9f4a8983e0216052
```

Table 25-79 explains the output fields.

Table 25-79: show running-config fields

Entry	Description
TACAS server host	TACACS+ server Domain Name Server (DNS) name.
Seq-num	Sequence number of user authentication attempt with the TACACS+ server.
VRF Management	The management traffic using VPN Routing and Forwarding (VRFs).

show tacacs-server

Use this command to display the TACACS+ server configuration.

Command Syntax

```
show tacacs-server (|vrf (management|all))((WORD)|(groups (GROUP|)|)|(sorted)
```

Parameters

WORD	DNS host name or IP address
groups	TACACS+ server group
GROUP	Group name; if this parameter is not specified, display all groups
sorted	Sort by TACACS+ server name
vrf	management or all VRFs

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show tacacs-server
total number of servers:1

Tacacs+ Server                 : 192.168.10.215/49(*)
           Sequence Number     : 1
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 14
   Failed Connect Attempts     : 0
 Last Successful authentication: 2017 December 18, 12:27:13

(*) indicates last active.
```

Table 25-80 explains the output fields.

Table 25-80: show tacacs-server output fields

Field	Description
Sequence Number	Sequence number of user authentication attempt with the TACACS+ server.
Failed Auth Attempts	Number of times user authentication failed with the TACACS+ server. Increments for server key mismatches and password mismatches or wrong password for the user.
Success Auth Attempts	Number of times user authenticated with TACACS+ server. Increments for each successful login.

© 2021 IP Infusion Inc. Proprietary

Table 25-80: show tacacs-server output fields

Field	Description
Failed Connect Attempts	Number of failed TCP socket connections to the TACACS+ server. Increments for server connection failure cases such as server not-reachable, server port mismatches.
Last Successful authentication	Timestamp when user successfully authenticated with the TACACS+ server.

tacacs-server login host

Use this command to set the TACACS+ server host name or IP address.

Use the `no` form of this command to remove an TACACS+ server (if only a host name or IP address is specified as parameter) or to remove all of a TACACS+ server's configuration settings (if any other parameters are also specified).

Command Syntax

```
tacacs-server login host (HOSTNAME | X:X::X:X | A.B.C.D) (vrf management|) (seq-num
  <1-8> |) (key ((0 WORD) | (7 WORD) | (WORD))|) (port <1025-65535> |) (timeout <1-
  60> |)
no tacacs-server login host (HOSTNAME | A.B.C.D | X:X::X:X) (vrf management|)
no tacacs-server login host (HOSTNAME | X:X::X:X | A.B.C.D) (vrf management|) (key
  ((0 WORD) | (7 WORD) | (WORD))|) (port <1025-65535> |) (timeout <1-60> |)
```

Parameters

`HOSTNAME`	Host name
`X:X::X:X`	IPv6 address
`A.B.C.D`	IPv4 address
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF
`seq-num`	Sequence Number / Priority index for tacacs-servers
`key`	Authentication and encryption key (“shared secret”)
`0`	Unencrypted (clear text) shared key
`WORD`	Unencrypted key value; maximum length 63 characters
`7`	Hidden shared key
`WORD`	Hidden key value; maximum length 512 characters
`WORD`	Unencrypted (clear text) shared key value; maximum length 63 characters
`port`	TACACS+ server port
`<1205-65535>`	TACACS+ server port number; the default is 49
`timeout`	TACACS+ server timeout
`<1-60>`	Timeout value in seconds; default is 5 seconds

Default

Enable authentication for TACACS+ server configured. Authorization is also enabled by default. The default server port is 49.The default timeout value is 5 seconds.

There is `no` command to enable authorization. Authorization functionality is enabled by default when remote.

authentication is enabled with TACACS+.

© 2021 IP Infusion Inc. Proprietary

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#tacacs-server login host 203.0.113.31 vrf management
```

tacacs-server login key

Use this command to set a global preshared key (“shared secret”) which is a text string shared between the device and TACACS+ servers.

Use the `no` form of this command to remove a global preshared key.

Command Syntax

```
tacacs-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
no tacacs-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
```

Parameters

`0`	Unencrypted (clear text) shared key
`WORD`	Unencrypted key value; maximum length 63 characters
`7`	Hidden shared key
`WORD`	Hidden key value; maximum length 512 characters
`WORD`	Unencrypted (clear text) shared key value; maximum length 63 characters
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#tacacs-server login key 7 jvn05mlQH1 vrf management
```


© 2021 IP Infusion Inc. Proprietary

tacacs-server login timeout

Use this command to set the period to wait for a response from the server before the client declares a timeout failure. The default timeout value is 5 seconds.

You can only give this command when the TACACS+ feature is enabled.

Use the `no` form of this command to set the timeout value to its default value (5 seconds).

Note: TELNET client session's default timeout is 60 seconds, so configuring timeout of 60 seconds timeout impacts TELNET client applications, because it cannot be fallback to use the other configured server/group. Hence it is recommended to configure 57 seconds or lesser timeout while using TELNET. This timeout doesn't have an impact on SSH connections.

Command Syntax

```
tacacs-server login timeout <1-60> (vrf management|)
no tacacs-server login timeout (vrf management|)
```

Parameters

`<1-60>`	Timeout value in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

Disabled

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 1.3.9

Examples

```
#configure terminal
(config)#tacacs-server login timeout 35 vrf management
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 26 Telnet

This chapter describes telnet commands.

Telnet is a client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of functions.

Note: In OcNOS, the default Linux terminal type is "export TERM=xterm"

Note: The commands below are supported only on the "management" VRF.

This chapter contains these commands:

- debug telnet server
- feature telnet
- show debug telnet-server
- show running-config telnet server
- show telnet-server
- telnet
- telnet6
- telnet server port
- telnet server session-limit

debug telnet server

Use this command to display telnet debugging information.

Use the `no` form of this command to stop displaying telnet debugging information.

Command Syntax

```
debug telnet server
no debug telnet server
```

Parameters

None

Default

By default, disabled.

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug telnet-server

telnet server debugging is on
#
```


© 2021 IP Infusion Inc. Proprietary

feature telnet

Use this command to enable the telnet server.

Use the `no` form of this command to disable the telnet server.

Command Syntax

```
feature telnet (vrf management|)
no feature telnet (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

By default, feature telnet is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature telnet vrf management
```

show debug telnet-server

Use this command to display whether telnet debugging is enabled.

Command Syntax

```
show debug telnet-server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug telnet-server
telnet server debugging is on
```


© 2021 IP Infusion Inc. Proprietary

show running-config telnet server

Use this command to display telnet settings in the running configuration.

Command Syntax

```
show running-config telnet server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config telnet server
telnet server port 1025 vrf management
feature telnet vrf management
```

show telnet-server

Use this command to display the telnet server status.

Command Syntax

```
show telnet server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show telnet server
telnet server enabled port: 23
```


© 2021 IP Infusion Inc. Proprietary

telnet

Use this command to open a telnet session to an ipv4 address or host name resolved to ipv4 address.

Command Syntax

```
telnet (A.B.C.D | HOSTNAME) (vrf (NAME|management))
telnet (A.B.C.D | HOSTNAME) (<1-65535>) (vrf (NAME|management))
```

Parameters

A.B.C.D	Destination IPv4 Address to open a telnet session.
HOSTNAME	Destination Hostname to resolve into IPv4 address to open a telnet session.
1-65535	Destination Port to open a telnet session. Default is 23.
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

Default

By default, telnet is 23

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#telnet 10.12.16.17 2543 vrf management
Trying 10.12.16.17...
```

telnet6

Use this command to open a telnet session to an ipv6 address or host name resolved to ipv6 address.

Command Syntax

```
telnet6 (X:X::X:X| HOSTNAME) (vrf (NAME|management))
telnet6 (X:X::X:X | HOSTNAME) (<1-65535>) (vrf (NAME|management))
```

Parameters

X:X::X:X	Destination IPv6 Address to open a telnet session.
HOSTNAME	Destination Host name to resolve into IPv6 address to open a telnet session.
1-65535	Destination Port to open a telnet session. Default is 23.
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

Default

By default, telnet is 23.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#telnet6 2:2::2:2 2543 vrf management
 Trying 2:2::2:2...
```


© 2021 IP Infusion Inc. Proprietary

telnet server port

Use this command to set the port number on which the telnet server listens for connections. The default port on which the telnet server listens is 23.

You can only give this command when the telnet server is disabled. See the feature telnet command.

Use the `no` form of this command to set the default port number (23).

Command Syntax

```
telnet server (port <1024-65535>) (vrf management|)
no telnet server port (vrf management|)
```

Parameters

`<1024-65535>`	Port number
`management`	Virtual Routing and Forwarding name

Default

By default, telnet server port number is 23

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#telnet server port 1157 vrf management
```

telnet server session-limit

Use this command to limit number of Telnet sessions. Only 40 sessions allowed including Telnet and SSH.

This command can be used only when the telnet server is disabled. Refer to feature telnet command section for more information.

Use no form of this command to set to default value.

Command Syntax

```
telnet server session-limit <1-40> (vrf management|)
no telnet server session-limit (vrf management|)
```

Parameters

`<1-40>`	Number of sessions
`management`	Virtual Routing and Forwarding name

Default

By default, 40 sessions are allowed.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS-SP version 4.2

Examples

```
#configure terminal
(config)#telnet server session-limit 4 vrf management
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 27 Time Range Commands

This chapter describes the commands used to create and manage time range objects which are used to add a timing boundary for specified activities. The activity starts, ends, and repeats at the specific times that you set.

- end-time (absolute)
- end-time after (relative)
- frequency
- frequency days (specific days)
- start-time (absolute)
- start-time after (relative)
- start-time now (current)
- time-range

end-time (absolute)

Use this command to set the end time for the time range to an absolute time.

Command Syntax

```
end-time HH:MM <1-31> (january | february | march | april | may | june | july |
  august | september | october | november | december) <1995-2035>
```

Parameters

`HH:MM`	End time hour and minutes
`<1-31>`	Day of the month
`april`	Month of April
`august`	Month of August
`december`	Month of December
`february`	Month of February
`january`	Month of January
`july`	Month of July
`june`	Month of June
`march`	Month of March
`may`	Month of May
`november`	Month of November
`october`	Month of October
`september`	Month of September
`<1995-2035>`	Year

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#end-time 10:10 20 february 2021
```


© 2021 IP Infusion Inc. Proprietary

end-time after (relative)

Use this command to set the end time for the time range to a relative time in minutes, from the configured start time.

Command Syntax

```
end-time after <1-129600>
```

Parameters

<1-129600>	Number of minutes from the start time

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#end-time after 100
```

frequency

Use this command to set the frequency for the time range.

Command Syntax

```
frequency (daily|hourly|weekly)
```

Parameters

`daily`	Daily frequency
`hourly`	Hourly frequency
`weekly`	Weekly frequency

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#frequency hourly
```


© 2021 IP Infusion Inc. Proprietary

frequency days (specific days)

Use this command to set the frequency for the time range to specific days of the week.

Command Syntax

```
frequency days WORD
```

Parameters

WORD	Colon-separated list of 3-letter days of the week for the days on which the range is repeated. For example: `mon:tue:wed:thu:fri:sat:sun`

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#frequency days mon:wed:fri
(config)#exit
(config)#time-range TIMER2
(config-tr)#frequency days mon:tue:wed:thu:fri:sat:sun
```

start-time (absolute)

Use this command to set the start time for the time range to an absolute time.

Command Syntax

```
start-time HH:MM <1-31> (january | february | march | april | may | june | july |
  august | september | october | november | december) <1995-2035>
```

Parameters

HH:MM	End time hour and minutes
<1-31>	Day of the month
april	Month of April
august	Month of August
december	Month of December
february	Month of February
january	Month of January
july	Month of July
june	Month of June
march	Month of March
may	Month of May
november	Month of November
october	Month of October
september	Month of September
<1995-2035>	Year

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#start-time 09:09 20 february 2021
```


© 2021 IP Infusion Inc. Proprietary

start-time after (relative)

Use this command to set the start time for the time range to a relative time in minutes, from the current time.

Command Syntax

```
start-time after <1-129600>
```

Parameters

<1-129600>	Number of minutes from the current time

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#start-time after 100
```

start-time now (current)

Use this command to set the start time for the time range to the current system time.

Command Syntax

```
start-time now
```

Parameters

None

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#start-time now
```


© 2021 IP Infusion Inc. Proprietary

time-range

Use this command to create a time range and go into the time range mode to configure the time range. If the time range already exists, then it will be edited.

Use the `no` form of this command to remove a time range object.

Command Syntax

```
time-range NAME
no time-range NAME
```

Parameters

`NAME`	Name of the time range.

Default

N/A

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#configure terminal
(config)# time-range TIMER1
(config-tr)#?
Time Range configuration commands:
  WORD        String
  abort       Abort Transaction
  commit      commit
  end         End current mode and change to EXEC mode
  end-time    The end time for the Time Range
  exit        End current mode and down to previous mode
  frequency   The frequency of the Time Range
  help        Description of the interactive help system
  no          Delete
  quit        Exit current mode and down to previous mode
  show        Show running system information
  start-time  The start time for the Time Range
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 28 Traffic Mirroring Commands

This chapter provides a description of syntax, and examples for Traffic Mirroring. It includes the following commands:

- monitor session
- monitor session shut
- source port
- source vlan
- destination port
- no shut
- shut
- filter
- description
- remote destination
- show monitor
- show monitor session
- show filter
- show monitor running configuration

monitor session

Use this command to create a local or remote monitor session. By default, a local monitor session is created.

A monitor session consists of:

- A single destination interface, referred to as a mirror-to port or a single remote destination
- One or more source interfaces (egress, ingress, or both)
- One or more VLAN sources in the ingress direction
- One or more filters that can be applied to filter the mirrored packets

Use the `no` parameter to delete a monitor session.

Command Syntax

```
monitor session <1-18> ( | type ( local | remote ))
no monitor session ( <1-18> | all )
```

Parameters

`<1-18>`	Session number
`local`	Create a local session
`remote`	Create a remote source node session
`all`	All sessions

Default

By default, monitor session type is local and will not be active by default

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#monitor session 1
(config-monitor)#exit
(config)#monitor session 3 type remote
(config-monitor)#exit
(config)#no monitor session 1
```


© 2021 IP Infusion Inc. Proprietary

monitor session shut

Use this command to deactivate one or all monitor sessions.

Use the `no` parameter to activate one or all monitor sessions.

Command Syntax

```
monitor session (<1-18> | all) shut
no monitor session (<1-18> | all) shut
```

Parameters

`<1-18>`	Session number
`all`	All sessions

Default

Monitor session will not be active by default

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#monitor session 3 shut

(config)#no monitor session 3 shut
```

source port

Use this command to configure a source port per monitor session in either ingress or egress or both directions. Source port can be physical interface or a trunk port.

Use the `no` parameter to remove the source port.

Command Syntax

```
source interface IFNAME ( rx | tx | both | )
no source interface IFNAME ( rx | tx | both | )
```

Parameters

`IFNAME`	Interface name
`rx`	Ingress direction
`tx`	Egress direction
`both`	Both directions

Default

Source port will be mirrored for both directions if the direction is not specified

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 1
(config-monitor)#source interface xe1 both
(config-monitor)#no source interface xe1 tx
```


© 2021 IP Infusion Inc. Proprietary

source vlan

Use this command to configure one or more VLANs as source per monitor session. A VLAN as source will be mirrored only in the ingress direction. Up to 32 VLANs can be configured as source per monitor session.

Use the `no` parameter to remove vlan source from monitor session.

Command Syntax

```
source vlan VLAN_RANGE
no source vlan VLAN_RANGE
```

Parameters

`VLAN_RANGE`	VLAN identifier or VLAN identifier range

Default

A trunk port is a member of all VLANs by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 1
(config-monitor)#source vlan 2
(config-monitor)#source vlan 4-10
(config-monitor)#no source vlan 2-5,10
```

destination port

Use this command to configure a mirror-to port per local monitor session. A destination port can be a physical port or a trunk port.

Use the `no` parameter to remove the destination port from a local monitor session.

Command Syntax

```
destination interface IFNAME
no destination interface IFNAME
```

Parameters

`IFNAME`	Interface name

Default

No default value is specified

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe3
(config-if)#switchport
(config-if)#exit
(config)#monitor session 1
(config-monitor)#destination interface xe3
(config-monitor)#no destination interface xe3
```


© 2021 IP Infusion Inc. Proprietary

no shut

Use this command to activate a monitor session

Command Syntax

```
no shut
```

Parameters

None

Default

Monitor session will not be active by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#no shut
```

shut

Use this command to de-activate a monitor session.

Command Syntax

```
shut
```

Parameters

None

Default

Monitored session is not active by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#shut
```


© 2021 IP Infusion Inc. Proprietary

filter

Use this command to add filters to the monitor session. Filters can be applied only in case of ingress mirroring.

Use the `no` parameter to remove the filter from monitor session.

Command Syntax

```
filter {vlan <2-4094> | cos <0-7> | dest-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX
  XXXX.XXXX.XXXX) | src-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX XXXX.XXXX.XXXX) |
  frame-type (ETHTYPE | arp (req | resp|) (sender-ip A.B.C.D|) (target-ip A.B.C.D|)
  | ipv4 (src-ip (A.B.C.D | A.B.C.D/M)|) (dest-ip (A.B.C.D | A.B.C.D/M)|) | ipv6
  (src-ip X:X::X:X/M |) (dest-ip X:X::X:X/M |))}
no filter {vlan <2-4094> | cos <0-7> | dest-mac (host XXXX.XXXX.XXXX |
  XXXX.XXXX.XXXX XXXX.XXXX.XXXX) | src-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX
  XXXX.XXXX.XXXX) | frame-type (ETHTYPE | arp (req | resp|) (sender-ip A.B.C.D|)
  (target-ip A.B.C.D|) | ipv4 (src-ip (A.B.C.D | A.B.C.D/M)|) (dest-ip (A.B.C.D |
  A.B.C.D/M)|) | ipv6 (src-ip X:X::X:X/M |) (dest-ip X:X::X:X/M |))}
```

Parameters

`<2-4094>`	VLAN identifier
`<0-7>`	COS number
`XXXX.XXXX.XXXX`	MAC address
`ETHTYPE`	Ethertype
`arp`	ARP frames
`req`	Request frames
`resp`	Response frames
`A.B.C.D`	Single IP address
`A.B.C.D/M`	IP addresses with mask
`X:X::X:X/M`	IPv6 addresses with mask

Default

No default value is specified.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#filter dest-mac host 0000.0001.2421 frame-type ipv4
(config-monitor)#filter cos 3 frame-type arp req sender-ip 2.2.2.1
(config-monitor)#no filter dest-mac host 0000.0001.2421 frame-type ipv4
(config-monitor)#no filter cos 3 frame-type arp req sender-ip 2.2.2.1
```

Note: When filter parameters are configured in a single CLI, SPAN considers it as a single set of filters and matches all the parameters given

Example

```
(config-monitor)#filter vlan 10 cos 5
#show monitor session 1 filter
   session 1
---------------
filter count      : 1

  ---------------
  match set 1
  ---------------
  vlan : 10
  cos : 5
```

When filter parameters are configured using separate CLIs, SPAN considers it as separate set of filters and only the first matching filter is applied and rest of the filters are ignored

Example

```
(config-monitor)#filter vlan 10
(config-monitor)#filter cos 5
#show monitor session 1 filter
   session 1
---------------
filter count      : 2

  ---------------
  match set 1
  ---------------
  vlan : 10

  ---------------
  match set 2
  ---------------
 cos : 5
```

 © 2021 IP Infusion Inc. Proprietary

description

Use this command to add a description to the monitor session.

Use the `no` parameter to delete a description of the monitor session.

Command Syntax

```
description LINE
no description
```

Parameters

`LINE`	Enter the description string

Default

No default value is specified.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#description “port mirror rx”
(config-monitor)#no description
```

remote destination

Use this command to configure a destination VLAN and the reflector port for the remote monitor session.

Use the `no` parameter to remove a destination from a remote monitor session.

Command Syntax

```
destination remote vlan <2-4094> reflector-port IFNAME
no destination remote
```

Parameters

`<2-4094>`	VLAN identifier
`IFNAME`	Interface name

Default

No default value is specified

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#no vlan 900 bridge 1
(config)#interface xe3
(config-if)#switchport
(config)#monitor session 1
(config-monitor)#destination remote vlan 900 reflector-port xe3
(config-monitor)#no destination remote
```


© 2021 IP Infusion Inc. Proprietary

show monitor

Use this command to display states of all monitor sessions. If a session is down, the reason is displayed.

Command Syntax

```
show monitor
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor
Session   State          Reason                Description
------- ----------- --------------------- --------------------------------
1       down        No sources configured
2       down        Dst in wrong mode
```

Table 28-81 explains the output fields.

Table 28-81: show monitor fields

Entry	Description
Session admin shut	If the monitoring session is administratively shutdown, session will be in this state. This is the default state for any newly created monitoring session. Monitoring sessions can be activated using the command 'no shut' on monitoring session mode.
Dst in wrong mode	If both source and destination is configured on monitoring session and session is activated, then: 1. In case of local monitoring, if the destination port is not configured with 'switchport' or the destination is associated with bridge, then session will be in this state. Destination port shouldn't participate in regular switching. Hence this configuration state is mandatory. 2. In case of remote monitoring, if the reflector port is not configured with 'switchport' or the destination is associated with bridge and/or if remote VLAN is part of bridge then session will be in this state. Remote VLAN ID used for encapsulation should be unused VLAN ID by bridge on the mirroring node.
No sources configured	If no source configured on the monitoring session (either source VLAN or source ports) and monitoring session is activated, then the session will be in this state. In order to recover, source needs to be configured on the monitoring session. Multiple sources can be configured on a monitoring session.
No dest configured	If a session is not configured with destination (either destination port in case of local monitoring or with remote vlan and reflector port in case of remote monitoring) and if the monitoring session is activated, then session will be in this state. In order to recover, destination needs to be configured on the monitoring session. Only one destination can be configured per monitoring session.

Table 28-81: show monitor fields

Entry	Description
No operational src/dst	If both source and destination configured on monitoring session, destination is configured in right mode and session is activated, but 1. In case of local monitoring, if the destination port link state is down, then session will be in this state. 2. In case of remote monitoring, if the reflector port link state is down, then session will be in this state. 3. In case the sources configured are ports and none of them are in link up state, then session will be in this state. 4. In case the sources configured are VLAN and none of the VLANs are part of bridge forwarding, then session will be in this state.
No hardware resource	If all the configurations are correct and multiple sessions are configured and activated, then one of the hardware limitation may be reached: 1. Destination port exceeding maximum limit. 2. Filters exceeding maximum limit. 3. VLAN source ports exceeding maximum limit. In these cases, effected sessions will be in this state.
Hardware failure	If all the configurations are correct and sessions are activated but due to some expected or unexpected cases if the configuration cannot be applied in hardware, then the session will be in this state. This is not accepted state for a session and the issue needs to be analyzed and fixed.

© 2021 IP Infusion Inc. Proprietary

show monitor session

Use this command to display the configuration details of one or more monitor sessions.

Command Syntax

```
show monitor session (<1-18>|all|(range RANGE)) (brief|)
```

Parameters

`<1-18>`	Session number
`all`	All sessions
`RANGE`	Session number range (n1-n2)
`brief`	Brief information

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor session 1
session 1
---------------
type              : local
state             : down (Session admin shut)
source intf       :
tx                : xe1 xe3 xe4
rx                : xe2 xe3 xe4
both              : xe3 xe4
source VLANs      :
rx                : 2,5-10,15,18-20
destination ports : xe5
filter count      :

Legend: f = forwarding enabled, l = learning enabled
#
```

Table 28-82 explains the output fields.

Table 28-82: show monitor session output fields

Entry	Description
Type	Type of monitor session.
State	State of the security flow filter. There are different error messages when you do RSPAN configuration: 1. Session admin shut 2. Dst in wrong mode 3. No sources configured 4. No dest configured 5. No operational src/dst 6. No hardware resource 7. Hardware failure.
Session admin shut	If the monitoring session is administratively shutdown, session will be in this state. This is the default state for any newly created monitoring session. Monitoring sessions can be activated using the command 'no shut' on monitoring session mode.
Dst in wrong mode	If both source and destination is configured on monitoring session and session is activated, then: 1. In case of local monitoring, if the destination port is not configured with 'switchport' or the destination is associated with bridge, then session will be in this state. Destination port shouldn't participate in regular switching. Hence this configuration state is mandatory. 2. In case of remote monitoring, if the reflector port is not configured with 'switchport' or the destination is associated with bridge and/or if remote VLAN is part of bridge then session will be in this state. Remote VLAN ID used for encapsulation should be unused VLAN ID by bridge on the mirroring node.
No sources configured	If no source configured on the monitoring session (either source VLAN or source ports) and monitoring session is activated, then the session will be in this state. In order to recover, source needs to be configured on the monitoring session. Multiple sources can be configured on a monitoring session.
No dest configured	If a session is not configured with destination (either destination port in case of local monitoring or with remote vlan and reflector port in case of remote monitoring) and if the monitoring session is activated, then session will be in this state. In order to recover, destination needs to be configured on the monitoring session. Only one destination can be configured per monitoring session.
No operational src/dst	If both source and destination configured on monitoring session, destination is configured in right mode and session is activated, but: 1. In case of local monitoring, if the destination port link state is down, then session will be in this state. 2. In case of remote monitoring, if the reflector port link state is down, then session will be in this state. 3. In case the sources configured are ports and none of them are in link up state, then session will be in this state. 4. In case the sources configured are VLAN and none of the VLANs are part of bridge forwarding, then session will be in this state.
No hardware resource	If all the configurations are correct and multiple sessions are configured and activated, then one of the hardware limitation may be reached: 1. Destination port exceeding maximum limit. 2. Filters exceeding maximum limit. 3. VLAN source ports exceeding maximum limit. In these cases, effected sessions will be in this state.
Hardware failure	If all the configurations are correct and sessions are activated but due to some expected or unexpected cases if the configuration cannot be applied in hardware, then the session will be in this state. This is not accepted state for a session and the issue needs to be analyzed and fixed.

© 2021 IP Infusion Inc. Proprietary

Table 28-82: show monitor session output fields

Entry	Description
Rx	Incoming flow (source and destination IP addresses).
Tx	Reverse flow (source and destination IP addresses).
Both	Incoming and reverse flow (source and destination IP address)
Destination Port	Name of the destination port to be matched.
Source intf	Number of maximum intf central source session.
Source VLANs	Number of maximum VLANs central source session.
Filter count	Used to count number of lines in a file or table.

show filter

Use this command to display filters for one or more monitor sessions.

Command Syntax

```
show monitor session (<1-18>|all|(range RANGE)) filter
```

Parameters

`<1-18>`	Session number
`all`	All sessions
`RANGE`	Session number range (n1-n2)

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor session 1 filter
session 1
---------------
filter count : 3
---------------

match set 1
---------------
destination mac address : 0000.0002.4451 (host)
source mac address : 0000.0012.2288 (host)
---------------

match set 2
---------------
frame type : arp
sender ip address : 2.2.2.5
target ip addres : 2.2.2.8
---------------

match set 3
---------------
destination mac address : 0000.0001.1453 (host)
frame type : ipv4
source ip address : 3.3.3.5
#
```


© 2021 IP Infusion Inc. Proprietary

show monitor running configuration

Use this command to display the mirror-related running configuration.

Command Syntax

```
show running-config monitor (all|)
```

Parameters

`all`	Show running configuration with defaults

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config monitor
!
monitor session 1
 source interface xe10 rx
 destination interface po1
 no shut

#
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 29 Trigger Failover Commands

This chapter describes the trigger failover (TFO) commands.

- clear tfo counter
- fog
- fog tfc
- fog type
- link-type
- show tfo
- tfo

clear tfo counter

Use this command to clear the TFO counters. If you do not specify a parameter, this command clears counters for all FOG indexes.

Command Syntax

```
clear tfo counter
clear tfo counter fog <1-64>
```

Parameters

<1-64>	Clear counters for this Failover Group Index

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear tfo counter
```


© 2021 IP Infusion Inc. Proprietary

fog

Use this command to:

- Create or delete a failover group (FOG)
- Enable or disable an exisitng FOG

Even if FOG index do not exit, FOG can be created as enabled with “enable” option in CLI.

If the FOG index already exists:

- When the FOG status is disabled and Control Port Group (CPG) links are previously disabled (because of TFO), then the links are enabled. If a particular CPG member belongs to multiple CPGs, then this CPG member is enabled only if all corresponding Monitor Port Groups (MPG) are enabled.
- When the FOG status is enabled and MPG is down, then the corresponding CPG links are disabled.

Use the `no` form of this command to delete a FOG.

Command Syntax

```
fog <1-64> (enable|disable)
no fog <1-64>
```

Parameters

`<1-64>`	Failover Group Index
`enable`	Enable Failover Group
`disable`	Disable Failover Group

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#fog 5 enable
```

fog tfc

Use this command to set the number of links to trigger failover for a Monitor Port Groups (MPG).

Command Syntax

```
fog <1-64> tfc <0-63>
```

Parameters

<1-64>	Failover Group index
<0-63>	Trigger failover count

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#fog 5 tfc 7
```


© 2021 IP Infusion Inc. Proprietary

fog type

Use this command to map upstream/downstream links in a FOG as a Monitor Port Group (MPG) or Control Port Group (CPG).

Use the `no` form of this command to unmap upstream/downstream links.

Command Syntax

```
fog <1-64> type (mpg|cpg)
no fog <1-64> type (mpg|cpg)
```

Parameters

`<1-64>`	Failover Group Index
`mpg`	Map the interface to an MPG
`cpg`	Map the interface to a CPG

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#interface eth1
(config-if)#fog 5 type mpg
```

link-type

Use this command to make a port an uplink or downlink.

Use the `no` form of this command to remove the configuration.

Command Syntax

```
link-type (uplink|downlink)
no link-type
```

Parameters

`uplink`	Make the port an uplink
`downlink`	Make the port a downlink

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#interface eth1
(config-if)#link-type downlink
```


© 2021 IP Infusion Inc. Proprietary

show tfo

Use this command to display FOG configuration and statistics.

Command Syntax

```
show tfo
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show tfo
TFO : Enable

Failover Group 1 : Enable
Failover Status : MPG Link Failure
No. of links to trigger failover : 0
MPG Port(s) :
xe9   Status : DOWN
xe12   Status : DOWN
CPG Port :
xe4   Status : DOWN
No. of times MPG link failure : 1
No. of times MPG link recovered : 0
No. of times CPG got auto disabled : 1
No. of times CPG got auto enable : 0
```

Table 29-83 Explains the show command output fields.

Table 29-83: show tfo output fields

Field	Description
Failover Group	Enable the failover group.
Failover Status	Display the failover status.
No. of links to trigger failover	Number of links to trigger the failover group.

Field	Description
MPG Port	Details of the monitor port group.
CPG Port	Details of the control port group.

© 2021 IP Infusion Inc. Proprietary

tfo

Use this command to enable or disable trigger failover (TFO). TFO can be enabled only if the bridge mode is STP or RSTP.

Command Syntax

```
tfo (enable|disable)
```

Parameters

`enable`	Enables Trigger failover
`disable`	Disables Trigger failover

Default

By default, TFO is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#tfo enable
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 30 User Management

This chapter is a reference for user management commands.

This chapter includes these commands:

- clear aaa local user lockout username
- clear line
- clear user
- debug user-mgmt
- show user-account
- username

clear aaa local user lockout username

Use this command to unlock the locked user due to three times wrong password login attempt.

Command Syntax

```
clear aaa local user lockout username USERNAME
```

Parameters

USERNAME	User name; length 2-15 characters

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear aaa local user lockout username testuser
```


© 2021 IP Infusion Inc. Proprietary

clear line

Use this command to clear or close the already opened vty line sessions.

Command Syntax

```
clear line WORD
```

Parameters

```
WORD Enter the Location name (Max Size 64)
```

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

          Line       User               Idle        Location/Session  PID
TYPE   Role
   (*) 130 vty 0    [C]ocnos              0d00h00m     pts/0
16725   Local  network-admin
#clear line pts/0
Connection closed by foreign host.
-bash-4.1#
```

clear user

Use this command to clear or close the already opened sessions based on the username.

Note: This command will close active telnet sessions if the account being cleared is already active, however the SSH sessions will continue to persist until disconnect.

Command Syntax

clear user WORD

Parameters

```
WORD Enter the username (Max Size 28)
```

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

          Line       User              Idle        Location/Session  PID
TYPE   Role
   (*) 130 vty 0    [C]ocnos              0d00h00m     pts/0
16725   Local  network-admin
#clear user ocnos
Connection closed by foreign host.
-bash-4.1#
```


© 2021 IP Infusion Inc. Proprietary

debug user-mgmt

Use this command to display user management debugging information.

Use the `no` form of this command stop displaying user management debugging information.

Command Syntax

```
debug user-mgmt
```

```
no debug user-mgmt
```

Parameters

None

Default

By default, disabled.

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug user-mgmt
```

```
#config t
(config)#debug user-mgmt
```

show user-account

Use this command to display information about all users or a given user.

Command Syntax

```
show user-account (WORD|)
```

Parameters

WORD	User name

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show user-account
User:user1
                roles: network-operator
User:user2
                roles: network-operator
User:user3
                roles: network-operator
```


© 2021 IP Infusion Inc. Proprietary

username

Use this command to add a user or to change a user password.

The `role` parameter maps to privilege levels in the TACACS+ server as shown in Table 30-84

Table 30-84: Role/privilege level mapping

Role	Privilege level
Network administrator	15
Network engineer	14
Network operator	1 to 13
Network user	0 or greater then 15

Use the `no` form of this command to remove a user.

Command Syntax

```
username USERNAME
username USERNAME password (encrypted|) PASSWORD
username USERNAME role (network-admin|network-engineer|network-operator|network-user)
username USERNAME role (network-admin|network-engineer|network-operator|network-user) password (encrypted|) PASSWORD
username USERNAME (role (network-admin|network-engineer|network-operator|network-user|ROLE-NAME)|) password (encrypted|) PASSWORD
username disable-default
no username disable-default
no username USERNAME
```

Parameters

`USERNAME` Name of the user (2-15 alphanumeric characters)

`encrypted` Encrypted password

`PASSWORD` Password; length 5-32 characters

`network-admin` Network administrator role with all access permissions that can make permanent changes to the configuration. Changes persist after a reset/reboot of the switch.

Only network administrators can manage other users with the enable password, Authentication, Authorization and Accounting, RADIUS, and TACACS+ commands.

`network-engineer`

Network engineer role with all access permission that can make permanent changes to the configuration. Changes persist after a reset/reboot of the switch.

`network-operator`

Network operator role with all access permissions that can make temporary changes to the configuration. Changes do not persist after a reset/reboot of the switch.

`network-user`	Network user role with access permissions to display the configuration, but cannot change the configuration.
`ROLE-NAME`	Refers to an user-defined RBAC role
`disable-default`	This option is used to disable the implicit configuration of default user by the system. This command can be executed only by users with "`network-admin`" privileges. When this option is configured, explicit configuration of default user will be rejected. If default-user is explicitly configured using "`username`" CLI, it should be removed using "`no username USERNAME`" before configuring "disable-default".

Default

By default, user name is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#username fred_smith password fred123
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 31 VLOG Commands

This chapter describes virtual router log (VLOG) commands.

- show vlog all
- show vlog clients
- show vlog terminals
- show vlog virtual-routers

show vlog all

Use this command to display the output of all virtual router log `show` commands. For column descriptions, refer to descriptions of the individual commands.

Command Syntax

```
show vlog all
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog all

Type     Name     FD  UserVR  AllVrs  VRCnt
tty   /dev/pts/8  12  vr222    ---        1
tty   /dev/pts/4  13  <PVR>    ---        1

VR-Name  VR-Id  PVR-Terms  VR-Terms                  LogFile
CurSize
<PVR>       0          1        0         /var/local/zebos/log/pvr/my-log
1624320
vr111       1          0        0         n/a
n/a
vr222        2          0        1          /var/local/zebos/log/vr222/log-
vr222        0
vr333        3          0        0          /var/local/zebos/log/vr333/log-
vr333        0

Name  Id  MsgCnt        ConTime             ReadTime
NSM    1       1  Fri May-15 21:05:04  Fri May-15 21:05:04
IMI   19       1  Fri May-15 21:05:02  Fri May-15 21:05:02
```


© 2021 IP Infusion Inc. Proprietary

show vlog clients

Use this command to display all attached virtual router log clients (protocol modules).

Command Syntax

```
show vlog clients
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog clients

Name  Id  MsgCnt          ConTime                ReadTime
NSM    1       1     Fri May-15 21:05:04  Fri May-15 21:05:04
IMI   19       1     Fri May-15 21:05:02  Fri May-15 21:05:02
```

Table 31-85 explains the output:

Table 31-85: Virtual router log clients

Name	Name of protocol module
Id	Protocol module identifier
MsgCnt	Number of log messages received from protocol module
ConTime	Time the connection was established
ReadTime	Time the last log message was received

show vlog terminals

Use this command to display all active connections where VLOGD is forwarding log output.

Command Syntax

```
show vlog terminals
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog terminals

Type     Name      FD  UserVR  AllVrs  VRCnt
tty   /dev/pts/8  12  vr222    ---        1
tty   /dev/pts/4  13  <PVR>    ---        1
```

Table 31-86 explains the output:

Table 31-86: Virtual router log terminals

Type	Type of terminal
Name	Device name
FD	File descriptor
UserVR	Name of the Virtual Router where in which the user is logged in
AllVRs	Whether the PVR user requested debug output from all VRs
VRCnt	Number of VRs to which a terminal is attached

© 2021 IP Infusion Inc. Proprietary

show vlog virtual-routers

Use this command to display virtual router statistics such as the number of terminals attached.

Command Syntax

```
show vlog virtual-routers
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog virtual-routers

VR-Name  VR-Id  PVR-Terms  VR-Terms LogFile
CurSize
<PVR>         0  1          0        /var/local/zebos/log/pvr/my-log
1624320
vr111         1  0          0        n/a                                    n/a
vr222         2  0          1        /var/local/zebos/log/vr222/log-vr222   0
vr333         3  0          0        /var/local/zebos/log/vr333/log-vr333   0
```

Table 31-87 explains the output:

Table 31-87: Virtual router statistics

VR-Name	Virtual router name
VR-Id	Virtual router identifier
PVR-Terms	Number of attached PVR terminals
VR-Terms	Number of attached VR terminals
LogFile	Name of VR log file (this column is empty if writing to a log file is disabled)
CurSize	Log file current size

© 2021 IP Infusion Inc. Proprietary

SECTION 3

Installing, Licensing, and Upgrading

Install, License, and Upgrade Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *Install, License, and Upgrade Configuration*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Install, License, and Upgrade Configuration

The *OcNOS Installation Guide* contains the procedures for installing and licensing OcNOS, including:

- Downloading the OcNOS installation image.
- Downloading an OcNOS license.
- Installing OcNOS:
  - From an FTP, HTTP, or TFTP server
  - From a USB stick
  - Using Zero Touch Provisioning
- Setting up a license

OcNOS supports both patch upgrades and full upgrades:

- A patch upgrade means upgrading to a new OcNOS image with bug fixes, but without kernel changes.
- A full upgrade means upgrading to a new OcNOS ONIE image with bug fixes along with kernel changes.

The *OcNOS Installation Guide* also contains the procedures for upgrading an existing installation of OcNOS either by:

- Installing a new OcNOS version over an existing OcNOS version, which saves the existing configuration files.
- Installing a fresh version of OcNOS, which is destructive and removes existing configuration files, SSH keys, and trial licenses. You must manually restore such items from backups as needed.

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

Install, License, and Upgrade Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Licensing and Upgrade Commands*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Licensing and Upgrade Commands

This chapter describes the license and upgrade commands.

- license get
- license refresh
- license release
- show installers
- show license
- show sys-update details
- sys-update commit
- sys-update delete
- sys-update get
- sys-update install
- sys-update list-version
- sys-update rollback
- sys-update un-install

© 2021 IP Infusion Inc. Proprietary

license get

Use this command to fetch the license for this device from a network path or a USB mount path. This command validates the license against the device identifier.

Note: The system date must be correct to avoid installation failure.

For HTTP, FTP, or TFTP, ensure that the IP address is reachable from the OcNOS device and that the file location is correct.

If you install a license from a USB stick, insert it, and the contents of the USB are available as `///mnt/usb/`. For example:

```
>license get file:///mnt/usb/IPI-CC37ABBE0340.bin
```

After running the `license get` command, you can immediately use the switch without rebooting.

To verify, run the show license command after giving this command.

Command Syntax

```
license get (|(source-interface IFNAME)) WORD
```

Parameters

`IFNAME`	The interface used to download the license. If not specified, `eth0` is used. If the management interface of the switch is in the “management” VRF, then this command uses the “management” VRF to get the license from the specified path. You do need not to know if the management port is in the default VRF or the “management” VRF.

`WORD`	Where to get the license:
	`ftp://your-server-ip/path/to/file/IPI_deviceId.bin`
	`http://your-server-ip/path/to/file/IPI_deviceId.bin`
	`tftp://your-server-ip/path/to/file/IPI_deviceId.bin`
	`file:///mnt-point/usb/path/to/file/IPI_deviceId.bin`

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>license get http://myServer/IPI-CC37ABBE0340.bin
```

Specify the `source-interface` parameter to set the interface to use:

```
>license get source-interface xe2 http://myServer/IPI-CC37ABBE0340.bin
```


© 2021 IP Infusion Inc. Proprietary

license refresh

Use this command to install a license present on the device. This command is required only when the license get command reports error when installing the license but successfully downloaded the license.

When this command is given without a file name, the device installs the most recently downloaded license file.

Note: Always ensure that the device date is up to date to avoid license installation failures.

Once this command is successful, you can use the device without rebooting. Verify license installation with the show license command.

Command Syntax

```
license refresh (FILENAME|)
```

Parameters

FILENAME	License file name which exists on the device.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.7.

Examples

```
>license refresh
>license refresh IPI-CH3QX42.bin
```

license release

Use this command to release any type of license, node-locked or floating, on the device.

The device license is revoked immediately.

Command Syntax

```
license release
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
>license release
```


© 2021 IP Infusion Inc. Proprietary

show installers

Use this command to display a list of downloaded images on the device.

Command Syntax

```
show installers
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#show installers
/installers/DELL_S6000_ON-OcNOS-1.3.6.228a-DC_MPLS-S0-P0-installer
#
```

show license

Use this command to display the current license details and errors. The licenses are device locked, which means that a separate license is required for each device.

Command Syntax

```
show license
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>show license
License Type: Trial edition
Remaining day to expires : 21 day(s)
Node Identifier: 1402EC2DA140
Device Software : OCNOS-ENT-IPBASE

>show license
License Type: Evaluation, Limited edition
License Validity: Not Applicable
Node Identifier: A82BB59DCAD9
Device Software : OCNOS-DC-IPBASE
License Error: Invalid license file
```


© 2021 IP Infusion Inc. Proprietary

show sys-update details

Use this command to display upgrade details. The output indicates whether the current version is committed or rolled back.

Command Syntax

```
show sys-update details
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show sys-update details
Previous_version EC_AS5812_54X-OcNOS-1.3.4.265-DC_MPLS_ZEBM-S0-P0
Current_version EC_AS5812_54X-OcNOS-1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer
(committed)
Last_upgraded Wed Sep 26 14:40:06 UTC 2018
Auto Rollback end time NA
```

sys-update commit

Use this command to accept a new version. After a commit, you cannot roll back to a previous version. Until you commit a new version, you cannot save the configuration. Upgrading with an installer file is auto committed.

Command Syntax

```
sys-update commit
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sys-update commit
```


© 2021 IP Infusion Inc. Proprietary

sys-update delete

Use this command to delete a downloaded image.

Command Syntax

```
sys-update delete IMAGE_NAME
```

Parameters

IMAGE_NAME	Installer to delete

Default

None

Command mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#sys-update delete DELL_S6000_ON-OcNOS-1.3.6.228a-DC_MPLS-S0-P0-installer
```

sys-update get

Use this command to download an installer image.

Note: The URL must be compliant with RFC 3986.

Note: At times while downloading installer through TFTP protocol, download progress would show 100% from the start to the end of the download. This behavior is observed whenever the TFTP server doesn't support the TFTP Option Negotiation. Also at times TFTP download takes more time to download the installer though the client and server are part of the same subnet, eventually download operation even times out after 30 minutes. The reason for such issue is the latency, here some of the TFTP server implementations are lagging performance. In such instances we recommend to switch to a different TFTP server. This TFTP download operation is verified in Debian Linux machine against the server present in the `tftpd-hpa` package.

Command Syntax

```
sys-update get ((source-interface IFNAME)|) URL (verbose|)
```

Parameters

`IFNAME`	The interface used to download the new version. If not specified, eth0 is used.

`URL`	Where to get the installer:
	`http://your-server-ip/path/to/file/<abc-installer>`
	`ftp://your-server-ip/path/to/file/<abc-installer>`
	`tftp://your-server-ip/path/to/file/<abc-installer>`
	`file:///mnt/usb/path/to/file/<abc-installer>`

`verbose`	Include download logs in the output.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#sys-update get source-interface xe3 http://myServer/EC_AS5812_54X-OcNOS-1.3.7.52-DC_IPBASE-S0-P0-installer
```


© 2021 IP Infusion Inc. Proprietary

sys-update install

Use this command to upgrade the current software to a newer version. You can do two types of installation:

- If a `.deb` file is provided, the board is loaded with new binaries.
- If an installer file is provided, the board is completely installed with a new kernel and binaries.

Note:

1. During an upgrade, if a license is not available the existing configuration is not applied. Also, the `ZebOS.conf` file is not created and the `terminal monitor` command is not allowed.
2. The URL must be compliant with RFC 3986.
3. When this command is executed without the `source-interface` parameter, then eth0 and the default management VRF are used. When this command is executed with the `source-interface` parameter then that interface is used.
4. At times while downloading installer through TFTP protocol, download progress would show 100% from the start to the end of the download. This behavior is observed whenever the TFTP server doesn't support the TFTP Option Negotiation. Also at times TFTP download takes more time to download the installer though the client and server are part of the same subnet, eventually download operation even times out after 30 minutes. The reason for such issue is the latency, here some of the TFTP server implementations are lagging performance. In such instances we recommend to switch to a different TFTP server. This TFTP download operation is verified in Debian Linux machine against the server present in the `tftpd-hpa` package.

Command Syntax

```
sys-update install (|(source-interface IFNAME)) URL (verbose|)
```

Parameters

`IFNAME`	The interface used to download the new version. If not specified, `eth0` is used.

`URL`	Where to get the new version:
	`http://your-server-ip/path/to/file/<abc-updater.deb or abc-installer>`
	`ftp://your-server-ip/path/to/file/<abc-updater.deb or abc-installer>`
	`tftp://your-server-ip/path/to/file/<abc-updater.deb or abc-installer>`
	`file:///mnt/usb/path/to/file/<abc-updater.deb or abc-installer>`

`verbose`	Include upgrade logs in the output.

Default

None

Caution

OcNOS services are using `/usr/local/etc` path to store the device configuration, and this path mounted into a separate partition to isolate system configurations. This partition is meant only for system configuration. It will affect the system stability if the user uses this partition for storing general files. In this problematic state, if the device reboots, OcNOS services will not start properly, that would even create problems to the device connectivity. There will be an impact on normal system configuration operations.

User must take care of this problem just before issuing the following commands:

- `reload/sys-reload` - Reboots the device.
- `sys-shutdown` - This is to shutdown the device, but when users powers the device OcNOS services won't start cleanly.
- `reboot / shutdown` - From Linux shell
- Also includes all copy commands from Linux shell before issuing the user triggered reload commands.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sys-update install source-interface eth2 http://10.12.52.150/myServer/
EC_AS5812_54X-OcNOS-1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer verbose

#sys-update install http://10.12.52.150/myServer/EC_AS5812_54X-OcNOS-
1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer verbose

#sys-update install http://10.12.52.150/myServer/EC_AS5812_54X-OcNOS-
1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer

#sys-update install http://10.12.52.150/myServer/EC_AS5812_54X-OcNOS-
1.3.4.266-DC_MPLS_ZEBM-S0-P0-updater.deb
```


© 2021 IP Infusion Inc. Proprietary

sys-update list-version

Use this command to display files and folders. This command supports only FTP and the local file system.

Command Syntax

```
sys-update list-version ((source-interface IFNAME)|) URL
```

Parameters

`IFNAME`	The interface used to download the list. If not specified, `eth0` is used.

`URL`	Where to get the list:
	`ftp://(username@|)serverIP/path/to/file/`
	`file:///mnt/usb/path/to/file/`

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sys-update list-version ftp://10.12.52.150/
```

sys-update rollback

Use this command to roll back to the previous version. After a commit, you cannot roll back. Upgrading with an installer file does not support roll back.

Command Syntax

```
sys-update rollback (verbose|)
```

Parameters

`verbose`	Include details in the output.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sys-update rollback
#sys-update rollback verbose
```


© 2021 IP Infusion Inc. Proprietary

sys-update un-install

Use this command to un-install the device software remotely using the CLI and NetConf.management interfaces. This command decouples the device console dependency to un-install OcNOS.

This command puts the device in ONIE un-install mode and triggers device reboot. Upon reboot, ONIE detects the un-install mode and performs the un-installation. Once the un-installation completes, the device boots ONIE. To understand more about the un-installation technique, see the U-Boot and x86 Architecture sections at:

https://opencomputeproject.github.io/onie/design-spec/index.html#.

Note: By default, ONIE has SSH and Telnet services running, so you also have the option to trigger the installation through the management connection. For more information about SSH and Telnet connectivity, see:

https://opencomputeproject.github.io/onie/user-guide/index.html#debugging-an-installation.

Command Syntax

```
sys-update un-install
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
#sys-update un-install
```

© 2021 IP Infusion Inc. Proprietary

SECTION 4 # Layer 1

Layer 1 Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *Cross-Connect (XC)*
- Chapter 2, *Cross-Connect (XC) Resiliency*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Cross-Connect (XC)

This chapter contains the cross-connect configuration example.

Overview

This feature is to configure the cross connection between two ports.

The cross connect is bi-directional. The traffic which is received on the first interface is transmitted out to the second interface and the traffic which is received on the second interface is transmitted out to the first interface.

It is point-to-point and same end points (EP) cannot be used for another cross connect

This following are the types of end points supported by this port based cross connect.

1. Native Ethernet interface
2. LAG interface

Topology

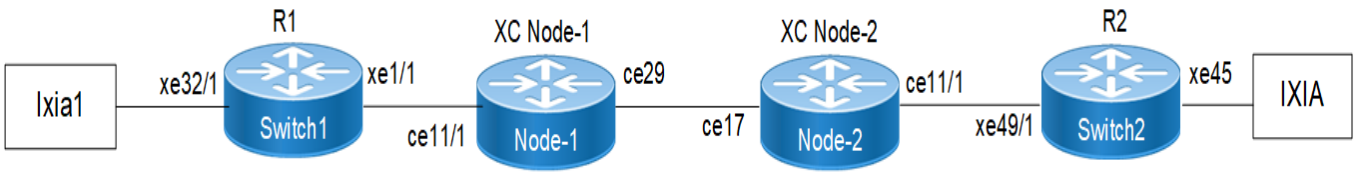


Figure 1-48: Cross-connect Topology-1

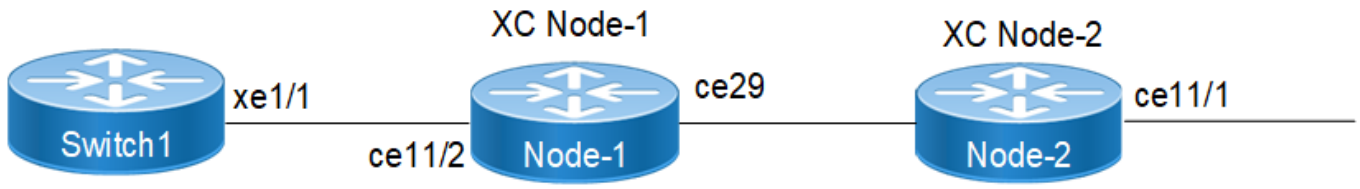


Figure 1-49: Cross-connect Topology-2

Configuration of the nodes using Topology-1

The following configuration example will illustrate OSPF, BFD and BGP session establishments via Cross-connect:

R1

`OcNOS#configure terminal`	Enter into configure terminal
`OcNOS(config)#hostname R1`	Configure the host name
`R1(config)#in xe1/1`	Enter into interface level
`R1(config-if)#ip address 10.10.10.1/24`	Configure ip address to the interface
`R1(config-if)#exit`	Exiting from interface level
`R1(config)#in xe32/1`	Enter into interface mode
`R1(config-if)#ip address 20.20.20.1/24`	Configure ip address to the interface
`R1(config-if)#exit`	Exiting from interface level
`R1(config)#interface lo`	Enter into loop-back interface
`R1(config-if)#ip address 1.1.1.1/24 secondary`	Configuring secondary ip address
`R1(config-if)#`	Exiting the loop-back interface level
`R1(config)#bfd interval 3 minrx 3 multiplier 3`	Configuring bfd options
`R1(config)#router ospf 10`	Configuring OSPF process
`R1(config-router)#router-id 1.1.1.1`	Configuring router-id
`R1(config-router)#network 10.10.10.0 0.0.0.255 area 0`	Configuring Network id and Area id
`R1(config-router)#redistribute connected`	Configuring redistribute connected
`R1(config-router)#bfd  all-interfaces`	Configuring bfd on all-interfaces
`R1(config-router)#exit`	Exiting the OSPF process
`R1(config)#router bgp 100`	Configuring bgp process
`R1(config-router)#neighbor 10.10.10.2 remote-as 200`	Configuring neighbor details
`R1(config-router)#end`	Exiting from the bgp process

XC Node-1

`OcNOS#configure terminal`	Entering into the configure terminal mode
`OcNOS(config)#hostname Xc Node-1`	Configuring the hostname
`Xc Node-1(config)#interface ce29`	Entering into interface level
`Xc Node-1(config-if)#switchport`	Configuring switchport
`Xc Node-1(config-if)#exit`	Exiting the interface level
`Xc Node-1(config)#in ce11/1`	Entering the interface level
`Xc Node-1(config-if)#switchport`	Configuring the switchport
`Xc Node-1(config-if)#exit`	Exiting the interface level
`Xc Node-1(config)#cross-connect OSPF_BFD_BGP`	Configuring the Cross-connect
`Xc Node-1(config-XC)#ep1 ce11/1 ep2 ce29`	Creating endpoints
`Xc Node-1(config-XC)#end`	Exiting cross-connect mode

© 2021 IP Infusion Inc. Proprietary

Xc Node-2

`OcNOS#configure terminal`	Entering into the configure terminal mode
`OcNOS(config)#hostname Xc Node-2`	Configuring the hostname
`Xc Node-2(config)#interface ce17`	Entering into interface level
`Xc Node-2(config-if)#switchport`	Configuring switchport
`Xc Node-2(config-if)#exit`	Exiting the interface level
`Xc Node-2(config)#interface ce11/1`	Entering the interface level
`Xc Node-2(config-if)#switchport`	Configuring the switchport
`Xc Node-2(config-if)#exit`	Exiting the interface level
`Xc Node-2(config)#cross-connect OSPF_BFD_BGP-1`	Configuring the Cross-connect
`Xc Node-2(config-XC)#ep1 ce17 ep2 ce11/1`	Creating endpoints
`Xc Node-2(config-XC)#end`	Exiting cross-connect mode

R2

`OcNOS#conf terminal`	Enter into configure terminal
`OcNOS(config)#hostname R2`	Configure the host name
`R2(config)#in xe49/1`	Enter into interface level
`R2(config-if)#ip address 10.10.10.2/24`	Configure ip address to the interface
`R2(config-if)#exit`	Exiting from interface level
`R2(config)#int xe45`	Enter into interface mode
`R2(config-if)#ip address 30.30.30.1/24`	Configure ip address to the interface
`R2(config-if)#exit`	Exiting from interface level
`R2(config)#interface lo`	Enter into loop-back interface
`R2(config-if)#ip address 2.2.2.2/24 secondary`	Configuring secondary ip address
`R2(config-if)#exit`	Exiting the loop-back interface level
`R2(config)#bfd interval 3 minrx 3 multiplier 3`	Configuring bfd options
`R2(config)#router ospf 10`	Configuring OSPF process
`R2(config-router)#router-id 2.2.2.2`	Configuring router-id
`R2(config-router)#network 10.10.10.0 0.0.0.255 area 0`	Configuring Network id and Area id
`R2(config-router)#redistribute connected`	Configuring redistribute connected
`R2(config-router)#bfd all-interfaces`	Configuring bfd on all-interfaces
`R2(config-router)#exit`	Exiting the OSPF process
`R2(config)#router bgp 200`	Configuring bgp process
`R2(config-router)#neighbor 10.10.10.1 remote-as 100`	Configuring neighbor details
`R2(config-router)#end`	Exiting from the bgp process

Validation

Cross-connect Validation:

```
Xc Node-1#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
-----------------+------+------+----------------+----------------+------------
OSPF_BFD_BGP       -      -      ce11/1           ce29             UP
-----------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
Xc Node-1#

Xc Node-1#show running-config cross-connect
cross-connect OSPF_BFD_BGP
 ep1 ce11/1 ep2 ce29

Xc Node-2#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
-----------------+------+------+----------------+----------------+------------
OSPF_BFD_BGP-1     -      -      ce17             ce11/1           UP
-----------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
Xc Node-2#
Xc Node-2#show running-config cross-connect
cross-connect OSPF_BFD_BGP-1
 ep1 ce17 ep2 ce11/1
```

OSPF Validation:

```
R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
       Instance ID
2.2.2.2           1   Full/Backup      00:00:37    10.10.10.2      xe1/1
          0
R1#


R2#show ip ospf neighbor
Total number of full neighbors: 1
OSPF process 10 VRF(default):
```


© 2021 IP Infusion Inc. Proprietary

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
       Instance ID
1.1.1.1           1   Full/Backup     00:00:38    10.10.10.1      xe49/1
          0
R2#
```

BFD Validation:

```
R1#show bfd interface xe1/1
Interface:      xe1/1  ifindex: 10001 state:   UP
Interface level configuration: NO ECHO, NO SLOW TMR
Min Tx: 3  Min Rx: 3  Multiplier: 3
R1#

R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
=====
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
      Down-Reason    Remote-Addr
1          1            IPv4         Single-Hop  Up          00:02:54  xe1/1
      NA             10.10.10.2/32
Number of Sessions:    1

R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
=====
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
      Down-Reason    Remote-Addr
1          1            IPv4         Single-Hop  Up          00:02:54  xe1/1
      NA             10.10.10.2/32
Number of Sessions:    1

R1#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================
====

Session Interface Index : 10001          Interface name :xe1/1
Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.10.10.1/32
Remote Discriminator : 1                 Remote Address : 10.10.10.2/32
Local Port : 49152                       Remote Port : 3784
```

```
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 3                 Min Rx: 3                 Multiplier: 3
Neg Tx: 3                 Neg Rx: 3                 Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000117138              Pkt Out : 00000000000000117172
Pkts Drop : 0000000000000000000            Auth Pkts Drop : 00000000000000000000
Echo Out : 0000000000000000000             IPv6 Echo Out : 0000000000000000000
IPv6 Pkt In : 0000000000000000000          IPv6 Pkt Out : 0000000000000000000
UP Count : 1                               UPTIME : 00:05:42

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
R1#

R2#show bfd interface xe49/1
Interface:     xe49/1  ifindex: 10049 state:   UP
Interface level configuration: NO ECHO, NO SLOW TMR
Min Tx: 3  Min Rx: 3  Multiplier: 3



R2#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
=====
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
      Down-Reason    Remote-Addr
1          1            IPv4         Single-Hop  Up          00:04:12  xe49/1
      NA             10.10.10.1/32
Number of Sessions:    1



R2#sh bfd session detail

BFD process for VRF: (DEFAULT VRF)
```


© 2021 IP Infusion Inc. Proprietary

```
================================================================================
====

Session Interface Index : 10049          Interface name :xe49/1
Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.10.10.2/32
Remote Discriminator : 1                 Remote Address : 10.10.10.1/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 3                Min Rx: 3                Multiplier: 3
Neg Tx: 3                Neg Rx: 3                Neg detect mult: 3
Min echo Tx: 1000        Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000044905              Pkt Out : 00000000000000044905
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                               UPTIME : 00:02:11

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

BGP Validation:

```
R1#sh bgp neighbors
BGP neighbor is 10.10.10.2, remote AS 200, local AS 100, external link
  BGP version 4, local router ID 10.10.10.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:04:00
  Last read 00:00:08, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 12 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
```

```
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.1, Local port: 179
Foreign host: 10.10.10.2, Foreign port: 58033
Nexthop: 10.10.10.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

R2#sh ip bgp neighbors
BGP neighbor is 10.10.10.1, remote AS 100, local AS 200, external link
  BGP version 4, local router ID 2.2.2.2, remote router ID 10.10.10.1
  BGP state = Established, up for 00:00:03
  Last read 00:00:03, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 2 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.2, Local port: 58033
Foreign host: 10.10.10.1, Foreign port: 179
Nexthop: 10.10.10.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
R2#
```

Show interface counters:

```
R1#sh interface counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1/1               6.91           13082945      6.91           13082949
```


© 2021 IP Infusion Inc. Proprietary

```
 xe32/1              6.91           13082325      6.91           13082325
R1#


Xc Node-1#sh interface counters rate gbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx gbps  |    Rx pps   |    Tx gbps  |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 ce11/1              6.91           13082437      6.91           13082437
 ce29                6.91           13082457      6.91           13082458
Xc Node-1#
Xc Node-1# sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
-----------------+------+------+---------------+---------------+------------
OSPF_BFD_BGP       -      -      ce11/1          ce29             UP
-----------------+------+------+---------------+---------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
Xc Node-1#

Xc Node-2#sh interface counters rate gbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx gbps  |    Rx pps   |    Tx gbps  |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 ce11/1              6.91           13082428      6.91           13082429
 ce17                6.91           13082381      6.91           13082378

 Xc Node-2#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
-----------------+------+------+---------------+---------------+------------
OSPF_BFD_BGP-1     -      -      ce17            ce11/1           UP
-----------------+------+------+---------------+---------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
Xc Node-2#

R2#sh interface counters rate gbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx gbps  |    Rx pps   |    Tx gbps  |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 xe45                6.91           13081988      6.91           13081988
 xe49/1              6.91           13082339      6.91           13082339
R2#
```

Configuration of the nodes using Topology-2

The following configuration example illustrates configuration of cross-connect using LAG interfaces on Xc Node:

Configuration on R1 Node:

`R1# configure terminal`	Enter configure mode
`R1(config)#interface po100`	Creating port channel interface
`R1(config-if)#exit`	Exit the interface level
`R1(config)#interface xe1/1`	Enter interface level
`R1(config-if)# channel-group 100 mode active`	Adding member port to the port channel interface
`R1(config-if)#exit`	Exit the interface level
`R1(config)#interface xe1/2`	Enter interface level
`R1(config-if)# channel-group 100 mode active`	Adding member port to the port channel interface
`R1(config-if)#exit`	Exit the interface level

© 2021 IP Infusion Inc. Proprietary

Configuring Cross connect using dynamic lag interfaces on XC_node1:

`XC_node1# configure terminal`	Enter configure mode
`XC_node1(config)#interface po100`	Creating port channel interface
`XC_node1(config-if)#switchport`	Configuring Switchport to the interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface po200`	Creating port channel interface
`XC_node1(config-if)#switchport`	Configuring Switchport to the interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce11/1`	Enter interface level
`XC_node1(config-if)# channel-group 100 mode active`	Adding member port to the port channel interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce11/2`	Enter interface level
`XC_node1(config-if)# channel-group 100 mode active`	Adding member port to the port channel interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce29`	Enter interface level
`XC_node1(config-if)# channel-group 200 mode active`	Adding member port to the port channel interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce30`	Enter interface level
`XC_node1(config-if)# channel-group 200 mode active`	Adding member port to the port channel interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#cross-connect lag`	Create cross-connect by providing the name
`XC_node1(config-XC)#ep1 po100 ep2 po200`	Adding end-points ep1 and ep2 as lag interfaces
`XC_node1(config-XC)#exit`	Exit Cross-connect mode
`XC_node1(config)#exit`	Exit Configure terminal mode

Configuring Cross connect using dynamic lag interfaces on XC_node2:

`XC_node2# configure terminal`	Enter configure mode
`XC_node2(config)#interface po200`	Creating port channel interface
`XC_node2(config-if)#switchport`	Configuring Switchport to the interface
`XC_node2(config-if)#exit`	Exit the interface level
`XC_node2(config)#interface ce29`	Enter interface level
`XC_node2(config-if)# channel-group 200 mode active`	Adding member port to the port channel interface
`XC_node2(config-if)#exit`	Exit the interface level
`XC_node2(config)#interface ce30`	Enter interface level
`XC_node2(config-if)# channel-group 200 mode active`	Adding member port to the port channel interface
`XC_node2(config-if)#exit`	Exit the interface level
`XC_node2(config)#interface ce11/1`	Enter interface level
`XC_node2(config-if)#Switchport`	Configure switchport to the interface
`XC_node2(config-if)#exit`	Exit the interface level
`XC_node2(config)#cross-connect lag`	Create cross-connect by providing the name
`XC_node2(config-XC)#ep1 po100 ep2 ce11/1`	Adding end-points ep1 and ep2 as lag interfaces
`XC_node2(config-XC)#exit`	Exit Cross-connect mode
`XC_node2(config)#exit`	Exit Configure terminal mode

Validation:

Cross-connect using Dynamic lag on XC_node1:

```
XC_node1#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
lag                -      -      po100            po200            UP
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0

XC_node1#sh running-config cross-connect
!
cross-connect lag
 ep1 po100 ep2 po200
!
XC_node1#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: Layer2
  Admin Key: 0100 - Oper Key 0100
     Link: ce11/1 (5073) sync: 1
```


© 2021 IP Infusion Inc. Proprietary

```
     Link: ce11/2 (5074) sync: 1
-------------------------------------
  Aggregator po200 100200
  Aggregator Type: Layer2
  Admin Key: 0200 - Oper Key 0200
     Link: ce30 (5005) sync: 1
     Link: ce29 (5006) sync: 1
```

Cross-connect using Dynamic lag on XC_node2:

```
XC_node2#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
lag                -      -      po200            ce11/1            UP
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0

XC Node-2#show running-config cross-connect
!
cross-connect lag
 ep1 po200 ep2 ce11/1

XC Node-2#sh etherchannel summary
  Aggregator po200 100200
  Aggregator Type: Layer2
  Admin Key: 0200 - Oper Key 0200
     Link: ce18 (5009) sync: 1
     Link: ce17 (5010) sync: 1
```

Configuring Cross connect using Static lag interfaces:

Configuration on R1 Node:

`R1# configure terminal`	Enter configure mode
`R1(config)#interface sa100`	Creating Static lag interface
`R1(config-if)#exit`	Exit the interface level
`R1(config)#interface xe1/1`	Enter interface level
`R1(config-if)# static-channel-group 100`	Adding member port to the static lag interface
`R1(config-if)#exit`	Exit the interface level
`R1(config)#interface xe1/2`	Enter interface level
`R1(config-if)# static-channel-group 100`	Adding member port to the static lag interface
`R1(config-if)#exit`	Exit the interface level

Configuring Cross connect using static lag interfaces on XC_node1:

`XC_node1# configure terminal`	Enter configure mode
`XC_node1(config)#interface sa100`	Creating static lag interface
`XC_node1(config-if)#switchport`	Configuring Switchport to the interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface sa200`	Creating static lag interface
`XC_node1(config-if)#switchport`	Configuring Switchport to the interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce11/1`	Enter interface level
`XC_node1(config-if)# static-channel-group 100`	Adding member port to the static lag interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce11/2`	Enter interface level
`XC_node1(config-if)# static-channel-group 100`	Adding member port to the static interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce29`	Enter interface level
`XC_node1(config-if)# static-channel-group 200`	Adding member port to the static lag interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#interface ce30`	Enter interface level
`XC_node1(config-if)# static-channel-group 200`	Adding member port to the static lag interface
`XC_node1(config-if)#exit`	Exit the interface level
`XC_node1(config)#cross-connect static-lag`	Create cross-connect by providing the name
`XC_node1(config-XC)#ep1 sa100 ep2 sa200`	Adding end-points ep1 and ep2 as lag interfaces
`XC_node1(config-XC)#exit`	Exit Cross-connect mode
`XC_node1(config)#exit`	Exit Configure terminal mode

© 2021 IP Infusion Inc. Proprietary

Configuring Cross connect using static lag interfaces on XC_node2:

`XC_node2# configure terminal`	Enter configure mode
`XC_node2(config)#interface sa200`	Creating static lag interface
`XC_node2(config-if)#switchport`	Configuring Switchport to the interface
`XC_node2(config-if)#exit`	Exit the interface level
`XC_node2(config)#interface ce29`	Enter interface level
`XC_node2(config-if)# static-channel-group 200`	Adding member port to the static lag interface
`XC_node2(config-if)#exit`	Exit the interface level
`XC_node2(config)#interface ce30`	Enter interface level
`XC_node2(config-if)# static-channel-group 200`	Adding member port to the static lag interface
`XC_node2(config-if)#exit`	Exit the interface level
`XC_node2(config)#interface ce11/1`	Enter interface level
`XC_node2(config-if)#Switchport`	Configure switchport to the interface
`XC_node2(config-if)#exit`	Exit the interface level
`XC_node2(config)#cross-connect static-lag`	Create cross-connect by providing the name
`XC_node2(config-XC)#ep1 po200 ep2 ce11/1`	Adding end-points ep1 and ep2 interfaces
`XC_node2(config-XC)#exit`	Exit Cross-connect mode
`XC_node2(config)#exit`	Exit Configure terminal mode

Validation:

Cross-connect using Static Lag on XC_node1:

```
XC_node1#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
static-lag         -      -      sa100            sa200            UP
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
```

Cross-connect using Static Lag on XC_node2:

```
XC_node2#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
------------------+------+------+----------------+----------------+------------
static-lag         -      -      sa200            ce11/1           UP
------------------+------+------+----------------+----------------+------------
cross-connect summary
Total : 1
```

```
Up    : 1
Down  : 0
```

Disable the Cross-connect on XC node1:

`Xc Node-1# configure terminal`	Enter configure mode
`Xc Node-1(config)#cross-connect lag`	Enter into cross-connect mode
`Xc Node-1(config-XC)#disable`	Disabling the cross-connect
`Xc Node-1(config-XC)# exit`	Exit the cross-connect

Validation:

Disable the cross-connect on XC node1:

```
Xc Node-1#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
-----------------+------+------+---------------+----------------+------------
lag                -      -      po100           po200            DOWN
-----------------+------+------+---------------+----------------+------------
cross-connect summary
Total : 1
Up    : 0
Down  : 1
```

Enable the Cross-connect XC_node1:

`Xc Node-1# configure terminal`	Enter configure mode
`Xc Node-1(config)#cross-connect lag`	Enter into cross-connect mode
`Xc Node-1(config-XC)#no disable`	Enable the cross-connect
`Xc Node-1(config-XC)#exit`	Exit the cross-connect

Validation:

Cross-connect after enable on XC_node1:

```
Xc Node-1#sh cross-connect
cross-connect status
XC name            o-vlan i-vlan Ep1              Ep2              Admin-Status
-----------------+------+------+---------------+----------------+------------
lag                -      -      po100           po200            UP
-----------------+------+------+---------------+----------------+------------
cross-connect summary
Total : 1
Up    : 1
Down  : 0
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Cross-Connect (XC) Resiliency

This Chapter contains the cross-connect resiliency configuration example.

Overview

This feature provides resiliency support for port level cross connect when primary link goes down. Whenever, any of the endpoint (EP) of cross-connect goes down, pre-configured backup EP will be chosen and cross-connect will be up with backup EP. Same backup EP cannot be used in another cross-connect link.

This following are the types of EPs supported as backup EPs.

1. Native Ethernet interface
2. LAG interface

Topology

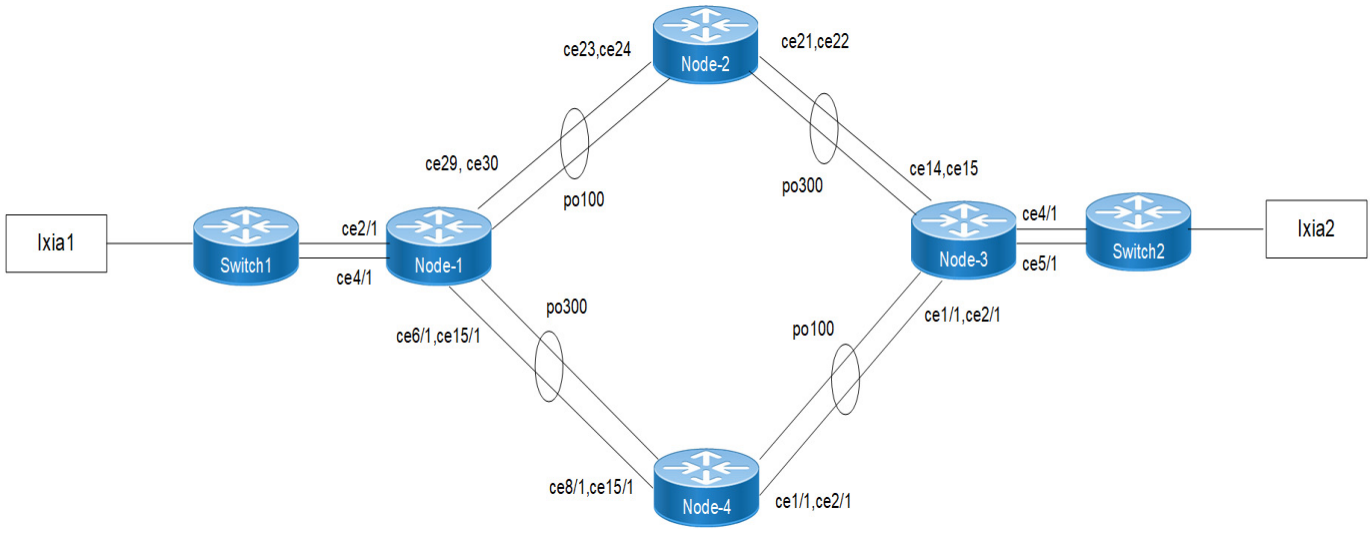


Figure 2-50: Cross-connect Resiliency Topology

LFPT (Link-Fault-Pass-Through)

If one endpoint goes down, other endpoint of the link is notified and port status is shown as DOWN.

Example: If po100 interface of Node-1 goes down, then Node-2 will inform to Node-3 via LFPT to down the po300 interface.

Revertive

When primary EP comes up, then traffic need to switch from backup EP to Primary EP.

Example: Suppose po100 is down on Node-1, the traffic flow is send to backup EP po300. Whenever the po100 comes up on Node-1 then the traffic flow is switched from backup EP po300 to primary EP po100.

Node-1

`#configure terminal`	Enter configure mode
`(config)#hostname Node-1`	Configure the hostname
`(config)#interface po100`	Create port channel interface
`(config-if)#switchport`	Configure switchport on LAG port
`(config-if)#exit`	Exit the interface level
`(config)#interface ce29`	Enter interface level
`(config-if)#channel-group 100 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface ce30`	Enter interface level
`(config-if)#channel-group 100 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface po300`	Create port channel interface
`(config-if)#switchport`	Configure switchport on LAG interface
`(config-if)#exit`	Exit the interface level
`(config)#interface ce6/1`	Enter interface level
`(config-if)#channel-group 300 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface ce15/1`	Enter interface level
`(config-if)#channel-group 300 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface ce2/1`	Enter interface level
`(config-if)#switchport`	Configure switchport
`(config)#interface ce4/1`	Enter interface level
`(config-if)#switchport`	Configure switchport
`(config-if)#exit`	Exit the interface level
`(config)#cross-connect sample`	Create cross-connect by providing the name
`(config-XC)#ep1 po100 ep2 ce2/1`	Add end-points end-point1 and end-point2
`(config-XC)#backup ep1 po300`	Add backup end-point1
`(config-XC)#backup ep2 ce4/1`	Add backup end-point2
`(config-XC)#cross-connect switchover type revertive`	Configure revertive mode
`(config-XC)#link-fault-pass-through enable`	Configure LFPT

© 2021 IP Infusion Inc. Proprietary

Node-2

`#configure terminal`	Enter configure mode
`(config)#hostname Node-2`	Configure the hostname
`(config)#interface po100`	Create port channel interface
`(config-if)#switchport`	Configure switchport on LAG port
`(config-if)#exit`	Exit the interface level
`(config)#interface ce23`	Enter interface level
`(config-if)#channel-group 100 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface ce24`	Enter interface level
`(config-if)#channel-group 100 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface po300`	Create port channel interface
`(config-if)#switchport`	Configure switchport on LAG interface
`(config-if)#exit`	Exit the interface level
`(config)#interface ce21`	Enter interface level
`(config-if)#channel-group 300 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#interface ce22`	Enter interface level
`(config-if)#channel-group 300 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level
`(config)#cross-connect sample2`	Create cross-connect by providing the name
`(config-XC)#ep1 po100 ep2 po300`	Add end-points end-point1 and end-point2
`(config-XC)#link-fault-pass-through enable`	Configure LFPT

Node-3

`#configure terminal`	Enter configure mode
`(config)#hostname Node-3`	Configure the hostname
`(config)#interface po300`	Create port channel interface
`(config-if)#switchport`	Configure switchport on LAG port
`(config-if)#exit`	Exit the interface level
`(config)#interface ce13`	Enter interface level
`(config-if)#channel-group 300 mode active`	Add member port to the port channel interface
`(config-if)#lacp timeout short`	Configure LACP timeout as short
`(config-if)#exit`	Exit the interface level

(config)#interface ce14	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface po100	Create port channel interface
(config-if)#switchport	Configure switchport on LAG interface
(config-if)#exit	Exit the interface level
(config)#interface ce1/1	Enter interface level
(config-if)#channel-group 100 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce2/1	Enter interface level
(config-if)#channel-group 100 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce4/1	Enter interface level
(config-if)#switchport	Configure switchport
(config)#interface ce5/1	Enter interface level
(config-if)#switchport	Configure switchport
(config-if)#exit	Exit the interface level
(config)#cross-connect sample3	Create cross-connect by providing the name
(config-XC)#ep1 po300 ep2 ce4/1	Add end-points end-point1 and end-point2
(config-XC)#backup ep1 po100	Add backup end-point1
(config-XC)#backup ep2 ce5/1	Add backup end-point2
(config-XC)#cross-connect switchover type revertive	Configure revertive mode
(config-XC)#link-fault-pass-through enable	Configure LFPT

Node-4

#configure terminal	Enter configure mode
(config)#hostname Node-4	Configure the hostname
(config)#interface po100	Create port channel interface
(config-if)#switchport	Configure switchport on LAG port
(config-if)#exit	Exit the interface level
(config)#interface ce1/1	Enter interface level
(config-if)#channel-group 100 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce2/1	Enter interface level
(config-if)#channel-group 100 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit the interface level
(config)#interface po300	Create port channel interface
(config-if)#switchport	Configure switchport on LAG interface
(config-if)#exit	Exit the interface level
(config)#interface ce8/1	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#interface ce15/1	Enter interface level
(config-if)#channel-group 300 mode active	Add member port to the port channel interface
(config-if)#lacp timeout short	Configure LACP timeout as short
(config-if)#exit	Exit the interface level
(config)#cross-connect sample4	Create cross-connect by providing the name
(config-XC)#ep1 po300 ep2 po100	Add end-points end-point1 and end-point2
(config-XC)#link-fault-pass-through enable	Configure LFPT

Validation

Cross-connect using Dynamic LAG on Node-1

```
Node-1#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: LayeNode-2
  Admin Key: 0100 - Oper Key 0100
     Link: ce29 (5073) sync: 1
     Link: ce30 (5074) sync: 1
-------------------------------------
  Aggregator po300 100300
  Aggregator Type: LayeNode-2
  Admin Key: 0300 - Oper Key 0300
     Link: ce6/1 (5005) sync: 1
     Link: ce15/1 (5006) sync: 1

Node-1#sh running-config cross-connect
!
cross-connect sample
 ep1 po100 ep2 ce2/1
 cross-connect switchover type revertive
 link-fault-pass-through enable
 backup ep1 po300
 backup ep2 ce4/1
!

Node-1#sh cross-connect
Codes: EP - Endpoint, Bkp_EP - Backup endpoint
       *  - Active Endpoint, none - not configured
Cross-connect name : sample
```

```
EP1:po100      EP2:ce2/1       Revertive:Yes        Bkp_EP1:po300      Bkp_EP2:ce4/1
Admin Status:UP          Oper Status:UP
+=============================================================================================
============================+
| EP      | OVID    | IVID    | Rx packets    | Rx bytes     | Tx packets    |Tx bytes
|Interface Status|
+=============================================================================================
============================+
| EP1*     |     -    |     -    |0              |0              |5974137342
|764688374912   |UP             |
| EP2*    |    -    |    -    |5973605019    |764619747456   |0            |0
|UP             |
| bkp_EP1  |    -    |    -    |5973879754    |764654827904   |0            |0
|UP             |
| bkp_EP2  |    -    |    -    |0             |0             |0             |0
|UP             |
+=============================================================================================
============================+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

Cross-connect using Dynamic LAG on Node-2

```
Node-2#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: LayeNode-2
  Admin Key: 0100 - Oper Key 0100
     Link: ce23 (5067) sync: 1
     Link: ce24 (5068) sync: 1
-------------------------------------
  Aggregator po300 100300
  Aggregator Type: LayeNode-2
  Admin Key: 0300 - Oper Key 0300
     Link: ce21 (5063) sync: 1
     Link: ce22 (5064) sync: 1

Node-2#show running-config cross-connect
!
cross-connect sample2
!
cross-connect sample2
 ep1 po100 ep2 po300
 link-fault-pass-through enable
!

Node-2#sh cross-connect
Codes: EP - Endpoint, Bkp_EP - Backup endpoint
       *  - Active Endpoint, none - not configured
Cross-connect name : sample2
```


© 2021 IP Infusion Inc. Proprietary

```
EP1:po100     EP2:po300      Revertive:No        Bkp_EP1:None      Bkp_EP2:None
Admin Status:UP         Oper Status:UP
+=============================================================================================
============================+
| EP      | OVID    | IVID    | Rx packets    | Rx bytes     | Tx packets    |Tx bytes
|Interface Status|
+=============================================================================================
============================+
| EP1*    |    -    |    -    |3710          |470780        |723           |90626
|UP             |
| EP2*    |    -    |    -    |72            |6468          |14            |1548
|UP             |
+=============================================================================================
============================+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

Cross-connect using Dynamic LAG on Node-3

```
Node-3#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: LayeNode-2
  Admin Key: 0100 - Oper Key 0100
     Link: ce1/1 (5005) sync: 1
     Link: ce2/1 (5006) sync: 1
-------------------------------------
  Aggregator po300 100300
  Aggregator Type: LayeNode-2
  Admin Key: 0300 - Oper Key 0300
     Link: ce13 (5011) sync: 1
     Link: ce14 (5012) sync: 1

Node-3#sh running-config cross-connect
!
cross-connect sample3
 ep1 po300 ep2 ce4/1
 cross-connect switchover type revertive
 link-fault-pass-through enable
 backup ep1 po100
 backup ep2 ce5/1
!

Node-3#sh cross-connect
Codes: EP - Endpoint, Bkp_EP - Backup endpoint
       *  - Active Endpoint, none - not configured
Cross-connect name : sample3
EP1:po300     EP2:ce4/1      Revertive:Yes        Bkp_EP1:po100     Bkp_EP2:ce5/1
Admin Status:UP         Oper Status:UP
```

```
+=============================================================================================
============================+
| EP      | OVID    | IVID    | Rx packets    | Rx bytes     | Tx packets    |Tx bytes
|Interface Status|
+=============================================================================================
============================+
| EP1*     |     -    |     -    |201            |13536          |83318167485
|10664725404928 |UP             |
| EP2*    |    -    |    -    |93501105144    |11968141426060 |2            |128
|UP             |
| bkp_EP1  |     -    |     -    |0              |0              |10171776397
|1301987373312  |UP             |
| bkp_EP2  |    -    |    -    |93501187674    |11968152089344 |0            |0
|UP             |
+=============================================================================================
============================+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

Cross-connect using Dynamic LAG on Node-4

```
Node-4#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: LayeNode-2
  Admin Key: 0100 - Oper Key 0100
     Link: ce1/1 (5005) sync: 1
     Link: ce2/1 (5006) sync: 1
-------------------------------------
  Aggregator po300 100300
  Aggregator Type: LayeNode-2
  Admin Key: 0300 - Oper Key 0300
     Link: ce8/1 (5009) sync: 1
     Link: ce15/1 (5012) sync: 1

Node-4#sh running-config cross-connect
!
 cross-connect sample4
 ep1 po300 ep2 po100
 link-fault-pass-through enable
!
```

Disable the Cross-connect on Node-1

`#configure terminal`	Enter configure mode
`(config)#cross-connect sample`	Enter into cross-connect mode
`(config-XC)#disable`	Disabling the cross-connect
`(config-XC)#exit`	Exit the cross-connect

© 2021 IP Infusion Inc. Proprietary

Validation

Disable the cross-connect on Node-1

```
Node-1#sh cross-connect
Codes: EP - Endpoint, Bkp_EP - Backup endpoint
       *  - Active Endpoint, none - not configured
Cross-connect name : sample
EP1:po100      EP2:ce2/1       Revertive:Yes        Bkp_EP1:po300      Bkp_EP2:ce4/1
Admin Status:DOWN          Oper Status:DOWN
+=============================================================================================
============================+
| EP      | OVID    | IVID    | Rx packets    | Rx bytes     | Tx packets    |Tx bytes
|Interface Status|
+=============================================================================================
============================+
| EP1*     |     -    |     -    |0              |0              |5974137342
|764688374912   |UP             |
| EP2*    |    -    |    -    |5973605019    |764619747456   |0            |0
|UP             |
| bkp_EP1  |    -    |    -    |5973879754    |764654827904   |0            |0
|UP             |
| bkp_EP2  |    -    |    -    |0             |0             |0            |0
|UP             |
+=============================================================================================
============================+


cross-connect summary
Total XC    : 1
Admin Up    : 0
Admin Down  : 1
Total Rules : 0
```

Enable the Cross-connect Node-1

`#configure terminal`	Enter configure mode
`(config)#cross-connect sample`	Enter into cross-connect mode
`(config-XC)#no disable`	Enable the cross-connect
`(config-XC)#exit`	Exit the cross-connect

Validation

Cross-connect after enable on Node-1

```
Node-1#sh cross-connect
Codes: EP - Endpoint, Bkp_EP - Backup endpoint
       *  - Active Endpoint, none - not configured
Cross-connect name : sample
EP1:po100      EP2:ce2/1       Revertive:Yes        Bkp_EP1:po300      Bkp_EP2:ce4/1
Admin Status:UP          Oper Status:UP
+=============================================================================================
============================+
| EP      | OVID    | IVID    | Rx packets    | Rx bytes     | Tx packets    |Tx bytes
|Interface Status|
```

```
+=============================================================================================
============================+
| EP1*     |     -    |     -    |0              |0              |5974137342
|764688374912   |UP             |
| EP2*    |    -    |    -    |5973605019    |764619747456   |0            |0
|UP             |
| bkp_EP1  |    -    |    -    |5973879754    |764654827904   |0            |0
|UP             |
| bkp_EP2  |    -    |    -    |0             |0             |0            |0
|UP             |
+=============================================================================================
============================+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```


© 2021 IP Infusion Inc. Proprietary

Layer 1 Command Reference

Contents

This guide contains these chapters:

- Chapter 1, *Port Based xConnect Commands*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Port Based xConnect Commands

This chapter contains the port based xConnect commands.

- backup
- cross-connect
- cross-connect switchover type revertive
- disable
- ep1 <interface_name> ep2 <interface_name>
- link-fault-pass-through enable
- show cross-connect

© 2021 IP Infusion Inc. Proprietary

backup

Use this command to configure backup for primary endpoints.

Use `no` form of this command to unconfigure backup for primary endpoint.

Command Syntax

```
backup (ep1|ep2) IFNAME
no backup (ep1|ep2)
```

Parameters

`IFNAME`	Interface name for backup endpoint

Default

None

Command Mode

Configure-XC mode

Applicability

This command was introduced in OcNOS-DC version 2.0.

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#backup ep1 xe35

(config-XC)#no backup ep1
```


© 2021 IP Infusion Inc. Proprietary

cross-connect

Use this command to provide name for a xConnect. This command will change mode from config to cross-connect mode.

Command Syntax

```
cross-connect <xc-name>
```

Parameters

xc-name	Cross-connect name

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-DC version 2.0

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#
```

cross-connect switchover type revertive

Use this command to configure revertive mode for cross-connect.

Use the no form of this command to make it non-revertive mode for cross-connect.

Command Syntax

```
cross-connect switchover type revertive
no cross-connect switchover type revertive
```

Parameters

None

Default

Non-revertive by default.

Command Mode

Configure-XC mode

Applicability

This command was introduced in OcNOS-DC version 2.0.

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#cross-connect switchover type revertive
(config-XC)#no cross-connect switchover type revertive
```


© 2021 IP Infusion Inc. Proprietary

disable

Use this command to do admin shutdown on a cross-connect.

Use the `no` form of this command to enable cross-connect.

Command Syntax

```
disable
no disable
```

Parameters

None

Default

By default, the cross-connect will be enabled.

Command Mode

Configure-XC mode

Applicability

This command was introduced in OcNOS-DC version 2.0

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#disable
(config-XC)#no disable
```

ep1 <interface_name> ep2 <interface_name>

Use this command to configure xConnect between two endpoints.

Command Syntax

```
ep1 IFNAME1 ep2 IFNAME2
```

Parameters

IFNAME1	Interface name for ep1
IFNAME2	Interface name for ep2

Default

None

Command Mode

Configure-XC mode

Applicability

This command was introduced in OcNOS-DC version 2.0.

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#ep1 xe33 ep2 xe34
```


© 2021 IP Infusion Inc. Proprietary

link-fault-pass-through enable

Use this command to enable LFPT in the cross-connect.

Use the `no` form of this command to disable LFPT.

Command Syntax

```
link-fault-pass-through enable
no link-fault-pass-through enable
```

Parameters

None

Default

LFPT is disabled by default.

Command Mode

Configure-XC mode

Applicability

This command was introduced in OcNOS-DC version 2.0.

Example

```
#configure terminal
(config)#cross-connect temp
(config-XC)#link-fault-pass-through enable
(config-XC)#no link-fault-pass-through enable
```

show cross-connect

Use this command to show cross-connect entry.

Command Syntax

```
show cross-connect (name WORD| count|)
```

Parameters

WORD	Cross-connect name
count	Cross-connect count

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-DC version 2.0.

Example

```
OcNOS#sh cross-connect

Cross-connect name : temp
EP1:ce13/1     EP2:ce4/1      Revertive:No         Bkp_EP1:ce14/1     Bkp_EP2:ce15/1
Admin Status:UP          Oper Status:UP
+=============================================================================================
============================+
| EP      | OVID    | IVID    | Rx packets    | Rx bytes     | Tx packets    |Tx bytes
|Interface Status|
+=============================================================================================
============================+
| EP1*    |    -    |    -    |177629        |12078772      |0              |0
|UP             |
| EP2*    |    -    |    -    |0             |0             |177633         |12079044
|UP             |
| bkp_EP1 |    -    |    -    |0             |0             |0              |0
|UP             |
| bkp_EP2 |    -    |    -    |0             |0             |0              |0
|UP             |
+=============================================================================================
============================+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```


© 2021 IP Infusion Inc. Proprietary

```
OcNOS#sh cross-connect temp

Cross-connect name : temp
EP1:ce13/1     EP2:ce4/1      Revertive:No         Bkp_EP1:ce14/1     Bkp_EP2:ce15/1
Admin Status:UP          Oper Status:UP
+=============================================================================================
============================+
| EP      | OVID    | IVID    | Rx packets    | Rx bytes     | Tx packets    |Tx bytes
|Interface Status|
+=============================================================================================
============================+
| EP1*    |    -    |    -    |177629        |12078772      |0              |0
|UP             |
| EP2*    |    -    |    -    |0             |0             |177633         |12079044
|UP             |
| bkp_EP1 |    -    |    -    |0             |0             |0              |0
|UP             |
| bkp_EP2 |    -    |    -    |0             |0             |0              |0
|UP             |
+=============================================================================================
============================+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1

OcNOS#sh cross-connect count
cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

© 2021 IP Infusion Inc. Proprietary

SECTION 5 # Layer 2

Layer 2 Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *802.1X Configuration*
- Chapter 2, *Disabling Native VLAN Configuration*
- Chapter 3, *Disable Spanning Tree Configuration*
- Chapter 4, *Layer 2 Control Protocols Tunneling*
- Chapter 5, *Link Aggregation Configuration*
- Chapter 6, *Link Layer Discovery Protocol Configuration*
- Chapter 7, *MC-LAG Configuration*
- Chapter 8, *MSTP Configuration*
- Chapter 9, *Port Security Configuration*
- Chapter 10, *RPVST+ Configuration*
- Chapter 11, *RSTP Configuration*
- Chapter 12, *Spanning Tree Protocol Configuration*
- Chapter 13, *VLAN Configuration*
- Chapter 14, *VLAN Cross-Connect (XC)*
- Chapter 15, *Unidirectional Link Detection Configuration*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 802.1X Configuration

IEEE 802.1x restricts unauthenticated devices from connecting to a switch. Only after authentication is successful, traffic is allowed through the switch.

Topology

In this example, a radius server keeps the client information, validating the identity of the client and updating the switch about the authentication status of the client. The switch is the physical access between the two clients and the server. It requests information from the client, relays information to the server and then back to the client. To configure 802.1x authentication, enable authentication on ports eth1 and eth and specify the radius server IP address and port.

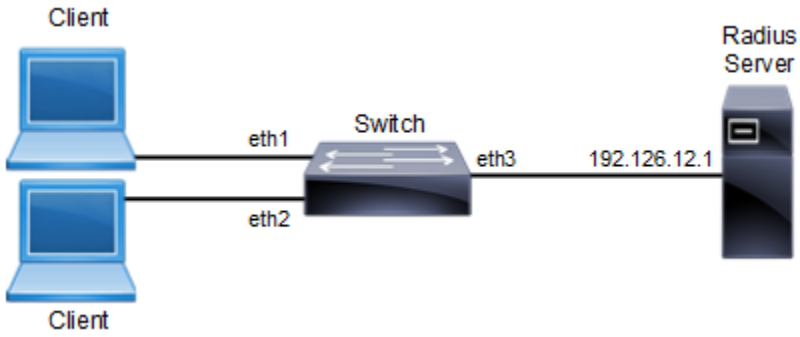


Figure 1-51: 802.1x Topology

Switch Configuration

`Switch#configure terminal`	Enter configure mode.
`Switch(config)# port-security disable`	Disable the port-security.
`Switch(config)#dot1x system-auth-ctrl`	Enable authentication globally.
`Switch(config)#interface eth2`	Enter interface mode.
`Switch(config)#switchport`	Enable switch port on interface.
`Switch(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (eth2).
`Switch(config-if)#exit`	Exit interface mode.
`Switch(config)#interface eth1`	Enter interface mode.
`Switch(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (eth1).
`Switch(config-if)#exit`	Exit interface mode.
`Switch(config)# radius-server dot1x host 192.126.12.1 key 0 testing124`	Specify the host IP and key with string name between radius server and client
`Switch(config)#interface eth3`	Enter interface mode.
`Switch(config-if)#ip address 192.126.12.2/24`	Set the IP address on interface eth3.

Validation

```
#show dot1x all
802.1X Port-Based Authentication Enabled RADIUS server address: 192.168.1.1:60000 Next radius message id: 147
```

© 2021 IP Infusion Inc. Proprietary1087

802.1X Configuration
RADIUS client address: not configured 802.1X info for interface eth1
portEnabled: true - portControl: Auto portStatus: Unauthorized - currentId: 29 protocol version: 2
reAuthenticate: disabled reAuthPeriod: 3600
abort:F fail:F start:F timeout:F success:F PAE: state: Connecting - portMode: Auto PAE: reAuthCount: 1 - rxRespId: 0
PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30 BE: state: Idle - reqCount: 0 - idFromServer: 0 BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in - operControlledDirections: in CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false

802.1X info for interface eth2 portEnabled: true - portControl: Auto portStatus: Unauthorized - currentId: 29 protocol version: 2
reAuthenticate: disabled reAuthPeriod: 3600
abort:F fail:F start:F timeout:F success:F PAE: state: Connecting - portMode: Auto PAE: reAuthCount: 1 - rxRespId: 0
PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30 BE: state: Idle - reqCount: 0 - idFromServer: 0 BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in - operControlledDirections: in CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
#show dot1x
802.1X Port-Based Authentication Enabled RADIUS server address: 192.168.1.1:60000 Next radius message id: 147
RADIUS client address: not configured

 © 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Disabling Native VLAN Configuration

This chapter contains sample configurations to check the functionality to drop the untagged traffic by disblaing the native vlan by configuring acceptable-frame-type vlan-tagged.

Topology

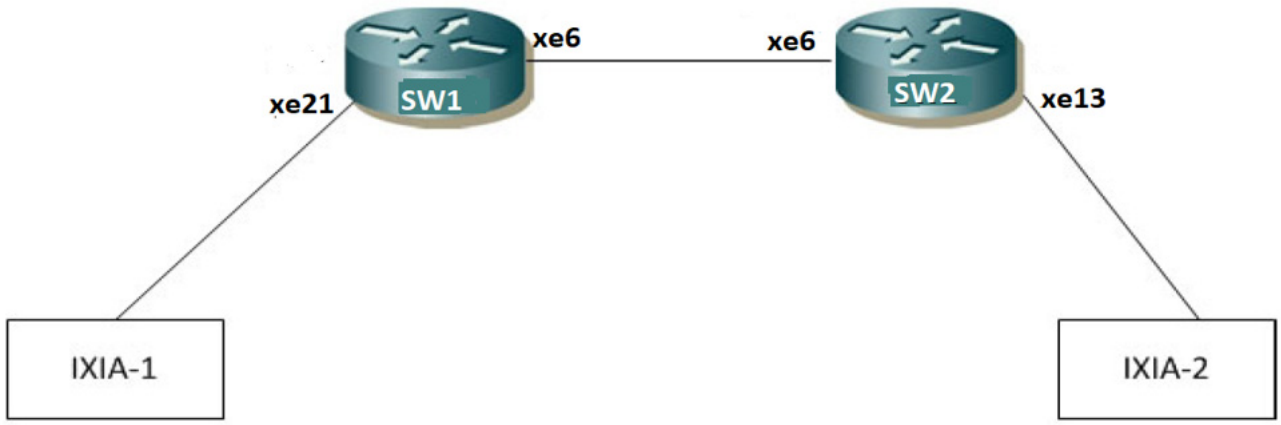


Figure 2-52: Native VLAN Topology

Configuration

SW1

`SW1#configure terminal`	Enter configuration mode
`SW1(config)# bridge 1 protocol rstp vlan-bridge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2-10 bridge 1 state enable`	Create 2-10 vlans
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface xe6`	Enter interface configuration mode for xe6
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode hybrid`	Configure port mode as hybrid
`SW1(config-if)# switchport hybrid allowed vlan all`	Allow all the vlans on the xe6 port
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#interface xe21`	Enter interface configuration mode for xe21
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1

© 2021 IP Infusion Inc. Proprietary

`SW1(config-if)#switchport mode hybrid`	Configure port mode as hybrid
`SW1(config-if)# switchport hybrid allowed vlan all`	Allow all the vlans on the xe21 port
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#commit`	Commit the candidate configuration to the running configuration

SW2

`SW2#configure terminal`	Enter configuration mode
`SW2(config)# bridge 1 protocol rstp vlan-bridge`	Create bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 2-10 bridge 1 state enable`	Create 2-10 vlans
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface xe6`	Enter interface configuration mode for xe6
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode hybrid`	Configure port mode as hybrid
`SW2(config-if)# switchport hybrid allowed vlan all`	Allow all the vlans on the xe6 port
`SW2(config-if)#exit`	Exit from interface mode
`SW2(config)#interface xe13`	Enter interface configuration mode for xe13
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode hybrid`	Configure port mode as hybrid
`SW2(config-if)# switchport hybrid allowed vlan all`	Allow all the vlans on the xe13 port
`SW2(config-if)#exit`	Exit from interface mode
`SW2(config)#commit`	Commit the candidate configuration to the running configuration

Validation

Without configuring acceptable-frame-type vlan-tagged

Sending untagged, vlan-5 and vlan-6 traffic from ixia-1 to ixia-2. In the show bridge o/p we can see all the mac entries learnt for all the traffics.

In the show vlan brief output for default vlan interface xe21 is having port type as untagged (u).

```
SW1#show bridge
bridge 1 is running on rstp vlan-bridge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
```


© 2021 IP Infusion Inc. Proprietary

```
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe21        0000.0000.0003    1     300
 1         5                   xe21        0000.0000.0005    1     300
 1         6                   xe21        0000.0000.0006    1     300

SW1#sh int counters rate mbps
+------------------+-------------+------------+-------------+------------+
|     Interface    |    Rx mbps  |    Rx pps  |    Tx mbps  |    Tx pps  |
+------------------+-------------+------------+-------------+------------+
 ce53                0.00          0            0.00          0
 xe6                 0.00          0            2960.63       246719
 xe8                 0.00          0            0.00          0
 xe9                 0.00          0            0.00          0
 xe21                2960.63       246719       0.00          0

SW1#sh vlan brief
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Success    xe6(u) xe21(u)
1       2       VLAN0002         ACTIVE  Success    xe6(t) xe21(t)
1       3       VLAN0003         ACTIVE  Success    xe6(t) xe21(t)
1       4       VLAN0004         ACTIVE  Success    xe6(t) xe21(t)
1       5       VLAN0005         ACTIVE  Success    xe6(t) xe21(t)
1       6       VLAN0006         ACTIVE  Success    xe6(t) xe21(t)
1       7       VLAN0007         ACTIVE  Success    xe6(t) xe21(t)
1       8       VLAN0008         ACTIVE  Success    xe6(t) xe21(t)
1       9       VLAN0009         ACTIVE  Success    xe6(t) xe21(t)
1       10      VLAN0010         ACTIVE  Success    xe6(t) xe21(t)
```

Configuring acceptable-frame-type vlan-tagged on ingress interface

SW1

`SW1(config)#interface xe21`	Enter interface configuration mode for xe21
`SW1(config-if)# switchport mode hybrid acceptable-frame-type vlan-tagged`	Configure acceptable-frame-type vlan-tagged
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#commit`	Commit the candidate configuration to the running configuration

Validation

After configuring acceptable-frame-type vlan-tagged, In the show bridge o/p we can see that un-tagged traffic is dropped (.0003 mac entry is not present), and traffic also getting dropped for that specific stream.

Now on show vlan brief output we can see that xe21 interface is having port type as tagged (t).

```
SW1#sh vlan brief
bridge 1 is running on rstp vlan-bridge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1         1                   xe21         0000.0000.0001    1     300
 1         5                   xe21         0000.0000.0005    1     300
SW1#sh int counters rate mbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+--------------------+--------------+-------------+--------------+-------------+
 ce53                 0.00           0             0.00           0
 xe6                  0.00           0             1971.13        164480
 xe8                  0.00           0             0.00           0
 xe9                  0.00           0             0.00           0
 xe21                 2960.64        246720        0.00           0

SW1#sh vlan brief
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ============================
1       1       default          ACTIVE  Success    xe6(u) xe21(t)
1       2       VLAN0002         ACTIVE  Success    xe6(t) xe21(t)
1       3       VLAN0003         ACTIVE  Success    xe6(t) xe21(t)
1       4       VLAN0004         ACTIVE  Success    xe6(t) xe21(t)
1       5       VLAN0005         ACTIVE  Success    xe6(t) xe21(t)
1       6       VLAN0006         ACTIVE  Success    xe6(t) xe21(t)
1       7       VLAN0007         ACTIVE  Success    xe6(t) xe21(t)
1       8       VLAN0008         ACTIVE  Success    xe6(t) xe21(t)
1       9       VLAN0009         ACTIVE  Success    xe6(t) xe21(t)
1       10      VLAN0010         ACTIVE  Success    xe6(t) xe21(t)
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 Disable Spanning Tree Configuration

This chapter describes disabling spanning tree operation on a per Multiple Spanning Tree Instance (MSTI) basis.

Topology

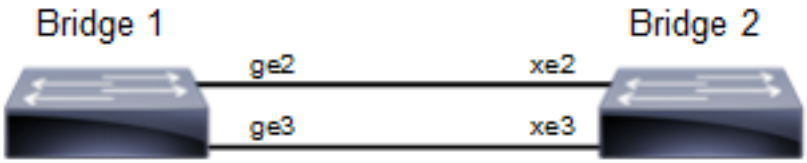


Figure 3-53: Disable Spanning Tree Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Disabling MSTP Configuration

Bridge 1

Disabling MSTP per instance

`Bridge1(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 2
`Bridge1(config-mst)#no bridge 1 instance 3`	Disable spanning tree for MSTP on instance 3

Disabling MSTP globally

`Bridge1(config)#no bridge 1 multiple-spanning-tree enable bridge-forward`	Disable spanning tree globally for MSTP and keeping the ports in forwarding state.

Disabling MSTP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for MSTP and put port on forwarding state. This command disables any type of STP on the port.

Bridge 2

Disabling MSTP per instance

`Bridge2(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 2
`Bridge2(config-mst)#no bridge 1 instance 3`	Disable spanning tree for MSTP on instance 3

© 2021 IP Infusion Inc. Proprietary

Disabling MSTP globally

`Bridge2(config)#no bridge 1 multiple-spanning-tree enable bridge-forward`	Disable spanning tree globally for MSTP.

Disabling MSTP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for MSTP and put port on forwarding state. This command disables any type of STP on the port.

Validation

Bridge 1

Verify MSTP details with the `show spanning-tree mst detail` command.

```
#show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 905 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 80003417ebfbe9c4
% 1: CIST Reg Root Id 80003417ebfbe9c4
% 1: CIST Bridge Id 800064006ac779a0
% 1: 9 topology change(s)  - last topology change Thu Nov 17 15:06:17 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport -
State Forwarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge2: Designated Port Id 0x838a - CIST Priority 128  -
%   ge2: CIST Root 80003417ebfbe9c4
%   ge2: Regional Root 80003417ebfbe9c4
%   ge2: Designated Bridge 80003417ebfbe9c4
%   ge2: Message Age 0 - Max Age 20
%   ge2: CIST Hello Time 2 - Forward Delay 15
%   ge2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   ge2: forward-transitions 1
%   ge2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Alternate -
State Discarding
%   ge3: Designated External Path Cost 0 -Internal Path Cost 20000
```


© 2021 IP Infusion Inc. Proprietary

```
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge3: Designated Port Id 0x838b - CIST Priority 128  -
%   ge3: CIST Root 80003417ebfbe9c4
%   ge3: Regional Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: CIST Hello Time 2 - Forward Delay 15
%   ge3: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change
timer 0
%   ge3: forward-transitions 2
%   ge3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 20000 -MSTI Root Port 5001 - MSTI Bridge Priority
32768
% 1: MSTI Root Id 80023417ebfbe9c4
% 1: MSTI Bridge Id 800264006ac779a0
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport -
State Forwarding
%   ge2: Designated Internal Path Cost 0  - Designated Port Id 0x838a
%   ge2: Configured Internal Path Cost 20000
%   ge2: Configured CST External Path cost 20000
%   ge2: CST Priority 128  - MSTI Priority 128
%   ge2: Designated Root 80023417ebfbe9c4
%   ge2: Designated Bridge 800264006ac779a0
%   ge2: Message Age 0
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0

% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800364006ac779a0
% 1: MSTI Bridge Id 800364006ac779a0
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated -
State Forwarding
%   ge3: Designated Internal Path Cost 0  - Designated Port Id 0x838c
%   ge3: Configured Internal Path Cost 20000
%   ge3: Configured CST External Path cost 20000
%   ge3: CST Priority 128  - MSTI Priority 128
%   ge3: Designated Root 800364006ac779a0
%   ge3: Designated Bridge 800364006ac779a0
%   ge3: Message Age 0
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
```

Verify MSTP configurations when MSTP is enabled globally.

```
#show running-config
!
bridge 1 protocol mstp
```

```
!
```

Verify MSTP configurations when MSTP is disabled globally.

```
#show running-config
!
bridge 1 protocol mstp
no bridge 1 multiple-spanning-tree enable bridge-forward
!
```

Verify MSTP configurations when MSTP instance 2 and 3 is enabled.

```
#show running-config spanning-tree
!
spanning-tree mst configuration
bridge 1  instance 2
bridge 1  instance 2 vlan 2
bridge 1  instance 3
bridge 1  instance 3 vlan 3
!
interface xe2
bridge-group 1 instance 2
!
interface xe3
bridge-group 1 instance 3
!
```

- Verify MSTP configurations when MSTP instance 2 is disabled

```
#show running-config spanning-tree
!
spanning-tree mst configuration
bridge 1 instance 3
bridge 1 instance 3 vlan 3
!
interface ge3
bridge-group 1 instance 3
!
```

Verify MSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode access
switchport access vlan 2
bridge-group 1 instance 2
!
```

Verify MSTP configurations when spanning-tree is disabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode access
switchport access vlan 2
bridge-group 1 instance 2
```

 © 2021 IP Infusion Inc. Proprietary

Verify MSTP details after disabling spanning-tree on interface ge2 with the `show spanning-tree mst details` command.

```
#show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 908 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 80003417ebfbe9c4
% 1: CIST Reg Root Id 80003417ebfbe9c4
% 1: CIST Bridge Id 800064006ac779a0
% 1: 10 topology change(s)  - last topology change Fri Nov 25 21:21:05 2016

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Forwarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge2: Designated Port Id 0x838a - CIST Priority 128  -
%   ge2: Message Age 0 - Max Age 20
%   ge2: CIST Hello Time 2 - Forward Delay 15
%   ge2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   ge2: forward-transitions 2
%   ge2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport -
State Forwarding
%   ge3: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge3: Designated Port Id 0x838b - CIST Priority 128  -
%   ge3: CIST Root 80003417ebfbe9c4
%   ge3: Regional Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: CIST Hello Time 2 - Forward Delay 15
%   ge3: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change
timer 0
%   ge3: forward-transitions 3
%   ge3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
```

```
% 1: MSTI Root Id 800264006ac779a0
% 1: MSTI Bridge Id 800264006ac779a0
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Discarding
%   ge2: Designated Internal Path Cost 0  - Designated Port Id 0x8389
%   ge2: Configured Internal Path Cost 20000
%   ge2: Configured CST External Path cost 20000
%   ge2: CST Priority 128  - MSTI Priority 128
%   ge2: Designated Root 800264006ac779a0
%   ge2: Designated Bridge 800264006ac779a0
%   ge2: Message Age 0
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 20000 -MSTI Root Port 5004 - MSTI Bridge Priority
32768
% 1: MSTI Root Id 80033417ebfbe9c4
% 1: MSTI Bridge Id 800364006ac779a0
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport -
State Forwarding
%   ge3: Designated Internal Path Cost 0  - Designated Port Id 0x838b
%   ge3: Configured Internal Path Cost 20000
%   ge3: Configured CST External Path cost 20000
%   ge3: CST Priority 128  - MSTI Priority 128
%   ge3: Designated Root 80033417ebfbe9c4
%   ge3: Designated Bridge 800364006ac779a0
%   ge3: Message Age 0
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1
```

STP Configuration

Bridge 1

Disabling STP globally

`Bridge1(config)#no bridge 1 spanning-tree enable bridge-forward`	Disable spanning tree globally for STP.

Disabling STP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for STP and put port on forwarding state. This command disables any type of STP on the port.

© 2021 IP Infusion Inc. Proprietary

Bridge 2

Disabling STP globally

`Bridge2(config)#no bridge 1 spanning-tree enable bridge-forward`	Disable spanning tree globally for STP.

Disabling STP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for STP and put port on forwarding state. This command disables any type of STP on the port.

Validation

Bridge 1

Verify STP details when stp is enabled globally and ge2 and ge3 are part of the bridge using the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled - topology change
% 1: Root Path Cost 4 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Root port 905
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: 3 topology changes - last topology change Tue Nov 15 21:33:53 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec

%ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 -
designated cost 0
%ge2: Designated Port Id 0x838a - state Forwarding -Priority 128
%ge2: Designated root 80003417ebfbe9c4
%ge2: Designated Bridge 80003417ebfbe9c4
%ge2: Message Age 0 - Max Age 20
%ge2: Hello Time 2 - Forward Delay 15
%ge2: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 1 - topo change  timer0
%ge2: forward-transitions 1
%ge2: No portfast configured – Current  portfast
%ge2: bpdu-guard default- Current bpdu-guard off
%ge2: bpdu-filter default- Current bpdu-filter off
%ge2: no root guard configured- Current root guard off
%ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - path cost 4 -
designated cost 0
%ge3: Designated Port Id 0x838b - state Blocked -Priority 128
%ge3: Designated root 80003417ebfbe9c4
%ge3: Designated Bridge 80003417ebfbe9c4
%ge3: Message Age 0 - Max Age 20
%ge3: Hello Time 2 - Forward Delay 15
%ge3: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 1 - topo change timer0
```

```
%ge3: forward-transitions 0
%ge3: No portfast configured - Currentportfast off
%ge3: bpdu-guarddefault- Current bpdu-guard off
%ge3: bpdu-filter default- Current bpdu-filter off
%ge3: no root guard configured- Current root guard off
%
```

Verify STP configurations when STP is enabled globally.

```
#show running-config
!
bridge 1 protocol ieee vlan-bridge
!
```

Verify STP configurations when STP is disabled globally.

```
#show running-config
!
bridge 1 protocol ieee vlan-bridge
no bridge 1 spanning-tree enable bridge-forward
!
```

Verify STP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
!
```

Verify STP configurations when spanning-tree is disabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode trunk
switchport trunk allowed vlan all
!
```

Verify STP details after disabling spanning-tree on interface ge2 with the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 4 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Root port 908
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: 5 topology changes - last topology change Fri Nov 25 21:15:35 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 -
designated cost 0
%   ge2: Designated Port Id 0x838a - state Disabled -Priority 128
%   ge2: Message Age 0 - Max Age 20
%   ge2: Hello Time 2 - Forward Delay 15
```

 © 2021 IP Infusion Inc. Proprietary

```
%   ge2: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change
timer 23
%   ge2: forward-transitions 2
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - path cost 4 -
designated cost 0
%   ge3: Designated Port Id 0x838b - state Forwarding -Priority 128
%   ge3: Designated root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 1 - topo change
timer 23
%   ge3: forward-transitions 2
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
```

RSTP Configuration

Bridge 1

Disabling RSTP globally

`Bridge1(config)#no bridge 1 rapid-spanning-tree enable bridge-forward`	Disable spanning tree globally for RSTP.

Disabling RSTP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for RSTP and put port on forwarding state. This command disables any type of STP on the port.

Bridge 2

Disabling RSTP globally

`Bridge2(config)#no bridge 1 rapid-spanning-tree enable bridge-forward`	Disable spanning tree globally for RSTP.

Disabling RSTP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for RSTP and put port on forwarding state. This command disables any type of STP on the port.

Validation

Bridge 1

Verify RSTP details when rstp is enabled globally and ge2 and ge3 are part of the bridge using the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled- topology change detected
% 1: Root Path Cost 20000 - Root Port 905 -Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: last topology change Tue Nov 15 21:44:31 2016
% 1: 7 topology change(s)- last topology change Tue Nov 15 21:44:31 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State
Forwarding
% ge2: Designated Path Cost 0
% ge2: Configured Path Cost 20000- Add type Explicit ref count 1
% ge2: Designated Port Id 0x838a - Priority 128-
% ge2: Root 80003417ebfbe9c4
% ge2: Designated Bridge 80003417ebfbe9c4
% ge2: Message Age 0 - Max Age 20
% ge2: Hello Time 2 - Forward Delay 15
% ge2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer
0
% ge2: forward-transitions 1
% ge2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge2: No portfast configured - Currentportfast off
% ge2: bpdu-guarddefault- Current bpdu-guard off
% ge2: bpdu-filter default- Current bpdu-filter off
% ge2: no root guard configured- Current root guard off
% ge2: Configured Link Type point-to-point - Current point-to-point
% ge2: No auto-edge configured - Current port Auto Edge off
% ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Alternate -
State Discarding
% ge3: Designated Path Cost 0
% ge3: Configured Path Cost 20000- Add type Explicit ref count 1
% ge3: Designated Port Id 0x838b - Priority 128-
% ge3: Root 80003417ebfbe9c4
% ge3: Designated Bridge 80003417ebfbe9c4
% ge3: Message Age 0 - Max Age 20
% ge3: Hello Time 2 - Forward Delay 15
% ge3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer
```


© 2021 IP Infusion Inc. Proprietary

```
0
% ge3: forward-transitions 2
% ge3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge3: No portfast configured - Currentportfast off
% ge3: bpdu-guarddefault- Current bpdu-guard off
% ge3: bpdu-filter default- Current bpdu-filter off
% ge3: no root guard configured- Current root guard off
% ge3: Configured Link Type point-to-point - Current point-to-point
% ge3: No auto-edge configured - Current port Auto Edge off
%
```

Verify RSTP configurations when RSTP is enabled globally.

```
#show running-config
!
bridge 1 protocol rstp vlan-bridge
!
```

- Verify RSTP configurations when RSTP is disabled globally

```
#show running-config
!
bridge 1 protocol rstp vlan-bridge
no bridge 1 rapid-spanning-tree enable bridge-forward
!
```

Verify RSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
!
```

Verify RSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode trunk
switchport trunk allowed vlan all
```

Verify RSTP details after disabling spanning-tree on interface ge2 with the `show spanning-tree` command.

```
#sh spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 20000 - Root Port 908 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: last topology change Fri Nov 25 21:08:56 2016
% 1: 11 topology change(s)  - last topology change Fri Nov 25 21:08:56 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
```

```
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Forwarding
%   ge2: Designated Path Cost 0
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge2: Designated Port Id 0x838a - Priority 128  -
%   ge2: Message Age 0 - Max Age 20
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer
0
%   ge2: forward-transitions 2
%   ge2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport -
State Forwarding
%   ge3: Designated Path Cost 0
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge3: Designated Port Id 0x838b - Priority 128  -
%   ge3: Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change timer
0
%   ge3: forward-transitions 3
%   ge3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off
```

 © 2021 IP Infusion Inc. Proprietary

CHAPTER 4 Layer 2 Control Protocols Tunneling

Overview

The Layer 2 Control Protocols (L2CP) processing specified here is based largely on the IEEE 802.1Q specification for handling L2CP Frames, i.e. if they should be forwarded, peered, or discarded.

IEEE 802.1Q provides a mechanism for separating the Layer2 control plane into multiple customer and provider control planes. It allows a certain layer 2 control protocol to operate only within a provider network, or to allow interaction between the customer and the provider network, or to pass transparently through a provider network with complete isolation from other customer networks.

In case of non-PB case, packet is forwarded without changing any MAC.

L2CP Tunneling for Provider Bridging

L2CP tunneling provides support for tunneling control plane frames between CE nodes.

In the context of PB, a L2CP frame is defined as any frame containing a destination MAC address as 01:00:0C:CD:CD:D0 or 01:04:DF:CD:CD:D0 (which can be changed via CLI)

When control frames received at CEP port of a PE bridge, predefined multicast address (01-00-C2-CD-CD-D0) is replaced as destination for tunneling the packets across service provider network. If control packets are customer vlan tagged or untagged, then PE bridge will append corresponding service vlan tag to the control packet as per registration table / vlan translation table mapped to the port and send it across the service provider as a data packet.

When tunneled control packet with multicast address (01-00-C2-CD-CD-D0) received on PNP port, the multicast address is replaced with corresponding control packet multicast address and cvlan/svlan removal or update is done as per registration table / vlan translation table.

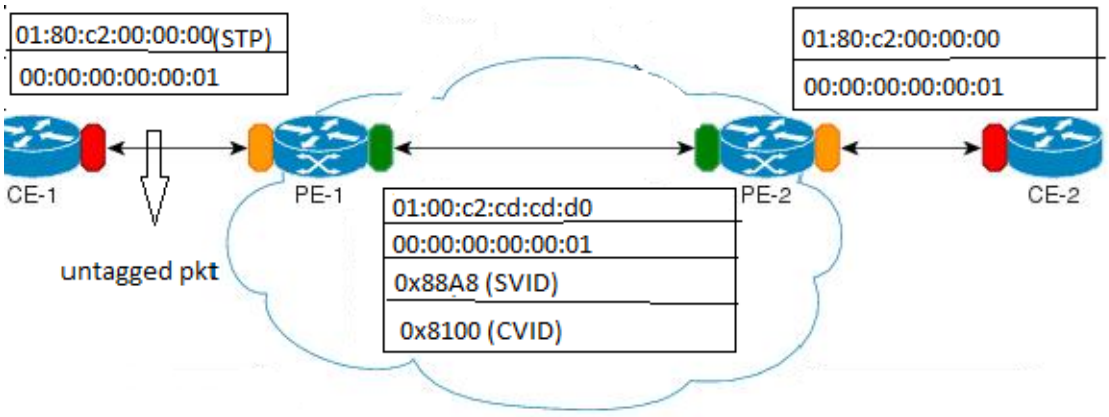


Figure 4-54: L2CP tunneling for provider bridging

L2CP Tunneling for VPLS/VPWS/Hybrid (Bridge+VPWS)

L2CP tunneling provides support for tunneling Control plane frames across L2VPN.

Default Behavior

If control packets are received at the PE router on AC port (vlan tagged/untagged), corresponding AC port properties will take care of forwarding to peer PE node. These packets are encapsulated with MPLS headers and sent across the network to the remote PE router. The egress PE router receives the packet and performs MPLS decapsulation and forwards to the CE. Except for LACP, all other control packets are tunnels across the MPLS circuit.

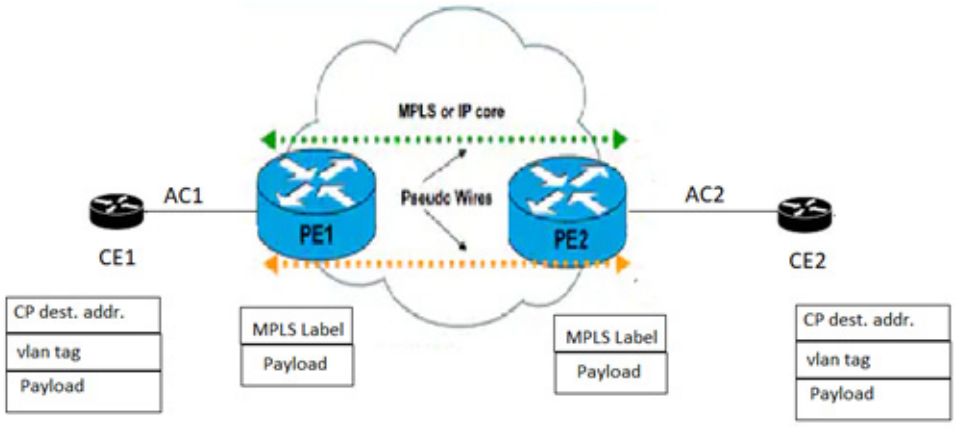


Figure 4-55: L2CP tunneling for VPLS/VPWS/Hybrid (bridge+VPWS)

Hybrid Port

When the incoming port is configured as Hybrid (Bridge+L2VPN), L2CP switches to peering mode. You can override this behavior with the help of L2CP configurations.

L2CP Behavior

The action taken for a given L2CP Frame at a given L2CP Decision Point depends upon the Destination Address within the frame, and upon the configured values of the L2CP Service Attributes.

The three possible actions at an L2CP Decision Points are: Discard, Peer, or Pass/Tunnel.

Discard	The L2CP frame is neither peered nor forwarded.
Peer	The L2CP frame will be processed.
Pass/Tunnel	Pass (or forwarded) means that the frame will be passed transparently in the same way as normal data frames.

© 2021 IP Infusion Inc. Proprietary

Default L2CP configuration

Default L2CP decision in Provider Bridging case:

Table 4-88: Default L2CP decision for Provider Bridging

Protocol Type	L2CP destination address	Ethertype/subtype	Default L2CP action
STP(Spanning Tree Protocols)	01-80-c2-00-00-00	N/A	PEER
SYNCE (Synchronous Ethernet)	01-80-c2-00-00-02	ethertype 0x8809 and subtype 0xE	PEER
LACP (Link Aggregation Control Protocol)	01-80-c2-00-00-02	ethertype 0x8809 and subtype 0x1 or 0x2	PEER
DOT1X (Port Authentication (802.1 X))	01-80-c2-00-00-03	N/A	PEER
LLDP (Link layer discovery protocol)	01-80-c2-00-00-0e	ethertype 0x88CC	PEER
EFM (Ethernet first mile (Link OAM))	01-80-c2-00-00-02	ethertype 0x8809 and subtype 0x3	PEER
ELMI (Ethernet Local Management Interface)	01-80-c2-00-00-07	ethertype 0x88EE	PEER

Default L2CP Decision in VPLS/VPWS/Hybrid case:

- For bridged packets in case of hybrid port:

Table 4-89: Default L2CP decision for hybrid port

Protocol Type	L2CP destination address	Default L2CP action
STP(Spanning Tree Protocols)	01-80-c2-00-00-00	PEER
LACP (Link Aggregation Control Protocol)	01-80-c2-00-00-02	PEER
DOT1X (Port Authentication (802.1 X))	01-80-c2-00-00-03	PEER
LLDP (Link layer discovery protocol)	01-80-c2-00-00-0e	PEER
EFM (Ethernet first mile (Link OAM))	01-80-c2-00-00-02	PEER
ELMI (Ethernet Local Management Interface)	01-80-c2-00-00-07	PEER

- For VPLS/VPWS:

Table 4-90: Default L2CP decision for VPLS/VPWS

Protocol Type	L2CP destination address	Default L2CP action
STP(Spanning Tree Protocols)	01-80-c2-00-00-00	TUNEEL
LACP (Link Aggregation Control Protocol)	01-80-c2-00-00-02	PEER
DOT1X (Port Authentication (802.1 X))	01-80-c2-00-00-03	TUNNEL
LLDP (Link layer discovery protocol)	01-80-c2-00-00-0e	TUNNEL
EFM (Ethernet first mile (Link OAM))	01-80-c2-00-00-02	TUNNEL
ELMI (Ethernet Local Management Interface)	01-80-c2-00-00-07	TUNNEL

Operational Concepts and Scenarios

Basic Configuration for L2CP for Hybrid+VPLS

Enabling tunneling at bridged interface:

```
(config-if)#show run in xe10
!
interface xe11
 speed 1g
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 mpls-l2-circuit vc1 service-template svc1

#config ter
#(config)interface xe11
(config-if)# l2protocol stp tunnel
(config-if)#end
```

To display L2CP information:

```
#show l2protocol processing interface xe11
Bridge   Interface Name  Protocol     Processing Status     Hardware Status
======   ==============  ========     =================     ===============
-        xe12             stp          Tunnel                Tunnel
-        xe12             lacp         None                  Peer
-        xe12             dot1x        None                  Peer
-        xe12             lldp         None                  Peer
-        xe12             efm          None                  Peer
```


© 2021 IP Infusion Inc. Proprietary

```
-        xe12             elmi         None                  Peer

(config)#in xe11
(config-if)#no l2protocol stp
(config-if)#end
#show l2protocol processing interface xe12
Bridge   Interface Name  Protocol     Processing Status     Hardware Status
======   ==============  ========     =================     ===============
-        xe12             stp          None                  Peer
-        xe12             lacp         None                  Peer
-        xe12             dot1x        None                  Peer
-        xe12             lldp         None                  Peer
-        xe12             efm          None                  Peer
-        xe12             elmi         None                  Peer
```

Note: If the configuration is not done, hardware status shows the default values while the configured will be none. On configuring L2CP on interface, configured and hardware status will be same.

Basic Configuration for L2CP in VPLS

Enabling tunneling at ingress VPLS interface:

```
#show run in xe12
!
interface xe12
 speed 1g
 mpls-l2-circuit vc1 service-template svc1
!
#config ter
#(config)interface xe12
```

To display L2CP information:

```
#show l2protocol processing interface xe12

Bridge   Interface Name  Protocol     Processing Status     Hardware Status
======   ==============  ========     =================     ===============
-        xe12             stp          Discard               Discard
-        xe12             lacp         None                  Peer
-        xe12             dot1x        None                  Tunnel
-        xe12             lldp         None                  Tunnel
-        xe12             efm          None                  Tunnel
-        xe12             elmi         None                  Tunnel
```

Basic Configuration for L2CP on Provider Bridging

Enabling tunneling at interface:

```
(config)#bridge 1 protocol provider-rstp edge
(config)#vlan database
(config-vlan)#vlan 2-10 bridge 1 state enable
```

```
(config-vlan)#vlan 11 type service point-point bridge 1 state enable
(config-vlan)#ex
(config)#cvlan registration table map1 bridge 1
(config-cvlan-registration)#cvlan 2 svlan 11
(config-cvlan-registration)#ex
(config)#interface xe1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode customer-edge hybrid
(config-if)#switchport customer-edge hybrid allowed vlan all
(config-if)#switchport customer-edge vlan registration map1
(config-if)#l2protocol ?
 dot1x  Port Authentication (802.1 X)
 efm    Ethernet first mile (Link OAM)
 elmi   Ethernet local management interface
 lacp   Link Aggregation (LACP)
 lldp   link layer discovery protocol
 stp    Spanning Tree Protocols
 synce  Synchronous Ethernet

(config-if)#l2protocol stp ?
 discard  Discard the protocol data unit
 peer     Discard the protocol data unit
 tunnel   tunnel

(config-if)#l2protocol stp tunnel
#show running-config interface xe1
!
 interface xe1
 speed 1g
 switchport
 bridge-group 1
 switchport mode customer-edge hybrid
 switchport customer-edge hybrid allowed vlan all
 switchport customer-edge vlan registration map1
 l2protocol stp tunnel
 customer-spanning-tree provider-edge svlan 11 path-cost 128
```

Configuring egress interfaces”

```
(config)#interface xe2
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode provider-network
(config-if)#switchport provider-network allowed vlan all
```

To display L2protocol information:

```
#show l2protocol processing interface xe1
Bridge   Interface Name  Protocol     Processing Status     Hardware Status
```


© 2021 IP Infusion Inc. Proprietary

```
======   ==============  ========     =================     ===============
1        xe1             stp          Tunnel                Tunnel
1        xe1             lacp         Peer                  Peer
1        xe1             dot1x        Peer                  Peer
1        xe1             lldp         Peer                  Peer
1        xe1             efm          Peer                  Peer
1        xe1             elmi         Peer                  Peer
```

To display L2protocol counters:

```
#show l2protocol interface counters
Interface xe0
Tunnel               :  stp                : 45
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 Link Aggregation Configuration

This chapter contains a complete sample Link Aggregation Group configuration.

LACP is based on the 802.3ad IEEE specification. It allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The spanning tree views it as one interface and not as two or three interfaces. When there is a failure in one physical interface, the other interfaces stay up and there is no disruption. Traffic can be load balanced within an LACP trunk group in a controlled manner using the hashing algorithm.The maximum number of physical Ethernet links in a single logical channel depends upon the hardware support.

Note:

- Physical interfaces will inherit the properties of LAG port once it is attached to be part of LAG, irrespective of the configuration present on the physical interface.
- In case of Dynamic and Static LAG, it is possible to move member ports from one LAG to another LAG.
- Configure LAG port as a switch or router port, before adding member ports into it.

Topology

In Figure 5-56, 3 links are configured between the two switches S1 and S2. These three links are assigned the same administrative key (1) so that they aggregate to form a single channel 1. They are viewed by the STP as one interface.



Figure 5-56: LACP Topology

Dynamic LAG Configuration

S1

`S1#configure terminal`	Enter configure mode.
`S1(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge
`S1(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`S1(config)#interface po10`	Enter into port channel interface po10.
`S1(config-if)#switchport`	Configure po10 as a layer 2 port.
`S1(config-if)#bridge-group 1`	Associate bridge to an interface.
`S1(config-if)#switchport mode trunk`	Configure port as a trunk.
`S1(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the po10 interface.
`S1(config-if)#exit`	Exit interface mode.
`S1(config)#interface eth1`	Enter interface mode.

`S1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S1(config-if)#exit`	Exit interface mode.
`S1(config)#interface eth2`	Enter interface mode.
`S1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S1(config-if)#exit`	Exit interface mode.
`S1(config)#interface eth3`	Enter interface mode.
`S1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.

S2

`S2#configure terminal`	Enter configure mode.
`S2(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge
`S2(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`S2(config)#interface po10`	Enter into port channel interface po10.
`S2(config-if)#switchport`	Configure po10 as a layer 2 port.
`S2(config-if)#bridge-group 1`	Associate bridge to an interface.
`S2(config-if)#switchport mode trunk`	Configure port as a trunk.
`S2(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the po10 interface.
`S2(config-if)#exit`	Exit interface mode.
`S2(config)#interface eth2`	Enter interface mode.
`S2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S2(config-if)#exit`	Exit interface mode.
`S2(config)#interface eth3`	Enter interface mode.
`S2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S2(config-if)#exit`	Exit interface mode.
`S2(config)#interface eth4`	Enter interface mode.
`S2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.

© 2021 IP Infusion Inc. Proprietary

Validation

show etherchannel detail, show etherchannel summary, show running-config interface po10, show running-config interface eth1

```
#show etherchannel detail
% Aggregator po10 7
% Aggregator Type: Layer2
%  Mac address: 08:00:27:50:6a:9b
%  Admin Key: 0010 - Oper Key 0010
%  Actor LAG ID- 0x4e20,08-00-27-ab-ea-38,0x000a
%  Receive link count: 3 - Transmit link count: 3
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x4e20,08-00-27-f8-3c-30,0x000a
%   Link: eth1 (3) sync: 1
%   Link: eth2 (4) sync: 1
%   Link: eth3 (5) sync: 1
%   Collector max delay: 5

#show etherchannel summary
% Aggregator po10 7
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
% Aggregator Type: Layer2
%   Link: eth1 (3) sync: 1
%   Link: eth2 (4) sync: 1
%   Link: eth3 (5) sync: 1

#show running-config interface po10
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all

#show running-config interface eth1
!
interface eth1
 channel-group 10 mode active
```

Static LAG Configuration

S1

`S1#configure terminal`	Enter configure mode.
`S1(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge
`S1(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`S1(config)#interface sa10`	Enter into port channel interface sa10.

S1(config-if)#switchport	Configure po10 as a layer 2 port.
S1(config-if)#bridge-group 1	Associate bridge to an interface.
S1(config-if)#switchport mode trunk	Configure port as a trunk.
S1(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the po10 interface.
S1(config-if)#exit	Exit interface mode.
S1(config)#interface eth1	Enter interface mode.
S1(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
S1(config-if)#exit	Exit interface mode.
S1(config)#interface eth2	Enter interface mode.
S1(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
S1(config-if)#exit	Exit interface mode.
S1(config)#interface eth3	Enter interface mode.
S1(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
S1(config-if)#exit	Exit interface mode.

S2

S2#configure terminal	Enter configure mode.
S2(config)# bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge
S2(config)#lacp system-priority 20000	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
S2(config)#interface sa10	Enter into port channel interface po10.
S2(config-if)#switchport	Configure po10 as a layer 2 port.
S2(config-if)#bridge-group 1	Associate bridge to an interface.
S2(config-if)#switchport mode trunk	Configure port as a trunk.
S2(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the po10 interface.
S2(config-if)#exit	Exit interface mode.
S2(config)#interface eth2	Enter interface mode.
S2(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
S2(config-if)#exit	Exit interface mode.
S2(config)#interface eth3	Enter interface mode.
S2(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.

© 2021 IP Infusion Inc. Proprietary

`S2(config-if)#exit`	Exit interface mode.
`S2(config)#interface eth4`	Enter interface mode.
`S2(config-if)#static-channel-group 10`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S2(config-if)#exit`	Exit interface mode.

Validation

```
#show static-channel-group
% Static Aggregator: sa10
% Member status:
   eth1    up
   eth2    up
   eth3    up

#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all


#show running-config interface eth1
!
interface eth1
 static-channel-group 10
```

Static LAG Minimum Link Configuration

Configure the minimum number of ports that must be linked up and bundled in the LACP port channel. We can configure the minimum links range from 2 to 32. If the number of ports aggregated to the port channel is less than the minimum number of links configured, then the port channel enters the Protocol Down because of the minimum link state.

Note: Minimum links should be configured the same on both sides for optimal performance.

Topology

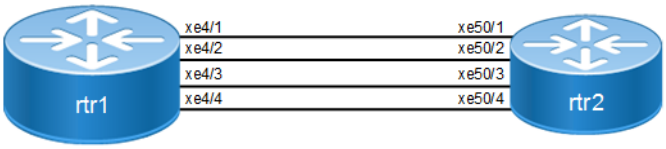


Figure 5-57: LAG Minimum Link

rtr1

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface static-lag sa10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4(range is 2-32)
`(config-if)#exit`	Exit the configure mode

Validation

rtr1

```
#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-Links 4
% Member status:
         xe4/1     up
         xe4/2     up
         xe4/3     up
         xe4/4     up


#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 4
```


© 2021 IP Infusion Inc. Proprietary

rtr2

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface port-channel sa10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#exit`	Exit the configure mode

Validation

rtr2

```
#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 4
!

#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-Links 4
% Member status:
         Xe50/1     up
         Xe50/2     up
         Xe50/3     up
         Xe50/4     up


Note:When a sa goes down due to the minimum links configured (number of
minimum links is greater than the links aggregated to the sa).
Rtr1:
=====
#OcNOS#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
```

```
Interface
-------------------------------------------------------------------------------
--
sa10          AGG    1      trunk              down      PD(Min L/B)   0
OcNOS#

Rtr2:
=====

OcNOS#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


-------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode               Status   Reason  Speed
Interface
-------------------------------------------------------------------------------
--
sa10          AGG    1      trunk              down      PD(Min L/B)   0
OcNOS#
```

Static-LAG Minimum Bandwidth Configuration

Configure the minimum bandwidth allowed for ports that must be linked up and bundled in the LACP port channel. We can configure the minimum bandwidth range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits. If the Total bandwidth of ports aggregated to the port channel is less than the minimum Bandwidth value configured, then the port channel enters the Protocol Down because of the minimum Bandwidth state.

Note: Minimum Bandwidth should be configured the same on both sides for optimal performance.

Topology

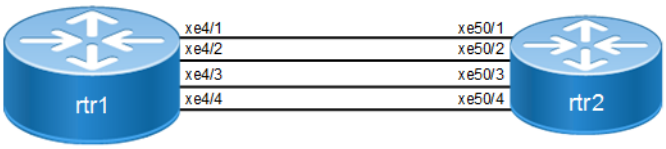


Figure 5-58: LAG Minimum Bandwidth

© 2021 IP Infusion Inc. Proprietary

rtr1

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface static-lag sa10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#exit`	Exit the configure mode

Validation

rtr1

```
#show static-channel-group 10
% Static Aggregator: sa10
% Minimum- 4
% Member status:
         xe4/1     up
         xe4/2     up
         xe4/3     up
         xe4/4     up



#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel load-balance src-dst-mac
 port-channel min-links 40g
```

rtr2

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface port-channel sa10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#exit`	Exit the configure mode

Validation

rtr2

```
#show running-config interface sa10
!
interface sa10
```

```
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-bandwidth 40g
!

#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-bandwidth 40g
% Member status:
         Xe50/1     up
         Xe50/2     up
         Xe50/3     up
         Xe50/4     up
```

Note: When sa goes down due to [Total Bandwidth of sa] <[Minimum Bandwidth value Configured]

```
Rtr1:
=====
#OcNOS #sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel Type PVID Mode              Status   Reason Speed
Interface
--------------------------------------------------------------------------------
--
sa10         AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#
```

Rtr2:

```
=====

OcNOS#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
```


© 2021 IP Infusion Inc. Proprietary

```
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


-------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
-------------------------------------------------------------------------------
--
sa10          AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#

!
```

Dynamic-LAG Minimum Link Configuration

Configure the minimum number of ports that must be linked up and bundled in the LACP port channel. We can configure the minimum links range from 2 to 32. If the number of ports aggregated to the port channel is less than the minimum number of links configured, then the port channel enters the Protocol Down because of the minimum link state.

Note: Minimum links should be configured the same on both sides for optimal performance.

Topology

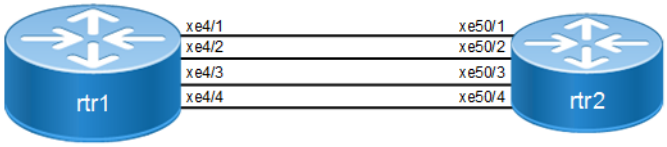


Figure 5-59: LAG Minimum Link

rtr1

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#exit`	Exit the configure mode

Validation

rtr1

```
#sh running-config interface po10

interface po10
```

```
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 4
!

!

#show etherchannel
-------------------------------------
% Lacp Aggregator: po10
% Min-links : 4
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4
-------------------------------------

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
%   Link: xe4/4 (10072) sync: 1
%   Link: xe4/1 (10069) sync: 1
%   Link: xe4/2 (10070) sync: 1
%   Link: xe4/3 (10071) sync: 1
--------------------------------------
```

rtr2

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#exit`	Exit the configure mode

Validation

rtr2

```
#show running-config interface po10
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 4
!

#show etherchannel
```


© 2021 IP Infusion Inc. Proprietary

```
% Lacp Aggregator: po10
% Min-links: 4
% Member:
   xe50/1
   xe50/2
   xe50/3
   xe50/4

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
%   Link: xe50/4 (10072) sync: 1
%   Link: xe50/1 (10069) sync: 1
%   Link: xe50/2 (10070) sync: 1
%   Link: xe50/3 (10071) sync: 1
```

Note: When a PO goes down due to the minimum links configured (number of minimum links is greater than the links aggregated to the PO).

```
Rtr1:
#OcNOS#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po10         AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#


OcNOS#sh etherchannel
% Lacp Aggregator: po10
% Min-links: 4
% Protocol Down (Min L/B): True
% Member:
   xe4/1
```

```
   xe4/2
   xe4/3
   xe4/4
```

Rtr2:

```
OcNOS#sh etherchannel
% Lacp Aggregator: po10
% Min-links: 4
% Protocol Down (Min L/B): True
% Member:
   Xe50/1
   Xe50/2
   Xe50/3
       xe50/4

OcNOS#sh int brief po100

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po10         AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#
```


© 2021 IP Infusion Inc. Proprietary

Dynamic LAG Minimum Bandwidth Configuration

Configure the minimum bandwidth allowed for ports that must be linked up and bundled in the LACP port channel. We can configure the minimum bandwidth range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits. If the Total bandwidth of ports aggregated to the port channel is less than the minimum Bandwidth value configured, then the port channel enters the Protocol Down because of the minimum Bandwidth state.

Note: Minimum Bandwidth should be configured the same on both sides for optimal performance.

Topology

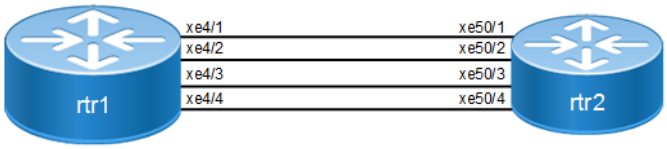


Figure 5-60: LAG Minimum Bandwidth

rtr1

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#exit`	Exit the configure mode

Validation

rtr1

```
#sh running-config interface po10

interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
port-channel min-bandwidth 40g
!

!

#show etherchannel
-------------------------------------
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Member:
   xe4/1
   xe4/2
   xe4/3
```

```
   xe4/4
-------------------------------------

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
%   Link: xe4/4 (10072) sync: 1
%   Link: xe4/1 (10069) sync: 1
%   Link: xe4/2 (10070) sync: 1
%   Link: xe4/3 (10071) sync: 1
-------------------------------------
```

rtr2

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#exit`	Exit the configure mode

Validation

rtr2

```
#show running-config interface po10
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-bandwidth 40g
!

#show etherchannel

% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Member:
   xe50/1
   xe50/2
   xe50/3
   xe50/4

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
%   Link: xe50/4 (10072) sync: 1
```


© 2021 IP Infusion Inc. Proprietary

```
%   Link: xe50/1 (10069) sync: 1
%   Link: xe50/2 (10070) sync: 1
%   Link: xe50/3 (10071) sync: 1
```

Note: When a PO goes down due to the [Total bandwidth] < [minimum bandwidth configured]

```
Rtr1:
=====
#OcNOS#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po10         AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#


OcNOS#sh etherchannel
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Protocol Down (Min L/B): True
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4


Rtr2:
=====
OcNOS#sh etherchannel
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Protocol Down (Min L/B): True
% Member:
   Xe50/1
   Xe50/2
   Xe50/3
       xe50/4
```

```
OcNOS#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po10         AGG   1     trunk             down     PD(Min L/B)  0
OcNOS#
```

LACP Minimum-Link, Minimum-Bandwidth Configurations on dynamic, static Channel-Groups with MC-LAG.

Overview

OcNOS allows the configuration of minimum number of the LAG members per LAG group. Both these configurations are meaningful in case the LAG is used for incremental-BW mode. The minimum configuration controls the minimum number of members /bandwidth that must be operationally up / bandwidth available to declare their LAG as operationally UP.

When static/dynamic LAG interface configured with minimum links / minimum bandwidth, the following conditions are to be met:

- Ports which are admin and operational up are considered for min-link.
- The specified minimum number of links should be up.
- Min-link and min-bandwidth cannot co-exist.
- When ports are down due to min-link/min-bandwidth, in show interface brief command output, port down with the corresponding reason code for the failure due to min-link/min-bandwidth.

Minimum Active Members/Bandwidth

The user can specify the minimum number of members that must be operationally up to declare their LAG as operationally UP. Note that this parameter applies to static/dynamic LAG.

```
port-channel min-links <2 - 32>
```

 © 2021 IP Infusion Inc. Proprietary

The minimum active member configuration will be allowed to be modified to be greater than the current number of active members. In such configuration, the LAG operational status will become operationally down.

The user can specify the minimum bandwidth, based on the configured value and the ports that satisfy the conditions LAG will be operationally UP. This parameter is applied for static/dynamic LAG.

```
port-channel min-bandwidth BANDWIDTH
```

BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.

When condition fails, the operational state changes to DOWN.

Note: Do not configure minimum-link, Minimum Bandwidth both on TORS and switches at the same time to avoid flaps of MLAG.

Topology

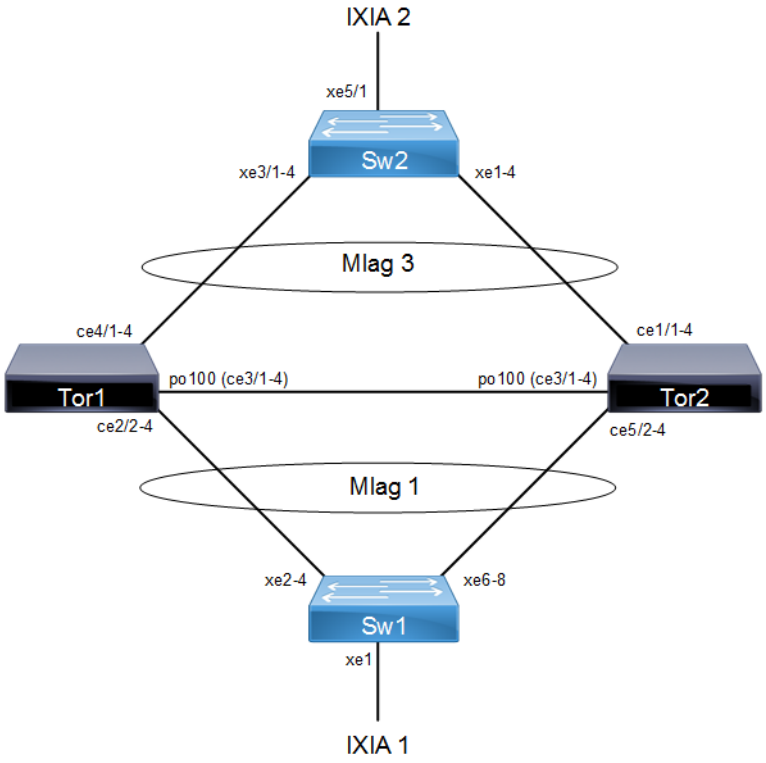


Figure 5-61: MC - LAG Topology

Configuration

TOR1:

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol rstp vlan-bridge end`	Configure bridge type
`configure terminal`	Enter Configure mode
`(config)# vlan database`	Enter vlan database
`(config-vlan)# vlan 600 bridge 1 state enable`	Configure vlans

(config-if)#exit	
(config)#interface mlag1	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,601,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)#exit	Return to privilege mode
(config)#interface mlag3	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)#exit	Return to privilege mode
(config)#interface po100	Enter Interface mode
(config-if)# switchport	Make po as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)# port-channel load-balance src-dst-mac	Enable load balance
(config-if)# mtu 9216	Configure mtu
(config-if)#exit	
(config)#interface sa1	Enter Interface mode
(config-if)# switchport	Make sa1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed all	Enable all VLAN identifiers on this interface.
(config-if)# port-channel load-balance src-dst-mac	Enable load balance
(config-if)#exit	Return to privilege mode
(config)#interface ce2/2	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#exit	Return to privilege mode
(config)#interface ce2/3	Enter Interface mode

© 2021 IP Infusion Inc. Proprietary

(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#exit	Return to privilege mode
(config)#interface ce2/4	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#exit	Return to privilege mode
(config)#interface ce3/1	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#exit	Return to privilege mode
(config)#interface ce3/2	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#exit	Return to privilege mode
(config)#interface ce3/3	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#exit	Return to privilege mode
(config)#interface ce3/4	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#exit	Return to privilege mode
(config)#interface ce4/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode
(config)#interface ce4/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode
(config)#interface ce4/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode
(config)#mcec domain configuration	Enter Multichasis Etherchannel domain configuration mode.
(config-mcec-domain)# domain-address 1111.2222.3333	Configure the domain address.
(config-mcec-domain)# domain-system-number 1	Configure the domain system number
(config-mcec-domain)# intra-domain-link po100	Specify the intra domain link for MLAG communication
(config-mcec-domain)#exit	Return to privilege mode
(config)#int mlag1	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag1
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#exit	Return to privilege mode
(config)#interface sa1	Enter Interface mode
(config-if)#mlag 1	Map sa1 to mlag1
(config-if)#exit	Return to privilege mode
(config)#int mlag3	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag3

(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#exit	Return to privilege mode
(config)#interface sa3	Enter Interface mode
(config-if)#mlag 3	Map sa3 to mlag3
(config-if)#exit	Return to privilege mode
(config-if)# interface sa1	Enter sa interface mode
(config-if)#port-channel min-links 3	Configure min-link value on sa interface
(config)#interface sa3	Enter sa Interface mode
(config-if)#port-channel min-bandwidth 30g	Configure min-bandwidth value on sa/po interface

TOR2

#configure terminal	Enter configure mode.
bridge 1 protocol rstp vlan-bridge end	Configure bridge type
configure terminal	Enter Configure mode.
(config)# vlan database	Enter vlan database
(config-vlan)# vlan 600 bridge 1 state enable	Configure vlans
#configure terminal	Enter Configure mode.
(config)#interface mlag1	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,601,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)#exit	Return to privilege mode
(config)#interface mlag3	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)#exit	Return to privilege mode
(config)#interface po100	Enter Interface mode
(config-if)# switchport	Make po(IDL) as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.

© 2021 IP Infusion Inc. Proprietary

(config-if)# port-channel load-balance src-dst-mac	Enable load balance
(config-if)# mtu 9216	Configure mtu
(config-if)#exit	Return to privilege mode
(config)#interface sa1	Enter Interface mode
(config-if)# switchport	Make sa1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed all	Enable all VLAN identifiers on this interface.
(config-if)# port-channel load-balance src-dst-mac	Enable load balance
(config-if)#exit	Return to privilege mode
(config)#interface sa3	Enter Interface mode
(config-if)# switchport	Make sa3 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed all	Enable all VLAN identifiers on this interface.
(config-if)# port-channel load-balance src-dst-mac	Enable load balance
(config-if)#exit	Return to privilege mode
(config)#interface ce1/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode
(config)#interface ce1/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode
(config)#interface ce1/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode
(config)#interface ce3/1	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#exit	Return to privilege mode
(config)#interface ce3/2	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#exit	Return to privilege mode
(config)#interface ce3/3	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#exit	Return to privilege mode
(config)#interface ce3/4	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100

(config-if)#exit	Return to privilege mode
(config)#interface ce5/1	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#exit	Return to privilege mode
(config)#interface ce5/2	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#exit	Return to privilege mode
(config)#interface ce5/3	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#exit	Return to privilege mode
(config)#mcec domain configuration	Enter Multichasis Etherchannel domain configuration mode.
(config-mcec-domain)# domain-address 1111.2222.3333	Configure the domain address.
(config-mcec-domain)# domain-system-number 2	Configure the domain system number
(config-mcec-domain)# intra-domain-link po100	Specify the intra domain link for MLAG communication
(config-mcec-domain)#end	Return to privilege mode
#configure terminal	Enter Configure mode.
(config)#int mlag1	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag1
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#exit	Return to privilege mode
(config)#interface sa1	Enter Interface mode
(config-if)#mlag 1	Map sa1 to mlag1
(config-if)#exit	Return to privilege mode
(config)#int mlag3	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag3
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#exit	Return to privilege mode
(config)#interface sa3	Enter Interface mode
(config-if)#mlag 3	Map sa3 to mlag3
(config-if)#exit	Return to privilege mode
(config-if)#interface sa1	Enter sa interface mode
(config-if)#port-channel min-links 3	Configure min-link value on sa interface
(config)#interface sa3	Enter sa Interface mode
(config-if)#port-channel min-bandwidth 30g	Configure min-bandwidth value on sa interface.

SW1

configure terminal	Enter Configure mode.
bridge 1 protocol rstp vlan-bridge	Configure bridge type
(config)#vlan database	Create vlan database

© 2021 IP Infusion Inc. Proprietary

(config-vlan)#vlan 600,601,502,101,100 bridge 1 state enable	Create Vlans
(config-vlan)#end	Return to privilege mode
configure terminal	Enter Configure mode.
(config)#interface xe1	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#spanning-tree edgeport	Configure port as edgeport
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#exit	Return to privilege mode
(config)#interface sa1	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan add 100,101,300,401,402	Enable all VLAN identifiers on this interface.
(config-if)# port-channel load-balance src-dst-mac	Enable load balance
(config-if)#spanning-tree edgeport	Configure port as edgeport
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#exit	Return to privilege mode
(config)#interface xe2	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#exit	Return to privilege mode
(config)#interface xe3	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#exit	Return to privilege mode
(config)#interface xe4	Enter Interface mode
(config-if)#static-channel-group 1	Add interface to sa1
(config-if)#exit	Return to privilege mode
(config)#interface xe6	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#exit	Return to privilege mode
(config)#interface xe7	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#exit	Return to privilege mode

(config)#interface xe8	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#exit	Return to privilege mode

SW2

(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge type
(config)#vlan database	Create vlan database
(config-vlan)#vlan 600,601,502,101,100 bridge 1 state enable	Create vlans
(config-vlan)#exit	Return to privilege mode
(config)#interface xe5/1	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#spanning-tree edgeport	Configure port as edge port
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#exit	Return to privilege mode
(config)#interface sa3	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan add 100,101,401,402,600,502	Enable all VLAN identifiers on this interface.
(config-if)# port-channel load-balance src-dst-mac	Enable load balance
(config-if)#spanning-tree edgeport	Configure port as edge port
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#exit	Return to privilege mode
(config)#interface xe3/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode
(config)#interface xe3/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode
(config)#interface xe3/3	Enter Interface mode
(config-if)#static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode

© 2021 IP Infusion Inc. Proprietary

(config)#interface xe1/1	Enter Interface mode
(config-if)#static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode
(config)#interface xe1/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode
(config)#interface xe1/3	Enter Interface mode
(config-if)#static-channel-group 3	Add interface to sa3
(config-if)#exit	Return to privilege mode

This configuration is applicable for the dynamic LAG with MC-LAG topology except dynamic LAG interface creations, which needs to be referred from the dynamic LAG configurations given above.

Validation Commands

sh int brief sa [id], sh int brief po [id], sh mlag-domain summary, sh static-channel-group <sa id>, <sh etherchannel>, sh running-config interface sa [id], <sh etherchannel summary>.

When sa or po goes down due to min-link or min-bandwidth not satisfied, below validations to be done:

rtr2

```
#sh int brief sa1
Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down

--------------------------------------------------------------------------------
Port-channel Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
sa1           AGG   1     trunk             down     PD(Min L/B)  0

#
#sh int brief po100

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
```

```
        DV - DDM Violation, NA - Not Applicable
        NOM - No operational members, PVID - Port Vlan-id
        Ctl - Control Port (Br-Breakout/Bu-Bundle)
        HD  - ESI Hold Timer Down


-------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
-------------------------------------------------------------------------------
--
po100         AGG   1     trunk             down     PD(Min L/B)  0

#
#sh etherchannel
% Lacp Aggregator: po100
% Min-Bandwidth : 40g
% Protocol Down (Min L/B) : True
% Member:
   ce3/1
   ce3/2
   ce3/3
   ce3/4
-----------------------------------
% Lacp Aggregator: po200
% Member:
   ce29/1
   ce29/2
-----------------------------------
% Lacp Aggregator: sa1
% Min-links : 3
% Protocol Down (Min L/B): True
% Member:
   ce2/2
   ce2/3
   ce2/4
-----------------------------------
% Lacp Aggregator: sa3
% Member:
   ce4/1
   ce4/2
   ce4/3
#
#sh running-config interface sa1
!
interface sa1
 switchport
 port-channel min-links 3
 mlag 1
!

#sh static-channel-group 1
 Static Aggregator: sa1
 Minimum-Links 3
 Member Status
  ce2/2          down
```


© 2021 IP Infusion Inc. Proprietary

```
  ce2/3          down
  ce2/4          down
#
#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: Layer2
  Admin Key: 0100 - Oper Key 0100
     Link: ce3/1 (5057) sync: 0
     Link: ce3/2 (5058) sync: 0
     Link: ce3/3 (5059) sync: 0
     Link: ce3/4 (5060) sync: 0
-------------------------------------
```

LACP Force-Up

In an aggregated environment, there are some parameters that are set for member ports in lag. Whenever the parameters are set and conditions are satisfied, the port channel will be in SYNC. If force-up mode is enabled for the member port, the port channel will always be in SYNC even if the parameters are not set i.e. the traffic will not be affected and the port channel will never go down.

LACP force-up with Dynamic LAG

Topology

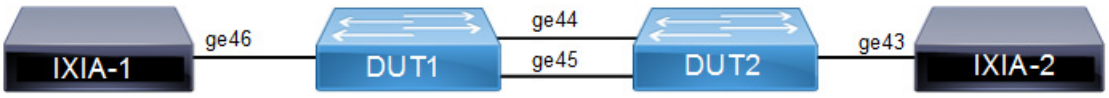


Figure 5-62: LACP force-up with Dynamic LAG

DUT1

`#configure terminal`	Enter configure mode.
`(config)#hostname DUT1`	Configure host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan 2-100 bridge 1 state enable`	Configure VLAN for the bridge
`(config)#interface ge46`	Enter interface mode
`(config-if)#switchport`	Make interface as Switchport
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as hybrid
`(config-if)#switchport hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`(config)#interface po1`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port

(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed vlan all for the hybrid mode
(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
(config)#interface ge44	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config)#interface ge45	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1

DUT2

#configure terminal	Enter configure mode.
(config)#hostname DUT2	Configure host name
(config)#bridge 1 protocol provider-rstp edge	Create provider rstp edge bridge
(config)#vlan database	Enter vlan database mode
(config-vlan)#vlan 2-100 type customer bridge 1 state enable	Configure customer VLAN for the bridge
(config-vlan)#vlan 100 type service point-point bridge 1 state enable	Configure service VLAN for the bridge
(config)#exit	Exit vlan database mode
(config)#cvlan registration table map1 bridge 1	Creating registration table
(config)#cvlan 2-100 svlan 100	Mapping cvlan to svlan
(config)#interface ge43	Enter interface mode
(config-if)#switchport	Make interface as Switchport
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode provider-network	Configure the mode as provider-network
(config-if)# switchport provider-network allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
(config)#interface po1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface with bridge group 1
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer-edge hybrid
(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan all
(config-if)#switchport customer-edge vlan registration map1	Configuring the registration table mapping on lag interface
(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
(config)#interface ge44	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#lacp force-up	Enable lacp force-up for the member port interface

© 2021 IP Infusion Inc. Proprietary

(config)#interface ge45	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1

Send L2 traffic with incremental source mac of 1000 and with VLAN 100 from IXIA1 and with incremental source mac of 1000 and with SVLAN 100(TPID 0x88a8), CVLAN 100 from IXIA2.

Validation

DUT1

```
DUT1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 2001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 2001

DUT1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5043) sync: 1
     Link: ge45 (5046) sync: 1

DUT1#show interface counters rate mbps
+------------------+-------------+------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps  |    Tx mbps  |    Tx pps   |
+------------------+-------------+------------+-------------+-------------+
 ge44               363.65        710252       772.76        1420506
 ge45               363.63        710222       0.00          0
 ge46               772.77        1420525      727.31        1420526
 po1                728.56        1422971      774.09        1422966

DUT2#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 2001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 2001

DUT2#show interface counters rate mbps
+------------------+-------------+------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps  |    Tx mbps  |    Tx pps   |
+------------------+-------------+------------+-------------+-------------+
 ge43               774.26        1423267      784.17        1361411
 ge44               774.26        1423268      364.36        711634
 ge45               0.00          0            364.36        711634
 po1                774.26        1423267      728.71        1423267

DUT2#show etherchannel summary
```

```
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5020) sync: 1
     Link: ge45 (5022) sync: 1
```

On server side (DUT1) to make LAG down you can unconfigure the channel-group 1 configurations and verify force-up is getting enabled in DUT2.

To simulate the force-up

`DUT1(config)#interface ge44`	Enter interface mode.
`DUT1(config-if)#no channel-group`	Removing channel-group configurations from interface.
`DUT1(config)#interface ge45`	Enter interface mode.
`DUT1(config-if)#no channel-group`	Removing channel-group configurations from interface.

DUT2

```
DUT2#show interface brief | include po1
po1            AGG   1     customer-edge     up       none    1g

DUT2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5020) sync: 0 (force-up)
     Link: ge45 (5022) sync: 0

DUT2#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
  Mac address: b8:6a:97:4d:65:d5
  Admin Key: 0001 - Oper Key 0001
   Actor LAG ID- 0x8000,b8-6a-97-28-a5-c0,0x0001
   Receive link count: 0 - Transmit link count: 0
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
    Link: ge44 (5020) sync: 0 (force-up)
    Link: ge45 (5022) sync: 0
  Collector max delay: 5
```

To forward traffic from ge44 of DUT1

`DUT1(config)#interface ge44`	Enter interface mode.
`DUT1(config-if)#switchport`	Make the interface as switch port.
`DUT1(config-if)#bridge-group 1`	Associate the interface to bridge.
`DUT1(config-if)#switchport mode hybrid`	Configure the mode as hybrid.
`DUT1(config-if)#switchport hybrid allowed vlan all`	Configure allowed vlan all for the hybrid mode.
`DUT1(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds.

© 2021 IP Infusion Inc. Proprietary

```
DUT2#show interface counters rate mbps
+------------------+-------------+------------+-------------+------------+
|     Interface    |    Rx mbps  |    Rx pps  |    Tx mbps  |    Tx pps  |
+------------------+-------------+------------+-------------+------------+
 ge43                774.25        1423257      784.17        1361400
 ge44                774.25        1423258      728.71        1423257
 ge45                0.00          0            0.00          0
 po1                 774.25        1423247      728.70        1423245
 DUT2#
DUT1#show interface counters rate mbps
+------------------+-------------+------------+-------------+------------+
|     Interface    |    Rx mbps  |    Rx pps  |    Tx mbps  |    Tx pps  |
+------------------+-------------+------------+-------------+------------+
 ge44                657.67        1284505      640.77        1177884
 ge45                0.00          0            0.00          0
 ge46                772.71        1420426      603.08        1177886
```

LACP force-up with McLAG

Topology

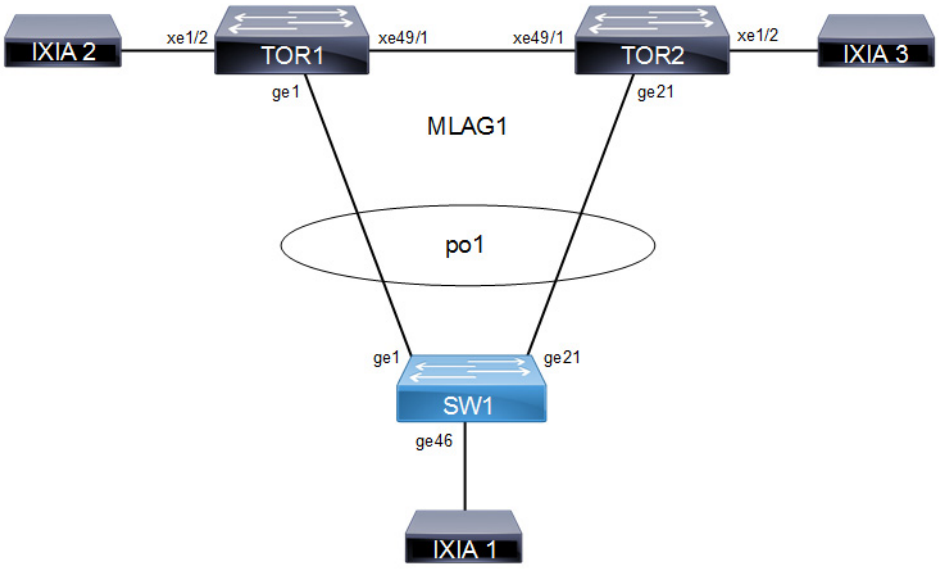


Figure 5-63: LACP force-up with McLAG

TOR1

(config)#bridge 1 protocol provider-rstp edge	Create provider rstp bridge.
(config)#vlan database	Enter vlan database mode
(config-vlan)#vlan 2-10 type customer bridge 1 state enable	Enabling customer vlan for bridge
(config-vlan)#vlan 2-10 type service point-point bridge 1 state enable	Enabling service vlan for bridge
(config)#cvlan registration table map1 bridge 1	Creating registration table
(config-cvlan-registration)#cvlan 2 svlan 2	Mapping cvlan to svlan
(config-cvlan-registration)#cvlan 10 svlan 2	Mapping cvlan to svlan
(config)#interface xe49/1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode provider-network	Set the switching characteristics of this interface to provider network
(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all vlan
(config-if)#interface mlag1	Entering mlag interface
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer-edge hybrid
(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan 2
(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan all
(config-if)#switchport customer-edge vlan registration map1	Configuring the registration table mapping on mlag interface
(config-if)#interface po1	Entering dynamic lag interface
(config-if)#switchport	Configuring interface as switchport
(config-if)#mlag 1	Enabling mlag group number
(config-if)#interface ge1	Entering interface mode
(config-if)#lacp force-up	Enable lacp force-up for the member port interface
(config-if)#channel-group 1 mode active	Add this interface to channel group 1
(config-if)#exit	Exit the interface mode
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 2222.2222.2222	Domain address for the mlag domain
(config-mcec-domain)#domain-system-number 1	Number to identify the node in a domain
(config-mcec-domain)#intra-domain-link xe49/1	Intra domain line between mlag domain

© 2021 IP Infusion Inc. Proprietary

TOR2

(config)#bridge 1 protocol provider-rstp edge	Create provider rstp bridge.
(config)#vlan database	Enter vlan database mode
(config-vlan)#vlan 2-10 type customer bridge 1 state enable	Enabling customer vlan for bridge
(config-vlan)#vlan 2-10 type service point-point bridge 1 state enable	Enabling service vlan for bridge
(config)#cvlan registration table map1 bridge 1	Creating registration table
(config-cvlan-registration)#cvlan 2 svlan 2	Mapping cvlan to svlan
(config-cvlan-registration)#cvlan 10 svlan 2	Mapping cvlan to svlan
(config)#interface xe49/1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode provider-network	Set the switching characteristics of this interface to provider network
(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all vlan
(config-if)#interface mlag1	Entering mlag interface
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer-edge hybrid
(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan 2
(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan all
(config-if)#switchport customer-edge vlan registration map1	Configuring the registration table mapping on mlag interface
(config-if)#interface po1	Entering dynamic lag interface
(config-if)#switchport	Configuring interface as switchport
(config-if)#mlag 1	Enabling mlag group number
(config-if)#interface ge21	Entering interface mode
(config-if)#lacp force-up	Enable lacp force-up for the member port interface
(config-if)#channel-group 1 mode active	Add this interface to channel group 1
(config-if)#exit	Exit the interface mode
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 2222.2222.2222	Domain address for the mlag domain
(config-mcec-domain)#domain-system-number 2	Number to identify the node in a domain
(config-mcec-domain)#intra-domain-link xe49/1	Intra domain line between mlag domain

SW1

(config)#config t	Enter configure terminal.
(config)#bridge 1 protocol rstp vlan-bridge	Configuring the rstp vlan bridge
(config)#vlan 4000-4040 bridge 1 state enable	Configure customer vlan.
(config)#interface po1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disabling spanning-tree
(config-if)#switchport mode access	Configure switchport mode as access
(config-if)#switchport access vlan 4001	Configure access vlan 4001
(config-if)#interface ge1	Entering interface mode
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 .
(config-if)#interface ge21	Entering interface mode
(config-if)#channel-group 1 mode active	Add this interface to channel group 1.
(config-if)#interface ge46	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode hybrid	Set the switching characteristics of this interface to hybrid
(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface to hybrid and allow vlan all

Validation

```
TOR1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 32769 - Oper Key 16385
     Link: ge1 (5026) sync: 1

TOR2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 16385 - Oper Key 16385
     Link: ge21 (5046) sync: 1

SW1#show etherchannel summary
  Aggregator po2 100002
  Aggregator Type: Layer2
  Admin Key: 0002 - Oper Key 0002
     Link: ge2 (5001) sync: 1
     Link: ge22 (5021) sync: 1
```


© 2021 IP Infusion Inc. Proprietary

```
TOR1#show mlag domain summary
-----------------------------------
Domain Configuration
-----------------------------------
Domain System Number            : 2
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : po99
Domain Adjacency                : UP
-----------------------------------
MLAG Configuration
-----------------------------------
MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 1 ef 71 4b 7f 37 5b 6a a5 8c e1 2f 95 9a fe cf
  Total Bandwidth               : 2g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Active
  Current Mlag state            : Active


TOR2#show mlag domain summary
-----------------------------------
Domain Configuration
-----------------------------------
Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : po99
Domain Adjacency                : UP
-----------------------------------
MLAG Configuration
-----------------------------------
MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 1 ef 71 4b 7f 37 5b 6a a5 8c e1 2f 95 9a fe cf
  Total Bandwidth               : 2g
  Mode                          : Active-Active
  Current Mlag state            : Activ



TOR1#show mac address-table count bridge 1 interface mlag1
MAC Entries for all vlans:
Dynamic Address Count: 1001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 1001
TOR1#show mac address-table l count bridge 1 interface mlag1
```

```
MAC Entries for all vlans:
Total MAC Addresses in Use: 500


TOR1#show mac address-table r count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 501


TOR2#show mac address-table count bridge 1 interface mlag1
MAC Entries for all vlans:
Dynamic Address Count: 1001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 1001


TOR2#show mac address-table l count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 501
TOR2#show mac address-table r count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 500
```

Note: For MLAG case, admin should configure 'force-up' port either on master node or slave node only.

Example: In a static trunk environment, Preboot eXecution Environment (PXE) images are too small for most operating systems to leverage LACP during the boot process. As a result, during a PXE build process, traffic sent by the server is dropped, and the build process can fail.

To correct this situation, a port on an ICX 7750 device connected to a server that is configured as an MCT client can be set to a “force-up” state so that even if the LACPDU is not received from the server, the connected port is up and forwards packets.

To simulate this scenario we can remove channel-group configurations from the server side switch SW1 and check LACP force-up is getting enabled on TOR1:

`DUT1(config)#interface ge1`	Enter interface mode.
`DUT1(config-if)#no channel-group`	Removing channel-group configurations from interface.
`DUT1(config)#interface ge21`	Enter interface mode.
`DUT1(config-if)#no channel-group`	Removing channel-group configurations from interface.

DUT2

```
TOR1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 32769 - Oper Key 16385
     Link: ge1 (5026) sync: 0 (force-up)

TOR2#show etherchannel summary
  Aggregator po1 100001
```


© 2021 IP Infusion Inc. Proprietary

```
  Aggregator Type: Layer2
  Admin Key: 16385 - Oper Key 16385
     Link: ge21 (5046) sync: 0


TOR1#show mlag domain summary
-----------------------------------
Domain Configuration
-----------------------------------
Domain System Number            : 2
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : po99
Domain Adjacency                : UP
-----------------------------------
MLAG Configuration
-----------------------------------
MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 1 ef 71 4b 7f 37 5b 6a a5 8c e1 2f 95 9a fe cf
  Total Bandwidth               : 1g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Active
  Current Mlag state            : Active


TOR2#show mlag domain summary
-----------------------------------
Domain Configuration
-----------------------------------
Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : po99
Domain Adjacency                : UP
-----------------------------------
MLAG Configuration
-----------------------------------
MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 1 ef 71 4b 7f 37 5b 6a a5 8c e1 2f 95 9a fe cf
  Total Bandwidth               : 1g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Active
  Current Mlag state            : Active
```

To forward traffic from ge1 of SW2:

DUT1(config)#interface ge1	Enter interface mode.
DUT1(config-if)#switchport	Make the interface as switch port.
DUT1(config-if)#bridge-group 1 spanning-tree disable	Associate the interface to bridge.
DUT1(config-if)#switchport mode access	Configure the mode as access.
DUT1(config-if)#switchport access vlan 4001	Configure allowed vlan 4001 for the access mode.
DUT1(config-if)#load-interval 30	Configure load period in multiple of 30 seconds.

```
TOR1#show mac address-table count bridge 1 interface mlag1
MAC Entries for all vlans:
Dynamic Address Count: 999
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 999
TOR1#show mac address-table l count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 999
TOR1#show mac address-table r count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 0


TOR2#show mac address-table count bridge 1 interface mlag1
MAC Entries for all vlans:
Dynamic Address Count: 0
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 0


TOR2#show mac address-table l count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 0
TOR2#show mac address-table r count bridge 1 interface mlag1
MAC Entries for all vlans:
Total MAC Addresses in Use: 0


TOR1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 32769 - Oper Key 16385
     Link: ge1 (5026) sync: 0 (force-up)


TOR1#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
```


© 2021 IP Infusion Inc. Proprietary

```
  Mac address: 14:02:ec:1c:31:5b
  Admin Key: 32769 - Oper Key 16385
   Actor LAG ID- 0x8000,11-11-22-22-33-33,0x4001
   Receive link count: 0 - Transmit link count: 0
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
    Link: ge1 (5026) sync: 0 (force-up)
  Collector max delay: 5


SW1#show interface counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps   |    Tx mbps  |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 ge1                0.00          0             726.53        1418994
 ge46               772.68        1420362       0.00          0


TOR1#show interface counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps   |    Tx mbps  |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 ge1                729.42        1424656       0.00          0
 mlag1              729.42        1424655       0.00          0
 po1                729.43        1424658       0.00          0
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 6 Link Layer Discovery Protocol Configuration

This chapter contains a complete sample Link Layer Discovery Protocol (LLDP) configuration.

LLDP is a neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise themselves to other devices on the same physical LAN, and then to store information about the network. It allows a device to learn higher-layer management reachability and connection endpoint information from adjacent devices. Using LLDP, a network device is able to advertise its identity, its capabilities and its media-specific configuration, as well as learn the same information from other connected devices.

Note: The `lldp-agent` command is not supported for SVLAN, VLAN, and loop-back interfaces.

Topology

Figure 6-64 displays a sample LLDP topology.

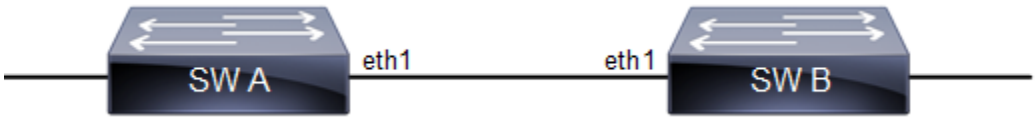


Figure 6-64: LLDP Topology

LLDPv2 (Interface Mode TLV)

Default Agent

All configuration commands in the table below should be followed for each machines.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv-select basic-mgmt port-description`	Enable the `port-description TLV` to be transmitted on the port

`(if-lldp-agent)#lldp tlv-select basic-mgmt system-name`	Enable the `system-name TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select basic-mgmt system-capabilities`	Enable the `system-capabilities TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select basic-mgmt system-description`	Enable the `system-description TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select basic-mgmt management-address`	Enable the `management-address TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific port-vlanid`	Enable the `VLAN-id TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific vlan-name`	Enable the `VLAN-NAME TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid`	Enable the `Port and Protocol VLAN id TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific ptcl-identity`	Enable the `Protocol Identity TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific vid-digest`	Enable the `VID Usage Digest TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific mgmt-vid`	Enable the `Management VID TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific link-agg`	Enable the `Link Aggregation TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8023-org-specific mac-phy`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8023-org-specific max-mtu-size`	Enable the Maximum Frame Size TLV to be transmitted on the port
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLDPDUs that are transmitted during a fast transmission period
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local machine

```
#show running-config lldp
!
set lldp system-name LLDP1
set lldp system-description Hardware Model:LLDP
!
interface lo
 lldp-agent
!
interface eth0
 lldp-agent
!
interface eth1
lldp-agent
set lldp enable txrx
set lldp chassis-id-tlv ip-address
```


© 2021 IP Infusion Inc. Proprietary

```
lldp tlv-select basic-mgmt port-description
lldp tlv-select basic-mgmt system-name
lldp tlv-select basic-mgmt system-capabilities
lldp tlv-select basic-mgmt system-description
lldp tlv-select basic-mgmt management-address
lldp tlv-select ieee-8021-org-specific port-vlanid
lldp tlv-select ieee-8021-org-specific vlan-name
lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid
lldp tlv-select ieee-8021-org-specific ptcl-identity
lldp tlv-select ieee-8021-org-specific vid-digest
lldp tlv-select ieee-8021-org-specific mgmt-vid
lldp tlv-select ieee-8021-org-specific link-agg
lldp tlv-select ieee-8023-org-specific mac-phy
lldp tlv-select ieee-8023-org-specific max-mtu-size
set lldp timer msg-fast-tx 5
set lldp tx-fast-init 6
!
interface eth2
 lldp-agent
!
interface eth3
 lldp-agent
!
interface sit0
 lldp-agent
!
interface svlan0.1
 lldp-agent
!
interface vlan1.1
 lldp-agent
!
interface vlan1.2
 lldp-agent
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 nearest-bridge

Agent Mode                   : Nearest bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 5
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Not Defined
 Traffic statistics          :
  Total frames transmitted   : 46
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
```

Customer Bridge

All configuration commands in the table below should be followed for each machine.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent customer-bridge`	Enter into the Customer Bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv-select basic-mgmt port-description`	Enable the port-description TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv-select basic-mgmt system-name`	Enable the system-name TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv-select basic-mgmt system-capabilities`	Enable the system-capabilities TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv-select basic-mgmt system-description`	Enable the system-description TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv-select basic-mgmt management-address`	Enable the management-address TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific port-vlanid`	Enable the VLAN-id TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific vlan-name`	Enable the VLAN-NAME TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific ptcl-identity`	Enable the Protocol Identity TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific vid-digest`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific mgmt-vid`	Enable the Management VID TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific link-agg`	Enable the Link Aggregation TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv-select ieee-8023-org-specific mac-phy`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8023-org-specific max-mtu-size`	Enable the Maximum Frame Size TLV to be transmitted on the port.
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods.

© 2021 IP Infusion Inc. Proprietary

`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLD PDUs that are transmitted during a fast transmission period.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local machine

```
#show running-config lldp
!
set lldp system-name LLDP1
set lldp system-description Hardware Model:LLDP
!
interface eth1
  lldp-agent customer-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  lldp tlv-select basic-mgmt port-description
  lldp tlv-select basic-mgmt system-name
  lldp tlv-select basic-mgmt system-capabilities
  lldp tlv-select basic-mgmt system-description
  lldp tlv-select basic-mgmt  management-address
  lldp tlv-select ieee-8021-org-specific port-vlanid
  lldp tlv-select ieee-8021-org-specific vlan-name
  lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid
  lldp tlv-select ieee-8021-org-specific ptcl-identity
  lldp tlv-select ieee-8021-org-specific vid-digest
  lldp tlv-select ieee-8021-org-specific mgmt-vid
  lldp tlv-select ieee-8021-org-specific link-agg
  lldp tlv-select ieee-8023-org-specific mac-phy
  lldp tlv-select ieee-8023-org-specific max-mtu-size
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6
!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 customer-bridge

Agent Mode                   : Customer-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 5
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Not Defined
 Traffic statistics          :
  Total frames transmitted   : 8
  Total entries aged         : 0
  Total frames received      : 7
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
```

Non-Tpmr-Bridge

The below configurations should be followed for each machines.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the Non tpmr Bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv-select basic-mgmt port-description`	Enable the port-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select basic-mgmt system-name`	Enable the system-name TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select basic-mgmt system-capabilities`	Enable the system-capabilities TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select basic-mgmt system-description`	Enable the system-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select basic-mgmt management-address`	Enable the management-address TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific port-vlanid`	Enable the VLAN-id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific vlan-name`	Enable the VLAN-NAME TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific ptcl-identity`	Enable the Protocol Identity TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific vid-digest`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific mgmt-vid`	Enable the Management VID TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8021-org-specific link-agg`	Enable the Link Aggregation TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8023-org-specific mac-phy`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv-select ieee-8023-org-specific max-mtu-size`	Enable the Maximum Frame Size TLV to be transmitted on the port
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods

© 2021 IP Infusion Inc. Proprietary

`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLD PDUs that are transmitted during a fast transmission period
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local machine

```
#show running-config lldp
!
set lldp system-name LLDP1
set lldp system-description Hardware Model:LLDP
!
interface eth1
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  lldp tlv-select basic-mgmt port-description
  lldp tlv-select basic-mgmt system-name
  lldp tlv-select basic-mgmt system-capabilities
  lldp tlv-select basic-mgmt system-description
  lldp tlv-select basic-mgmt  management-address
  lldp tlv-select ieee-8021-org-specific port-vlanid
  lldp tlv-select ieee-8021-org-specific vlan-name
  lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid
  lldp tlv-select ieee-8021-org-specific ptcl-identity
  lldp tlv-select ieee-8021-org-specific vid-digest
  lldp tlv-select ieee-8021-org-specific mgmt-vid
  lldp tlv-select ieee-8021-org-specific link-agg
  lldp tlv-select ieee-8023-org-specific mac-phy
  lldp tlv-select ieee-8023-org-specific max-mtu-size
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6
!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 non-tmpr-bridge

Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 5
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Not Defined
 Traffic statistics          :
  Total frames transmitted   : 4
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
```

LLDPV2 (Global Mode TLV)

LLDPv2 TLVs can be configured globally, making it applicable for all interfaces where LLDP is enabled.

Topology

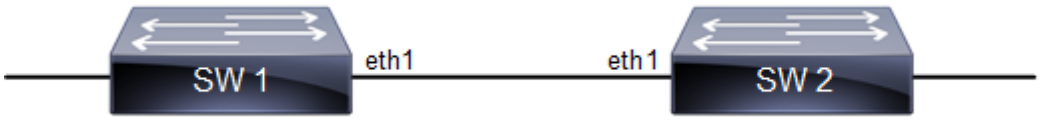


Figure 6-65: LLDP topology

SW1

`SW1#configure terminal`	Enter Configure mode
`SW1(config)#lldp tlv-select basic-mgmt port-description`	Enable LLDP port description TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-name`	Enable LLDP system name TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-capabilities`	Enable LLDP system capabilities TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-description`	Enable LLDP system description TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt management-address`	Enable LLDP port description TLV in global mode
`SW1(config)#interface eth1`	Enter interface mode
`SW1(config-if)#lldp-agent`	Enter LLDP interface mode
`SW1(if-lldp-agent)#set lldp enable txrx`	Enable LLDP TLV transmit and receive for the nearest bridge
`SW1(if-lldp-agent)#exit`	Exit LLDP mode
`SW1(config-if)#exit`	Exit interface mode
`SW1(config-if)#exit`	Exit the configure mode

SW2

`SW2(config)#lldp tlv-select basic-mgmt port-description`	Enable LLDP port description TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-name`	Enable LLDP system name TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-capabilities`	Enable LLDP system capabilities TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-description`	Enable LLDP system description TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt manage-ment-address`	Enable LLDP port description TLV in global mode
`SW2(config)#interface eth1`	Enter interface mode
`SW2(config-if)#lldp-agent`	Enter LLDP interface mode

© 2021 IP Infusion Inc. Proprietary

SW2(if-lldp-agent)#set lldp enable txrx	Enable LLDP TLV transmit and receive for the nearest bridge
SW2(if-lldp-agent)#exit	Exit LLDP mode
SW2(config-if)#exit	Exit interface mode
SW2(config)#end	Exit the configure mode

Validation

```
SW1#show running-config lldp
!
lldp tlv-select basic-mgmt port-description
lldp tlv-select basic-mgmt system-name
lldp tlv-select basic-mgmt system-capabilities
lldp tlv-select basic-mgmt system-description
lldp tlv-select basic-mgmt management-address
!
interface eth1
 lldp-agent
!


SW1#show lldp neighbors

Loc PortID      Rem Host Name      Rem Chassis Id     Rem Port Id       Agent Mode

--------------------------------------------------------------------------------
Eth1           OcNOS              cc37.ab56.6d80     cc37.abbb.ed81   Nearest bridge



SW1#show lldp neighbors detail

--------------------------------------------------------------------------------

Nearest bridge Neighbors
Interface Name               : eth1
 Mandatory TLVs
 Chassis id type          : MAC address [cc37.ab56.6d80]
 Port id type             : MAC address [cc37.abbb.ed81]
 Time to live             : 121
 Basic Management TLVs
 System Name              : SW2
 System Description       : Hardware Model:EC_AS4610-54, Software version: Oc
NOS,1.3.6.241a
 Port Description          : eth1
 Remote System Capabilities : Bridge
                              Router
 Capabilities Enabled     : Router
 Management Address        : MAC Address [cc37.abbb.ed81]
 Interface Number subtype  : ifindex
```

```
 Interface Number          10046
 OID Number              : 0
 802.1 Org specific TLVs
 Port vlan id            : 0
 Port & Protocol vlan id   : 0
 Remote Configured VLANs   : None
 Remote Protocols Advertised: None
 Remote VID Usage Digest   : 0
 Remote Management Vlan    : 0
 Link Aggregation Capability: not capable of being aggregated
 Link Aggregation Status   : not currently in aggregation
 Link Aggregation Port ID  :
 802.3 Org specific TLVs
 AutoNego Support          : Not-Supported
 AutoNego Status           : Disabled
 AutoNego Capability       : 0
 Operational MAU Type      : 0 [unknown]
  Max Frame Size            :
SW1#
```

LLDP-MED

LLDP extensions and behavior requirements are described specifically in the areas of network Configuration and policy, device location (including for Emergency Call Service / E911), Power over Ethernet management, and inventory management.

Based on the device type, different TLVs are advertised by the Station.

LLDP-MED Network Connectivity Device

LLDP-MED Network Connectivity Devices, as defined in this Standard, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

- LAN Switch/Router
- IEEE 802.1 Bridge
- IEEE 802.3 Repeater (included for historical reasons)
- IEEE 802.11 Wireless Access Point
- Any device that supports the IEEE 802.1AB and MED extensions defined by this Standard and can relay IEEE 802 frames via any method.

Configuration Command

```
set lldp med-devtype net-connect
```

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services, however do not support IP media or act as an end-user communication appliance. Such devices

 © 2021 IP Infusion Inc. Proprietary

may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services.

Configuration Command

```
set lldp med-devtype ep-class1
```

LLDP-MED Generic Endpoint (Class 2)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar

Configuration Command

```
set lldp med-devtype ep-class2
```

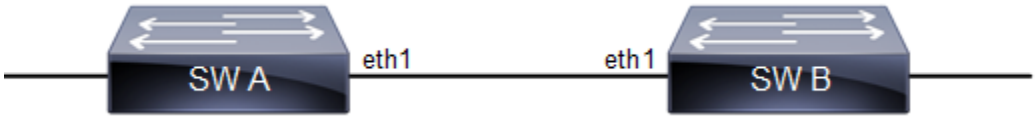
LLDP-MED Generic Endpoint (Class 3)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Configuration Command

```
set lldp med-devtype ep-class3
```

Topology



SW A

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.

`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(if-config-if)#lldp-agent customer-bridge`	Enter into the customer-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the non-tpmr-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#set lldp med-devtype net-connect`	Configure the med device type
`(config-if)#exit`	Exit interface mode.

SW B

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent customer-bridge`	Enter into the customer-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the non-tpmr-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#set lldp med-devtype {ep-class1|ep-class2|ep-class3}`	Configure the med device type
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

Validation

1. Verify the LLDP configurations on Machine A

```
#show running-config lldp
!
set lldp system-name LLDP1
set lldp system-description Hardware Model:LLDP
!
interface lo
 lldp-agent
!
interface eth0
 lldp-agent
!
interface eth1
lldp-agent
set lldp enable txrx
lldp tlv-select med media-capabilities
lldp tlv-select med network-policy
lldp tlv-select med location
set lldp med-devtype net-connect
lldp-agent non-tpmr-bridge
set lldp enable txrx
lldp tlv-select med media-capabilities
lldp tlv-select med network-policy
lldp tlv-select med location
lldp-agent customer-bridge
set lldp enable txrx
lldp tlv-select med media-capabilities
lldp tlv-select med network-policy
lldp tlv-select med location
!
interface eth2
 lldp-agent
!
interface eth3
 lldp-agent
!
interface sit0
 lldp-agent
!
interface svlan0.1
 lldp-agent
!
interface vlan1.1
 lldp-agent
!
interface vlan1.2
 lldp-agent
!
```

2. Verify the LLDP port statistics on machine A

```
#show lldp interface eth1
Agent Mode                    : Customer-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
```

```
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 11
  Total entries aged         : 0
  Total frames received      : 10
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 7
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Nearest bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 7
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0

#show lldp interface eth1 non-tpmr-bridge
Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 5
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Not Defined
 Traffic statistics          :
  Total frames transmitted   : 4
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
```


© 2021 IP Infusion Inc. Proprietary

```
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
```

3. Verify the LLDP configurations for end device ep-class3 on machine B

```
#show running-config lldp
!
interface lo
 lldp-agent
!
interface eth0
 lldp-agent
!
interface eth1
 set lldp med-devtype ep-class3
 lldp-agent
  set lldp enable txrx
  lldp tlv-select med network-policy
lldp-agent non-TPMR-bridge
  set lldp enable txrx
  lldp tlv-select med network-policy
lldp-agent customer-bridge
  set lldp enable txrx
  lldp tlv-select med network-policy
!
interface eth2
 lldp-agent
!
interface eth3
 lldp-agent
!
interface sit0
 lldp-agent
!
interface svlan0.1
 lldp-agent
!
interface vlan1.1
 lldp-agent
!
interface vlan1.2
 lldp-agent
!
```

4. Verify the LLDP port statistics on machine B

```
#show lldp interface eth1
Agent Mode                  : Customer-bridge
 Enable (tx/rx)             : Y/Y
 Message fast transmit time : 1
 Message transmit interval  : 30
 Reinitialisation delay     : 2
 MED Enabled                : Y
  Device Type               : End Point Class-3
 Traffic statistics         :
  Total frames transmitted  : 124
  Total entries aged        : 0
  Total frames received     : 125
```

```
    Total error frames received: 0
    Total frames discarded     : 0
    Total discarded TLVs       : 0
    Total unrecognised TLVs    : 0
  Agent Mode                   : Non-TPMR-bridge
   Enable (tx/rx)              : Y/Y
   Message fast transmit time  : 1
   Message transmit interval   : 30
   Reinitialisation delay      : 2
   MED Enabled                 : Y
    Device Type                : End Point Class-3
   Traffic statistics          :
    Total frames transmitted   : 120
    Total entries aged         : 0
    Total frames received      : 0
    Total error frames received: 0
    Total frames discarded     : 0
    Total discarded TLVs       : 0
    Total unrecognised TLVs    : 0
  Agent Mode                   : Nearest bridge
   Enable (tx/rx)              : Y/Y
   Message fast transmit time  : 1
   Message transmit interval   : 30
   Reinitialisation delay      : 2
   MED Enabled                 : Y
    Device Type                : End Point Class-3
   Traffic statistics          :
    Total frames transmitted   : 120
    Total entries aged         : 0
    Total frames received      : 0
    Total error frames received: 0
    Total frames discarded     : 0
    Total discarded TLVs       : 0
    Total unrecognised TLVs    : 0
  #
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 7 MC-LAG Configuration

This chapter contains a complete example of Multi-Chassis Link Aggregation (MC-LAG) configuration.

MC-LAG (also called DRNI, Distributed Resilient Network Interconnect) expands the concept of link aggregation so that it provides node-level redundancy by allowing two or more nodes to share a common LAG endpoint. MC-LAG emulates multiple nodes to represent as a single logical node to the remote node running link aggregation. As a result even if one of the nodes is down there exists a path to reach the destination through the other nodes.

Note: MC-LAG is compatible only with a RSTP VLAN-aware bridge or a spanning tree disabled bridge.

Note: All MC-LAG nodes must have the same MAC table size as specified by each node's switching ASIC forwarding profile limit.

Dynamic Configuration

Topology

As shown in Figure 7-66, switches 3 and 4 form an MC-LAG domain. Switches 3 and 4 are a single logical switch to switches 1 and 2. Even if either switch 3 or 4 is down, there exists a path to reach other destinations.

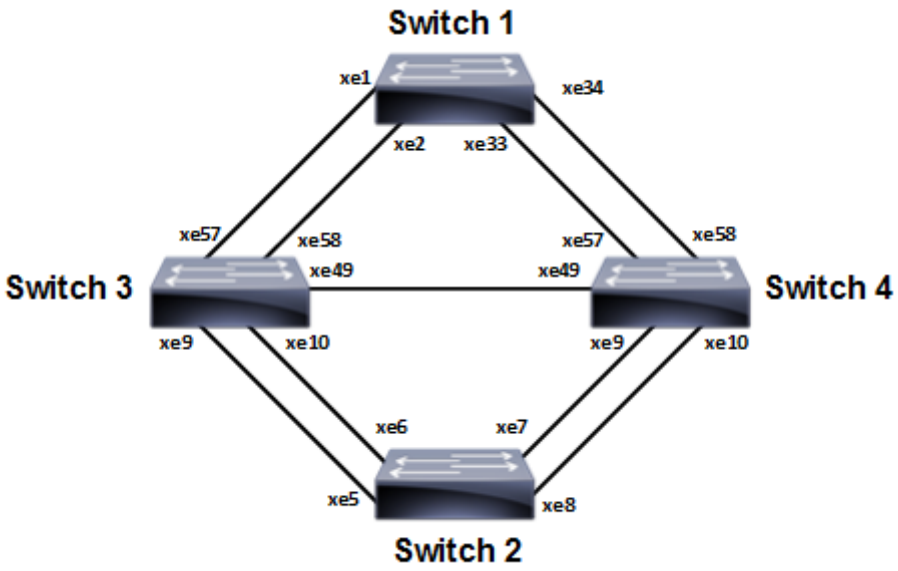


Figure 7-66: MC-LAG Topology

Switch 1

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol rstp vlan-bridge`	Create RSTP bridge 1.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)#interface po2`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#bridge-group 1`	Associate the interface with bridge group 1.

(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe33	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe34	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.

Switch 2

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface po1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe6	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit interface mode.
(config)#interface xe7	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe8	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.

Switch 3

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface mlag1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface mlag2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#mlag 1	Enabling Mlag group number
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#mlag 2	enabling Mlag group number
(config-if)#exit	Exit interface mode.
(config)#interface xe9	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.

(config-if)#exit	Exit interface mode.
(config)#interface xe57	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe58	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe10	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe49	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#exit	Exit interface mode.
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the mlag domain
(config-mcec-domain)#intra-domain link xe49	Intra domain line between mlag domain
(config-mcec-domain)#domain-system-number 1	Number to identify the node in a domain
(config-mcec-domain)#exit	Exit MCEC mode

Switch 4

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface mlag1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface mlag2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.

© 2021 IP Infusion Inc. Proprietary

(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#mlag 1	Enabling Mlag group number
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#mlag 2	enabling Mlag group number
(config-if)#exit	Exit interface mode.
(config)#interface xe9	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe10	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe57	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe58	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe49	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#exit	Exit interface mode.
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the Mlag domain
(config-mcec-domain)#intra-domain link xe49	Intra domain Link between Mlag domains
(config-mcec-domain)#domain-system-number 2	Number to identify the node in domain
(config-mcec-domain)#exit	Exit MCEC mode

Validation

Switch 3

```
#sh mlag domain details

-----------------------------------
Domain Configuration
-----------------------------------

Domain System Number           : 1
Domain Address                 : 1111.2222.3333
Domain Priority                : 1000
Intra Domain Interface         : xe49

Hello RCV State                : Current
Hello Periodic Timer State     : Fast Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator           : po1
  Admin Key                   : 16385
  Oper Key                    : 16385
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32769
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active


MLAG-2
  Mapped Aggregator           : po2
  Admin Key                   : 16386
  Oper Key                    : 16386
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32770
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
```


© 2021 IP Infusion Inc. Proprietary

```
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active


#sh etherchannel summary
% Aggregator po1 0
% Aggregator Type: Layer2
% Admin Key: 16385 - Oper Key 16385
%   Link: xe57 (5057) sync: 1 (Mlag-active-link)
%   Link: xe58 (5058) sync: 1 (Mlag-active-link)
% Aggregator po2 0
% Aggregator Type: Layer2
% Admin Key: 16386 - Oper Key 16386
%   Link: xe9 (5009) sync : 1 (Mlag-active-link)
%   Link: xe10 (5010) sync: 1 (Mlag-active-link)

#sh mlag 1 detail

MLAG-1
  Mapped Aggregator           : po1
  Admin Key                   : 16385
  Oper Key                    : 16385
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32769
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Total Bandwidth             : 20g
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active


sh mcec statistics

Unknown MCCPDU received on the system            : 0

-----------------------------------
IDP xe49
-----------------------------------
   Valid RX Hello PDUs                          : 398
   Valid TX Hello PDUs                          : 417
   Valid RX Info PDUs                           : 16
   Valid TX Info PDUs                           : 6

   Valid RX Mac Sync PDUs                       : 3
   Valid TX Mac Sync PDUs                       : 4
```

```
MLAG 1
  Valid RX Info PDUs                          : 8
  Valid TX Info PDUs                          : 3

MLAG 2
  Valid RX Info PDUs                          : 8
  Valid TX Info PDUs                          : 3
sh mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 1000
Intra Domain Interface          : xe49
Domain Adjacency                : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator           : po1
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active


MLAG-2
  Mapped Aggregator           : po2
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active
```


© 2021 IP Infusion Inc. Proprietary

Static Configuration

Static MC-LAG provides node-level redundancy by allowing two or more nodes in the network to share a common static-LAG endpoint. It emulates multiple nodes to represent as a single logical node to the remote node having static Link aggregation. As a result, even if one of the nodes is down there exists a path to reach the destination via other nodes.

Topology

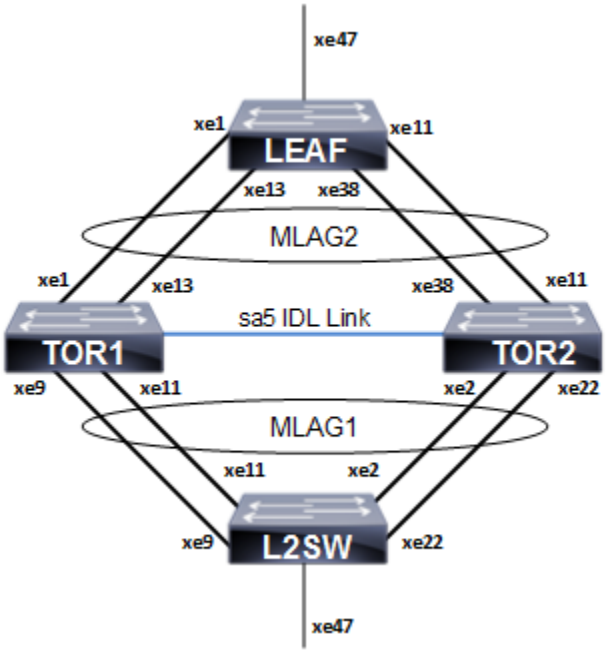


Figure 7-67: Static MLAG topology

L2SW

`#configure terminal`	Enter configure mode.
`(config)#hostname L2SW`	Configuring host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan 2 bridge 1 state enable`	Configure VLAN for the bridge
`(config)#interface sa1`	Enter the interface mode
`(config-if)# bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface
`(config-if)#switchport mode hybrid`	Configure the mode as hybrid
`(config-if)#switchport hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe2`	Enter the interface mode
`(config-if)# static-channel-group 1`	Map static channel to the interface
`(config-if)#exit`	Exit the interface mode

(config)#interface xe9	Enter the interface mode
(config-if)# static-channel-group 1	Map static channel to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe11	Enter the interface mode
(config-if)# static-channel-group 1	Map static channel to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe22	Enter the interface mode
(config-if)# static-channel-group 1	Map static channel to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe47	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)# bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#exit	Exit the interface mode

TOR1

#configure terminal	Enter configure mode.
(config)#hostname TOR1	Configuring host name
(config)#bridge 1 protocol provider-rstp edge	Create a PROVIDER-RSTP EDGE bridge
(config)#vlan 2 bridge 1 state enable	Configure VLAN for the bridge
(config)# vlan 200 type service point-point bridge 1 state enable	Configure SVLAN for the bridge
(config)#cvlan registration table map1 bridge 1	Configure cvlan-svlan mapping registration table for the bridge
(config-cvlan-registration)#cvlan 2 svlan 200	Map CVLAN to SVLAN
(config-cvlan-registration)#exit	Exit the config-cvlan-registration mode
(config)#interface mlag1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)# switchport mode customer-edge hybrid	Configure the mode as customer-edge hybrid
(config-if)# switchport customer-edge hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#switchport customer-edge vlan registration map1	Map the cvlan registration table into the MLAG interface
(config-if)#mode active-standby	Configuring MLAG mode
(config-if)#exit	Exit the interface mode
(config)#interface mlag2	Enter the interface mode
(config-if)#switchport	Make the interface as switch port

© 2021 IP Infusion Inc. Proprietary

(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)# switchport mode provider-network	Configure the mode as provider-network
(config-if)# switchport provider-network allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#mode active-standby	Configuring MLAG mode
(config-if)#exit	Exit the interface mode
(config)#interface sa1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#mlag 1	Map MLAG on SA interface
(config-if)#exit	Exit the interface mode
(config)#interface sa2	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#mlag 2	Map MLAG on SA interface
(config-if)#exit	Exit the interface mode
(config)#interface xe1	Enter the interface mode
(config-if)# static-channel-group 2	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe13	Enter the interface mode
(config-if)# static-channel-group 2	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe9	Enter the interface mode
(config-if)# static-channel-group 1	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe11	Enter the interface mode
(config-if)# static-channel-group 1	Map static channel to the interface
(config-if)#exit	Exit the interface mode
(config)#interface sa5	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#exit	Exit the interface mode
(config)#interface xe3	Enter the interface mode
(config-if)#static-channel-group 5	Map static channel-group to the interface
(config)#interface xe5	Enter the interface mode
(config-if)#static-channel-group 5	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#mcec domain configuration	Enter the MLAG domain configuration mode
(config-mcec-domain)#domain-address 1111.2222.3333	Configure the MLAG domain address
(config-mcec-domain)#domain-system-number 1	Configure MLAG domain system number
(config-mcec-domain)#intra-domain-link sa5	Configure the intra domain link

TOR2

`#configure terminal`	Enter configure mode.
`(config)#hostname TOR2`	Configuring host name
`(config)#bridge 1 protocol provider-rstp edge`	Create a PROVIDER-RSTP EDGE bridge
`(config)#vlan 2 bridge 1 state enable`	Configure VLAN for the bridge
`(config)# vlan 200 type service point-point bridge 1 state enable`	Configure SVLAN for the bridge
`(config)#cvlan registration table map1 bridge 1`	Configure cvlan-svlan mapping registration table for the bridge
`(config-cvlan-registration)#cvlan 2 svlan 200`	Map CVLAN to SVLAN
`(config-cvlan-registration)#exit`	Exit the config-cvlan-registration mode
`(config)#interface mlag1`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)# switchport mode customer-edge hybrid`	Configure the mode as customer-edge hybrid
`(config-if)# switchport customer-edge hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#switchport customer-edge vlan registration map1`	Map the cvlan registration table into the MLAG interface
`(config-if)#mode active-standby`	Configuring MLAG mode
`(config-if)#exit`	Exit the interface mode
`(config)#interface mlag2`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)# switchport mode provider-network`	Configure the mode as provider-network
`(config-if)# switchport provider-network allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#mode active-standby`	Configuring MLAG mode
`(config-if)#exit`	Exit the interface mode
`(config)#interface sa1`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port
`(config-if)#mlag 1`	Map MLAG on SA interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface sa2`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port
`(config-if)#mlag 2`	Map MLAG on SA interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe11`	Enter the interface mode
`(config-if)# static-channel-group 2`	Map static channel to the interface

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit the interface mode
(config)#interface xe38	Enter the interface mode
(config-if)# static-channel-group 2	Map static channel to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe2	Enter the interface mode
(config-if)# static-channel-group 1	Create static channel group
(config-if)#exit	Exit the interface mode
(config)#interface xe22	Enter the interface mode
(config-if)# static-channel-group 1	Create static channel group
(config-if)#exit	Exit the interface mode
(config)#interface sa5	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#exit	Exit the interface mode
(config)#interface xe3	Enter the interface mode
(config-if)#static-channel-group 5	Map static channel-group to the interface
(config)#interface xe5	Enter the interface mode
(config-if)#static-channel-group 5	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#mcec domain configuration	Enter the MLAG domain configuration mode
(config-mcec-domain)#domain-address 1111.2222.3333	Configure the MLAG domain address
(config-mcec-domain)#domain-system-number 2	Configure MLAG domain system number
(config-mcec-domain)#intra-domain-link sa5	Configure the intera domain link
(config-if)#exit	Exit the interface mode

LEAF

#configure terminal	Enter configure mode.
(config)#hostname LEAF	Configuring host name
(config)#bridge 1 protocol provider-rstp edge	Create a PROVIDER-RSTP EDGE bridge
(config)#vlan 2 bridge 1 state enable	Configure VLAN for the bridge
(config)# vlan 200 type service point-point bridge 1 state enable	Configure SVLAN for the bridge
(config)#cvlan registration table map1 bridge 1	Configure cvlan-svlan mapping registration table for the bridge
(config-cvlan-registration)#cvlan 2 svlan 200	Map CVLAN to SVLAN
(config-cvlan-registration)#exit	Exit the config-cvlan-registration mode
(config)#interface sa2	Enter the interface mode
(config-if)#swtichport	Make the interface a switch port
(config-if)# bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface

(config-if)#switchport mode provider-network	Configure the mode as provider-network
(config-if)#)# switchport provider-network allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe1	Enter the interface mode
(config-if)# static-channel-group 2	Map the interface to the static channel-group
(config-if)#exit	Exit the interface mode
(config)#interface xe13	Enter the interface mode
(config-if)# static-channel-group 2	Create static channel group
(config-if)#exit	Exit the interface mode
(config)#interface xe11	Enter the interface mode
(config-if)# static-channel-group 2	Map the interface to the static channel-group
(config-if)#exit	Exit the interface mode
(config)#interface xe38	Enter the interface mode
(config-if)# static-channel-group 2	Create static channel group
(config-if)#exit	Exit the interface mode
(config)#interface xe47	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)# bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)# switchport mode customer-edge hybrid	Configure the mode as customer-edge hybrid
(config-if)# switchport customer-edge hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#switchport customer-edge vlan registration map1	Map the cvlan registration table into the MLAG interface
(config-if)#exit	Exit the interface mode

Validation

```
TOR1#show mlag 1 detail

MLAG-1
  Mapped Aggregator            : sa1
  Admin Key                    : 16385
  Oper Key                     : 16385
  Physical properties Digest   : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc

  Neigh Admin Key              : 32769
  Neigh Physical Digest        : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Total Bandwidth              : 40g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Standby
  Current Mlag State           : Active
```


© 2021 IP Infusion Inc. Proprietary

```
Switchover-mode              : Revertive

TOR1#

TOR1#show mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : sa5
Domain Adjacency                : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator             : sa1
  Physical properties Digest    : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc
  Total Bandwidth               : 40g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Standby
  Current Mlag State            : Active
  Switchover-mode               : Revertive



MLAG-2
  Mapped Aggregator             : sa2
  Physical properties Digest    : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8

  Total Bandwidth               : 40g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Standby
  Current Mlag State            : Active
  Switchover-mode               : Revertive



TOR1#
TOR1#show mlag domain detail

-------------------------------------
Domain Configuration
-------------------------------------
```

```
Domain System Number           : 1
Domain Address                 : 1111.2222.3333
Domain Priority                : 32768
Intra Domain Interface         : sa5

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator            : sa1
  Admin Key                    : 16385
  Oper Key                     : 16385
  Physical properties Digest   : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc

  Neigh Admin Key              : 32769
  Neigh Physical Digest        : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Total Bandwidth              : 40g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Standby
  Current Mlag State           : Active
  Switchover-mode                 : Revertive


MLAG-2
  Mapped Aggregator            : sa2
  Admin Key                    : 16386
  Oper Key                     : 16386
  Physical properties Digest   : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8


  Neigh Admin Key              : 32770
  Neigh Physical Digest        : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8

  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Total Bandwidth              : 40g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Standby
  Current Mlag State           : Active
  Switchover-mode                 : Revertive
```


© 2021 IP Infusion Inc. Proprietary

```
TOR1#
```

ARP ACL Configuration

Topology

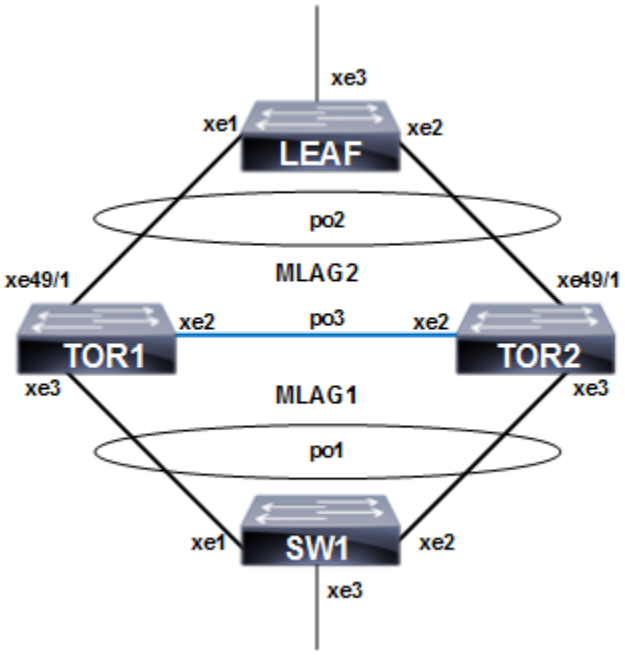


Figure 7-68: ARP ACL configuration with MC LAG

TOR1

`TOR1(config)#bridge 1 protocol provider-rstp edge`	Create provider rstp bridge
`TOR1(config)#vlan 2-3990 type customer bridge 1 state enable`	Enable customer vlan for bridge
`TOR1(config)#vlan 2-3990 type service point-point bridge 1 state enable`	Enable service vlan for bridge
`TOR1(config)#cvlan registration table map1 bridge 1`	Create registration table
`TOR1(config-cvlan-registration)#cvlan 2-3990 svlan 3990`	Map cvlan to svlan
`TOR1(config-cvlan-registration)#exit`	Exit the cvlan registration table mode
`TOR1(config-if)#interface mlag1`	Enter mlag interface
`TOR1(config-if)#switchport`	Configure interface as switchport
`TOR1(config-if)#exit`	Exit the interface mode
`TOR1(config)#interface mlag2`	Enter mlag interface
`TOR1(config-if)#switchport`	Configure interface as switchport
`TOR1(config-if)#bridge-group 1`	Associate the interface with bridge group 1
`TOR1(config-if)#switchport mode provider-network`	Set the switching characteristics of this interface to provider network

© 2021 IP Infusion Inc. Proprietary

TOR1(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all vlan
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#interface po1	Enter dynamic lag interface
TOR1(config-if)#switchport	Configure interface as switchport
TOR1(config-if)#mlag 1	Enable mlag group number
TOR1(config-if)#exit	Exit the interface mode
TOR1(config-if)#interface po2	Enter dynamic lag interface
TOR1(config-if)#switchport	Configure interface as switchport
TOR1(config-if)#mlag 2	Enable mlag group number
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#interface po3	Enter dynamic lag interface
TOR1(config-if)#switchport	Configure interface as switchport
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#interface xe2	Enter interface mode
TOR1(config-if)#channel-group 3 mode active	Make part of channel group 3
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#interface xe3	Enter interface mode
TOR1(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
TOR1(config-if)#exit	Exit the interface mode
TOR1(config-if)#interface xe49/1	Enter interface mode
TOR1(config-if)#channel-group 2 mode active	Enable channel-group 2
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#mcec domain configuration	Enter MCEC mode
TOR1(config-mcec-domain)#domain-address 2222.3333.4444	Domain address for the mlag domain
TOR1(config-mcec-domain)#domain-system-number 1	Number to identify the node in a domain
TOR1(config-mcec-domain)#intra-domain-link po3	Intra domain line between mlag domain
TOR1(config)#hardware-profile filter ingress-arp enable	Enable globally hardware profile for arp
TOR1(config)#arp access-list cep	Create access list with name as cep
TOR1(config-arp-acl)# 30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner-vlan 2	Create permit rule for particular arp request
TOR1(config-arp-acl)# 40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan 3990 inner-vlan 2	Create permit rule for particular arp response
TOR1(config)#arp access-list pnp	Create access list with name as pnp
TOR1(config-arp-acl)#20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner-vlan 2	Create permit rule for particular arp request

TOR1(config-arp-acl)#30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan 3990 inner-vlan 2	Create permit rule for particular arp response
TOR1(config-if)#interface mlag1	Enter mlag1 interface
TOR1(config-if)#arp access-group cep in	Attach rule with access-group cep
TOR1(config-if)#interface mlag2	Enter mlag2 interface
TOR1(config-if)#arp access-group pnp in	Attach rule with access-group pnp

TOR2

TOR2(config)#bridge 1 protocol provider-rstp edge	Create provider rstp bridge
TOR2(config)#vlan 2-3990 type customer bridge 1 state enable	Enable customer vlan for bridge
TOR2(config)#vlan 2-3990 type service point-point bridge 1 state enable	Enable service vlan for bridge
TOR2(config)#cvlan registration table map1 bridge 1	Create registration table
TOR2(config-cvlan-registration)#cvlan 2-3990 svlan 3990	Map cvlan to svlan
TOR2(config-cvlan-registration)#exit	Exit the cvlan registration table mode
TOR2(config)#interface mlag1	Enter mlag interface
TOR2(config-if)#switchport	Configure interface as switchport
TOR2(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
TOR2(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer-edge hybrid
TOR2(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan all
TOR2(config-if)#switchport customer-edge vlan registration map1	Configure the registration table mapping on mlag interface
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface mlag2	Enter mlag interface
TOR2(config-if)#switchport	Configure interface as switchport
TOR2(config-if)#bridge-group 1	Associate the interface with bridge group 1
TOR2(config-if)#switchport mode provider-network	Set the switching characteristics of this interface to provider network
TOR2(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all vlan
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface po1	Enter dynamic lag interface
TOR2(config-if)#switchport	Configure interface as switchport
TOR2(config-if)#mlag 1	Enable mlag group number
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface po2	Enter dynamic lag interface
TOR2(config-if)#switchport	Configure interface as switchport

© 2021 IP Infusion Inc. Proprietary

TOR2(config-if)#mlag 2	Enable mlag group number
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface po3	Enter dynamic lag interface
TOR2(config-if)#switchport	Configure interface as switchport
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface xe2	Enter interface mode
TOR2(config-if)#channel-group 3 mode active	Make part of channel group 3
TOR2(config-if)#interface xe3	Enter interface mode
TOR2(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#Interface xe49/1	Enter interface mode
TOR2(config-if)#channel-group 2 mode active	Enable channel-group 2
TOR2(config)#mcec domain configuration	Configure mcec domain information
TOR2(config-mcec-domain)#domain-address 2222.3333.4444	Domain address for the mlag domain
TOR2(config-mcec-domain)#domain-system-number 2	Number to identify the node in a domain
TOR2(config-mcec-domain)#intra-domain-link po3	Intra domain line between mlag domain
TOR2(config)#hardware-profile filter ingress-arp enable	Enable globally hardware profile for arp
TOR2(config)#arp access-list cep	Create access list with name as cep
TOR2(config-arp-acl)# 30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner-vlan 2	Create permit rule for particular arp request
TOR2(config-arp-acl)# 40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan 3990 inner-vlan 2	Create permit rule for particular arp response
TOR2(config)#arp access-list pnp	Create access list with name as pnp
TOR2(config-arp-acl)#20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner-vlan 2	Create permit rule for particular arp request
TOR2(config-arp-acl)#30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan 3990 inner-vlan 2	Create permit rule for particular arp response
TOR2(config-if)#interface mlag1	Enter mlag1 interface
TOR2(config-if)#arp access-group cep in	Attach rule with access-group cep
TOR2(config-if)#interface mlag2	Enter mlag2 interface
TOR2(config-if)#arp access-group pnp in	Attach rule with access-group pnp

SW1

`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Configure the rstp vlan bridge
`SW1(config)#vlan 2-3990 type customer bridge 1 state enable`	Enable customer vlan for bridge
`SW1(config-if)#interface po1`	Enter dynamic lag interface
`SW1(config-if)#switchport`	Configure interface as switchport
`SW1(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1and disabling spanning-tree
`SW1(config-if)#switchport mode hybrid`	Set the switching characteristics of this interface hybrid
`SW1(config-if)#switchport hybrid allowed vlan all`	Set the switching characteristics of this interface hybrid and allowing all vlan
`SW1(config-if)#exit`	Exit the interface mode
`SW1(config)#interface xe1`	Enter interface mode
`SW1(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
`SW1(config-if)#exit`	Exit the interface mode
`SW1(config)#interface xe2`	Enter interface mode
`SW1(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
`SW1(config-if)#exit`	Exit the interface mode
`SW1(config)#interface xe3`	Enter interface mode
`SW1(config-if)#switchport`	Configure interface as switchport
`SW1(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1and disabling spanning-tree
`SW1(config-if)#switchport mode hybrid`	Set the switching characteristics of this interface hybrid
`SW1(config-if)#switchport hybrid allowed vlan all`	Set the switching characteristics of this interface hybrid and allowing all vlan
`SW1(config-if)#exit`	Exit the interface mode

LEAF

`Leaf(config)#bridge 1 protocol provider-rstp edge`	Configure the rstp vlan bridge
`Leaf(config)#vlan 2-3990 type customer bridge 1 state enable`	Enable customer vlan for bridge
`Leaf(config)#vlan 2-3990 type service point-point bridge 1 state enable`	Enable service vlan for bridge
`Leaf(config)#cvlan registration table map1 bridge 1`	Create registration table
`Leaf(config-cvlan-registration)#cvlan 2-3990 svlan 3990`	Map cvlan to svlan
`Leaf(config-if)#exit`	Exit the cvlan registration table mode
`Leaf(config)#interface po2`	Enter interface mode

© 2021 IP Infusion Inc. Proprietary

`Leaf(config-if)#switchport`	Configure interface as switchport
`Leaf(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1and disabling spanning-tree
`Leaf(config-if)#switchport mode provider-network`	Set the switching characteristics of this interface provider network
`Leaf(config-if)#switchport provider-network allowed vlan all`	Set the switching characteristics of this interface provider and allowing all vlan
`Leaf(config-if)#exit`	Exit the interface mode
`Leaf(config)#interface xe1`	Enter interface mode
`Leaf(config-if)#channel-group 2 mode active`	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
`Leaf(config-if)#exit`	Exit the interface mode
`Leaf(config)#interface xe2`	Enter interface mode
`Leaf(config-if)#channel-group 2 mode active`	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
`Leaf(config-if)#exit`	Exit the interface mode
`Leaf(config)#Interface xe3`	Enter interface mode
`Leaf(config-if)#switchport`	Configure interface as switchport
`Leaf(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1and disabling spanning-tree
`Leaf(config-if)#switchport mode customer-edge hybrid`	Set the switching characteristics of this interface to customer-edge hybrid
`Leaf(config-if)#switchport customer-edge hybrid allowed vlan all`	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan all
`Leaf(config-if)#switchport customer-edge vlan registration map1`	Configure the registration table mapping on mlag interface
`Leaf(config-if)#exit`	Exit the interface mode

Validation

```
TOR1#show access-lists
ARP access list cep
        30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner-vlan 2
        40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan
3990 inner-vlan 2
        default deny-all
ARP access list pnp
       20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner-vlan 2 [match=1]
        30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan
3990 inner-vlan 2 [match=1]
        default deny-all log

TOR2#show access-lists
ARP access list cep
       30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner-vlan 2 [match=1]
        40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan
3990 inner-vlan 2 [match=1]
```

```
        default deny-all log
ARP access list pnp
        20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner-vlan 2
        30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan
3990 inner-vlan 2
        default deny-all
```

Disabling STP for MC-LAG

The command `no bridge 1 provider-rstp enable bridge-forward` is used to disable the spanning tree globally.

Enabling Provider RSTP

`OcNOS#configure terminal`	Enter Configure mode.
`OcNOS(config)# bridge 1 protocol provider-rstp edge`	Configure Provider-rstp edge bridge.
`OcNOS(config)# interface xe13/2`	Configure interface xe13/2\
`OcNOS(config-if)# switchport`	Configure the interface as switchport
`OcNOS(config-if)# bridge-group 1`	Assign the above created bridge to this port.
`OcNOS(config-vrf)#exit`	Exit from interface mode to config mode
`OcNOS(config)# interface po1`	Configure interface po1
`OcNOS(config-if)# switchport`	Configure the interface as switchport
`OcNOS(config-if)# bridge-group 1`	Assign the above created bridge to this port.
`OcNOS(config-vrf)#exit`	Exit from interface mode to config mode
`OcNOS(config)# interface mlag2`	Configure interface mlag1
`OcNOS(config-if)# switchport`	Configure the interface as switchport
`OcNOS(config-if)# bridge-group 1 spanning-tree disable`	Assign the above created bridge to this port and disable the spanning tree.
`OcNOS(config-vrf)#exit`	Exit from interface mode to config mode

Validation

```
OcNOS#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8000ecf4bbfc6928
% 1: Bridge Id 8000ecf4bbfc6928
% 1: last topology change Tue Jul 30 06:47:37 2019
% 1: 2 topology change(s)  - last topology change Tue Jul 30 06:47:37 2019

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   xe13/2: Port Number 942 - Ifindex 5038 - Port Id 0x83ae - Role Designated - State
Forwarding
```


© 2021 IP Infusion Inc. Proprietary

```
%   xe13/2: Designated Path Cost 0
%   xe13/2: Configured Path Cost 2000  - Add type Explicit ref count 1
%   xe13/2: Designated Port Id 0x83ae - Priority 128  -
%   xe13/2: Root 8000ecf4bbfc6928
%   xe13/2: Designated Bridge 8000ecf4bbfc6928
%   xe13/2: Message Age 0 - Max Age 20
%   xe13/2: Hello Time 2 - Forward Delay 15
%   xe13/2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   xe13/2: forward-transitions 3
%   xe13/2: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   xe13/2: No portfast configured - Current  portfast off
%   xe13/2: bpdu-guard  default  - Current bpdu-guard off
%   xe13/2: bpdu-filter default  - Current bpdu-filter off
%   xe13/2: no root guard configured     - Current root guard off
%   xe13/2: Configured Link Type point-to-point - Current point-to-point
%   xe13/2: No auto-edge configured - Current port Auto Edge off
%
%   po1: Port Number 1697 - Ifindex 100001 - Port Id 0x86a1 - Role Designated - State
Forwarding
%   po1: Designated Path Cost 0
%   po1: Configured Path Cost 2000  - Add type Explicit ref count 1
%   po1: Designated Port Id 0x86a1 - Priority 128  -
%   po1: Root 8000ecf4bbfc6928
%   po1: Designated Bridge 8000ecf4bbfc6928
%   po1: Message Age 0 - Max Age 20
%   po1: Hello Time 2 - Forward Delay 15
%   po1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   po1: forward-transitions 1
%   po1: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   po1: No portfast configured - Current  portfast off
%   po1: bpdu-guard  default  - Current bpdu-guard off
%   po1: bpdu-filter default  - Current bpdu-filter off
%   po1: no root guard configured     - Current root guard off
%   po1: Configured Link Type point-to-point - Current point-to-point
%   po1: No auto-edge configured - Current port Auto Edge off
%
%   mlag2: Port Number 2690 - Ifindex 400002 - Port Id 0x8a82 - Role Disabled - State
Forwarding
%   mlag2: Designated Path Cost 0
%   mlag2: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   mlag2: Designated Port Id 0x0 - Priority 128  -
%   mlag2: Message Age 0 - Max Age 0
%   mlag2: Hello Time 0 - Forward Delay 0
%   mlag2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   mlag2: forward-transitions 1
%   mlag2: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   mlag2: No portfast configured - Current  portfast off
%   mlag2: bpdu-guard  default  - Current bpdu-guard off
%   mlag2: bpdu-filter default  - Current bpdu-filter off
%   mlag2: no root guard configured     - Current root guard off
%   mlag2: Configured Link Type point-to-point - Current point-to-point
```

```
%   mlag2: No auto-edge configured - Current port Auto Edge off
%
```

Disabling RSTP Globally

`OcNOS#configure terminal`	Enter Configure mode.
`OcNOS(config)# no bridge 1 provider-rstp enable bridge-forward`	Disable spanning tree globally for Provider-RSTP and keeping the ports in Forwarding state.
`OcNOS(config)# interface mlag1`	Configure interface mlag1
`OcNOS(config-if)# switchport`	Configure the interface as switchport
`OcNOS(config-if)# bridge-group 1`	Assign the above created bridge to this port.
`OcNOS(config-vrf)#exit`	Exit from interface mode to config mode

Validation

```
OcNOS#sh run int mlag2
!
interface mlag2
 switchport
 bridge-group 1 spanning-tree disable
 switchport mode provider-network
!
OcNOS#sh run int mlag1
!
interface mlag1
 switchport
 bridge-group 1
 switchport mode provider-network
!
OcNOS#
OcNOS#sh spanning-tree
% 1: Bridge up - Spanning Tree Disabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8000000000000000
% 1: Bridge Id 8000000000000000
% 1: 2 topology change(s)  - last topology change Tue Jul 30 06:47:37 2019

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   xe13/2: Port Number 942 - Ifindex 5038 - Port Id 0x83ae - Role Disabled - State
Forwarding
%   xe13/2: Designated Path Cost 0
%   xe13/2: Configured Path Cost 2000  - Add type Explicit ref count 1
%   xe13/2: Designated Port Id 0x83ae - Priority 128  -
%   xe13/2: Message Age 0 - Max Age 20
%   xe13/2: Hello Time 2 - Forward Delay 15
%   xe13/2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   xe13/2: forward-transitions 4
```


© 2021 IP Infusion Inc. Proprietary

```
%   xe13/2: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   xe13/2: No portfast configured - Current  portfast off
%   xe13/2: bpdu-guard  default  - Current bpdu-guard off
%   xe13/2: bpdu-filter default  - Current bpdu-filter off
%   xe13/2: no root guard configured     - Current root guard off
%   xe13/2: Configured Link Type point-to-point - Current point-to-point
%   xe13/2: No auto-edge configured - Current port Auto Edge off
%
%   po1: Port Number 1697 - Ifindex 100001 - Port Id 0x86a1 - Role Disabled - State
Forwarding
%   po1: Designated Path Cost 0
%   po1: Configured Path Cost 2000  - Add type Explicit ref count 1
%   po1: Designated Port Id 0x86a1 - Priority 128  -
%   po1: Message Age 0 - Max Age 20
%   po1: Hello Time 2 - Forward Delay 15
%   po1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   po1: forward-transitions 2
%   po1: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   po1: No portfast configured - Current  portfast off
%   po1: bpdu-guard  default  - Current bpdu-guard off
%   po1: bpdu-filter default  - Current bpdu-filter off
%   po1: no root guard configured     - Current root guard off
%   po1: Configured Link Type point-to-point - Current point-to-point
%   po1: No auto-edge configured - Current port Auto Edge off
%
%   mlag1: Port Number 2689 - Ifindex 400001 - Port Id 0x8a81 - Role Disabled - State
Forwarding
%   mlag1: Designated Path Cost 0
%   mlag1: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   mlag1: Designated Port Id 0x0 - Priority 128  -
%   mlag1: Message Age 0 - Max Age 0
%   mlag1: Hello Time 0 - Forward Delay 0
%   mlag1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   mlag1: forward-transitions 2
%   mlag1: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   mlag1: No portfast configured - Current  portfast off
%   mlag1: bpdu-guard  default  - Current bpdu-guard off
%   mlag1: bpdu-filter default  - Current bpdu-filter off
%   mlag1: no root guard configured     - Current root guard off
%   mlag1: Configured Link Type point-to-point - Current point-to-point
%   mlag1: No auto-edge configured - Current port Auto Edge off
%
%   mlag2: Port Number 2690 - Ifindex 400002 - Port Id 0x8a82 - Role Disabled - State
Forwarding
%   mlag2: Designated Path Cost 0
%   mlag2: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   mlag2: Designated Port Id 0x0 - Priority 128  -
%   mlag2: Message Age 0 - Max Age 0
%   mlag2: Hello Time 0 - Forward Delay 0
%   mlag2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   mlag2: forward-transitions 2
```

```
%   mlag2: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   mlag2: No portfast configured - Current  portfast off
%   mlag2: bpdu-guard  default  - Current bpdu-guard off
%   mlag2: bpdu-filter default  - Current bpdu-filter off
%   mlag2: no root guard configured     - Current root guard off
%   mlag2: Configured Link Type point-to-point - Current point-to-point
%   mlag2: No auto-edge configured - Current port Auto Edge off
%
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 8 MSTP Configuration

This chapter contains a complete sample Multiple Spanning Tree Protocol (MSTP) configuration. MSTP allows multiple VLANs to be grouped into one spanning-tree instance. Every MST instance has a spanning-tree that is independent of other spanning-tree instances providing multiple forwarding paths for data traffic.

Topology

This example gives a simple multi-bridge topology and its configuration.

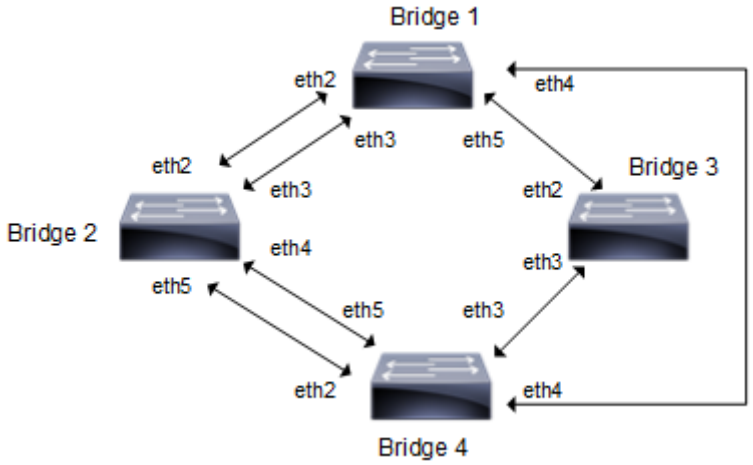


Figure 8-69: MSTP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Configuration

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol mstp`	Add a bridge (1) to the multiple spanning tree table.
`Bridge1(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge1(config-vlan)#vlan 2 bridge 1 state enable`	Enable the state of VLAN 2 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 1.
`Bridge1(config-vlan)#vlan 3 bridge 1 state enable`	Enable the state of VLAN 3 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 1.
`Bridge1(config-vlan)#vlan 4 bridge 1 state enable`	Enable the state of VLAN 4 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 1.
`Bridge1(config-vlan)#vlan 5 bridge 1 state enable`	Enable the state of VLAN 5 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 1.
`Bridge1(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge1(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree

`Bridge1(config-mst)#bridge 1 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 3 vlan 3`	Create another instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 4 vlan 4`	same as mention above.
`Bridge1(config-mst)#bridge 1 instance 5 vlan 5`	same as mention above.
`Bridge1(config-mst)#exit`	Exit MST Configuration mode.
`Bridge1(config)#interface eth2`	Enter interface mode for eth2
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode for eth3.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode for eth4.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter interface mode for eth5.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1

© 2021 IP Infusion Inc. Proprietary

`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol mstp`	Add a bridge (2) to the multiple spanning
`Bridge2(config)#bridge 2 priority 4096`	Assign priority to this bridge.
`Bridge2(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge2(config-vlan)#vlan 2 bridge 2 state enable`	Enable the state of VLAN 2 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 2.
`Bridge2(config-vlan)#vlan 3 bridge 2 state enable`	Enable the state of VLAN 3 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 2
`Bridge2(config-vlan)#vlan 4 bridge 2 state enable`	Enable the state of VLAN 4 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 2
`Bridge2(config-vlan)#vlan 5 bridge 2 state enable`	Enable the state of VLAN 5 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 2
`Bridge2(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge2(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree configuration mode
`Bridge2(config-mst)#bridge 2 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#bridge 2 instance 3 vlan 3`	same as mention above.
`Bridge2(config-mst)#bridge 2 instance 4 vlan 4`	same as mention above.
`Bridge2(config-mst)#bridge 2 instance 5 vlan 5`	same as mention above.
`Bridge2(config-mst)#exit`	Exit MST Configuration mode.
`Bridge2(config)#interface eth2`	Enter interface mode for eth2
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance

`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode for eth3
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3 priority 16`	Assign bridge-group 2 to this instance and set a port priority in order of 16 for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4 priority 16`	Assign bridge-group 2 to this instance and set a port priority in order of 16 for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#exit`	Exit interface mode
`Bridge2(config)#interface eth4`	Enter interface mode for eth4
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode for eth5
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol mstp`	Add a bridge (3) to the multiple spanning tree table
`Bridge3(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge3(config-vlan)#vlan 2 bridge 3 state enable`	Enable the state of VLAN 2 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 3.
`Bridge3(config-vlan)#vlan 3 bridge 3 state enable`	Enable the state of VLAN 3 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 3.
`Bridge3(config-vlan)#vlan 4 bridge 3 state enable`	Enable the state of VLAN 4 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 3.
`Bridge3(config-vlan)#vlan 5 bridge 3 state enable`	Enable the state of VLAN 5 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 3.
`Bridge3(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge3(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.
`Bridge3(config-mst)#bridge 3 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#bridge 3 instance 3 vlan 3`	same as mention above.
`Bridge3(config-mst)#bridge 3 instance 4 vlan 4`	same as mention above.
`Bridge3(config-mst)#bridge 3 instance 5 vlan 5`	same as mention above.
`Bridge3(config-mst)#exit`	Exit MST Configuration mode.
`Bridge3(config)#interface eth2`	Enter interface mode for eth2
`Bridge3(config-if)#bridge-group 3`	Associating the interface to bridge-group 3
`Bridge3(config-if)#bridge-group 3 instance 2`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 3`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 4`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 5`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode for eth3
`Bridge3(config-if)#bridge-group 3`	Associating the interface to bridge-group 3

© 2021 IP Infusion Inc. Proprietary

`Bridge3(config-if)#bridge-group 3 instance 2`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 3`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 4`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 5`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#exit`	Exit interface mode.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol mstp`	Add a bridge (4) to the multiple spanning tree table
`Bridge4(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge4(config-vlan)#vlan 2 bridge 4 state enable`	Enable the state of VLAN 2 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 4.
`Bridge4(config-vlan)#vlan 3 bridge 4 state enable`	Enable the state of VLAN 3 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 4.
`Bridge4(config-vlan)#vlan 4 bridge 4 state enable`	Enable the state of VLAN 4 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 4.
`Bridge4(config-vlan)#vlan 5 bridge 4 state enable`	Enable the state of VLAN 5 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 4.
`Bridge4(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge4(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.
`Bridge4(config-mst)#bridge 4 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#bridge 4 instance 3 vlan 3`	same as mention above.
`Bridge4(config-mst)#bridge 4 instance 4 vlan 4`	same as mention above.
`Bridge4(config-mst)#bridge 4 instance 5 vlan 5`	same as mention above.
`Bridge4(config-mst)#exit`	Exit MST Configuration mode.
`Bridge4(config)#interface eth2`	Enter interface mode for eth2
`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode for eth3

© 2021 IP Infusion Inc. Proprietary

`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode for eth4
`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode for eth5
`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#exit`	Exit interface mode.

Validation

show spanning-tree, show spanning-tree mst detail

```
#show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 3 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 1000525400d15789
% 1: CIST Reg Root Id 1000525400d15789
% 1: CIST Bridge Id 8000525400244323
% 1: 26 topology change(s)  - last topology change Mon Mar  4 12:58:35 2019

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
```

```
% 1: portfast errdisable timeout interval 300 sec
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Rootport - State
Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth1: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth1: Designated Port Id 0x8003 - CIST Priority 128  -
%   eth1: CIST Root 1000525400d15789
%   eth1: Regional Root 1000525400d15789
%   eth1: Designated Bridge 1000525400d15789
%   eth1: Message Age 0 - Max Age 20
%   eth1: CIST Hello Time 2 - Forward Delay 15
%   eth1: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change
timer 0
%   eth1: forward-transitions 1
%   eth1: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth2: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
%   eth2: CIST Root 1000525400d15789
%   eth2: Regional Root 1000525400d15789
%   eth2: Designated Bridge 1000525400d15789
%   eth2: Message Age 0 - Max Age 20
%   eth2: CIST Hello Time 2 - Forward Delay 15
%   eth2: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change
timer 0
%   eth2: forward-transitions 2
%   eth2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth3: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400d15789
%   eth3: Regional Root 1000525400d15789
%   eth3: Designated Bridge 8000525400244323
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   eth3: forward-transitions 3
%   eth3: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
%   eth3: No portfast configured - Current  portfast off
```


© 2021 IP Infusion Inc. Proprietary

```
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth4: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400d15789
%   eth4: Regional Root 1000525400d15789
%   eth4: Designated Bridge 8000525400244323
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   eth4: forward-transitions 3
%   eth4: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8002525400244323
% 1: MSTI Bridge Id 8002525400244323
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 20000
%   eth1: Configured CST External Path cost 20000
%   eth1: CST Priority 128  - MSTI Priority 128
%   eth1: Designated Root 8002525400244323
%   eth1: Designated Bridge 8002525400244323
%   eth1: Message Age 0
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 20000
%   eth2: Configured CST External Path cost 20000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8002525400244323
%   eth2: Designated Bridge 8002525400244323
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
```

```
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 20000
%   eth3: Configured CST External Path cost 20000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 8002525400244323
%   eth3: Designated Bridge 8002525400244323
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 20000
%   eth4: Configured CST External Path cost 20000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 8002525400244323
%   eth4: Designated Bridge 8002525400244323
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1


% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8003525400244323
% 1: MSTI Bridge Id 8003525400244323
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Masterport - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 20000
%   eth1: Configured CST External Path cost 20000
%   eth1: CST Priority 128  - MSTI Priority 128
%   eth1: Designated Root 8003525400244323
%   eth1: Designated Bridge 8003525400244323
%   eth1: Message Age 0
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 20000
%   eth2: Configured CST External Path cost 20000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8003525400244323
%   eth2: Designated Bridge 8003525400244323
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 20000
```

 © 2021 IP Infusion Inc. Proprietary

```
%   eth3: Configured CST External Path cost 20000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 8003525400244323
%   eth3: Designated Bridge 8003525400244323
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 20000
%   eth4: Configured CST External Path cost 20000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 8003525400244323
%   eth4: Designated Bridge 8003525400244323
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1


% Instance  4:  Vlans: 4

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8004525400244323
% 1: MSTI Bridge Id 8004525400244323
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Masterport - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 20000
%   eth1: Configured CST External Path cost 20000
%   eth1: CST Priority 128  - MSTI Priority 128
%   eth1: Designated Root 8004525400244323
%   eth1: Designated Bridge 8004525400244323
%   eth1: Message Age 0
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 20000
%   eth2: Configured CST External Path cost 20000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8004525400244323
%   eth2: Designated Bridge 8004525400244323
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 20000
%   eth3: Configured CST External Path cost 20000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 8004525400244323
```

```
%   eth3: Designated Bridge 8004525400244323
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 20000
%   eth4: Configured CST External Path cost 20000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 8004525400244323
%   eth4: Designated Bridge 8004525400244323
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1


% Instance  5:  Vlans: 5

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8005525400244323
% 1: MSTI Bridge Id 8005525400244323
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Masterport - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 20000
%   eth1: Configured CST External Path cost 20000
%   eth1: CST Priority 128  - MSTI Priority 128
%   eth1: Designated Root 8005525400244323
%   eth1: Designated Bridge 8005525400244323
%   eth1: Message Age 0
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 20000
%   eth2: Configured CST External Path cost 20000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8005525400244323
%   eth2: Designated Bridge 8005525400244323
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 20000
%   eth3: Configured CST External Path cost 20000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 8005525400244323
%   eth3: Designated Bridge 8005525400244323
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
```


© 2021 IP Infusion Inc. Proprietary

```
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 20000
%   eth4: Configured CST External Path cost 20000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 8005525400244323
%   eth4: Designated Bridge 8005525400244323
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1


#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 3 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 1000525400d15789
% 1: CIST Reg Root Id 1000525400d15789
% 1: CIST Bridge Id 8000525400244323
% 1: 26 topology change(s)  - last topology change Mon Mar  4 12:58:35 2019

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Rootport - State
Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth1: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth1: Designated Port Id 0x8003 - CIST Priority 128  -
%   eth1: CIST Root 1000525400d15789
%   eth1: Regional Root 1000525400d15789
%   eth1: Designated Bridge 1000525400d15789
%   eth1: Message Age 0 - Max Age 20
%   eth1: CIST Hello Time 2 - Forward Delay 15
%   eth1: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change
timer 0
%   eth1: forward-transitions 1
%   eth1: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth2: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
%   eth2: CIST Root 1000525400d15789
%   eth2: Regional Root 1000525400d15789
%   eth2: Designated Bridge 1000525400d15789
```

```
%   eth2: Message Age 0 - Max Age 20
%   eth2: CIST Hello Time 2 - Forward Delay 15
%   eth2: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change
timer 0
%   eth2: forward-transitions 2
%   eth2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth3: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400d15789
%   eth3: Regional Root 1000525400d15789
%   eth3: Designated Bridge 8000525400244323
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   eth3: forward-transitions 3
%   eth3: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 20000
%   eth4: Configured Path Cost 20000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400d15789
%   eth4: Regional Root 1000525400d15789
%   eth4: Designated Bridge 8000525400244323
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 3
%   eth4: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off%
#
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 9 Port Security Configuration

The Port Security feature allows network administrators to block unauthorized access to the network. Network administrators can configure each port of the switch to allow network access from only secured MACs, so that the switch forwards traffic from only secured MACs.

Users can limit each port's ingress traffic by limiting MAC addresses (source MACs) that are used to send traffic into ports. Port Security enables users to configure the maximum number of secured MACs for each port. Switches learn secured MAC dynamically (learned by switch during traffic inflow) or statically (User configured MACs). Dynamically Learned or statically programmed MAC addresses cannot exceed the maximum number of secured MACs configured for a particular port. Once the switch reaches the maximum limit for secured MACs, traffic from all other MAC addresses are dropped.

The violated MACs are logged in syslog messages. Refer to `cpu queue portsec-drop` using the command `show interface cpu counter queue-stats` for information on the number of violated MACs.

Secured MACs Learned Dynamically



Figure 9-70: Secured MACs learned dynamically

Send Layer-2 traffic with incremental source MAC of 100 and with VLAN 100 from IXIA1 and since max limit is configured as 3 – only 3 secure MAC addresses will be learned by SW1.

SW1

`#configure terminal`	Enter configure mode.
`(config)#hostname SW1`	Set the host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan 2-200 bridge 1 state enable`	Configure VLAN for the bridge
`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as trunk
`(config-if)#switchport hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#switchport port-security`	Enable port security mode dynamic
`(config-if)#switchport port-security maximum 3`	Limit secure MAC to 3 mac addresses.
`(config-if)#exit`	Exit interface mode
`(config)#interface ge2`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as trunk

© 2021 IP Infusion Inc. Proprietary

`(config-if)#switchport hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#exit`	Exit interface mode
`(config)#logging monitor 7`	Enable logging level as 7 for debugging

Validation

Validation commands are "`show port-security`," "`show port-security interface <ifname>`," "`show mac address-table count bridge 1`," "`show bridge`," and "`show mac address-table bridge 1`."

```
SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
-------+-------------------+---------+------+------+-----------------
ge1     dynamic             3

SW1#show port-security interface ge1
Port Security Mode     : Dynamic
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+---------------

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 3
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         100                  ge1         0000.0300.0500    1     100
 1         100                  ge1         0000.0300.055b    1     100
 1         100                  ge1         0000.0300.055c    1     100

SW1#show mac address-table bridge 1
 VLAN   MAC Address     Type      Ports     Port-security
------+--------------+---------+---------+--------------
 100   0000.0300.0500   dynamic   ge1       Enable
 100   0000.0300.055b   dynamic   ge1       Enable
 100   0000.0300.055c   dynamic   ge1       Enable
SW1#
```


© 2021 IP Infusion Inc. Proprietary

Secured MAC Addresses Learned Statically

1. Stop the traffic from IXIA1 and do "`clear mac address-table dynamic bridge 1`" on SW1.
2. Verify all dynamic secured MAC addresses are cleared.
3. Configure 3 static secure MAC addresses using the commands below in port security configured interface.
4. Try to add a fourth static secure MAC address.
5. Verify operator log message is displayed, saying "`port security mac limit reached`."

`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaaa vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaab vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaac vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode

Validation

```
SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
------+-------------------+---------+------+------+-----------------
ge1     dynamic             3          100           0000.0000.aaaa
                                       100           0000.0000.aaab
                                       100           0000.0000.aaac

SW1#show port-security interface ge1
Port Security Mode     : Dynamic
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+----------------
 100           0000.0000.aaaa
 100           0000.0000.aaab
 100           0000.0000.aaac

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 0
Static (User-defined) Unicast MAC Address Count: 3
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
```

```
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         100                  ge1         0000.0000.aaaa    1     -
 1         100                  ge1         0000.0000.aaab    1     -
 1         100                  ge1         0000.0000.aaac    1     -

SW1#show mac address-table bridge 1
 VLAN   MAC Address     Type      Ports     Port-security
------+---------------+---------+---------+--------------
 100   0000.0000.aaaa   static    ge1       Enable
 100   0000.0000.aaab   static    ge1       Enable
 100   0000.0000.aaac   static    ge1       Enable
SW1#
```

Remove the port-security configuration method using the two commands below:

(

`config)#interface ge1`	Enter interface mode
`(config-if)#no switchport port-security`	Set the port-security method to static.

Static Mode

Use the below command to configure the port-security method to static and configure static secure MAC addresses using the commands the in static port-security method, below.

`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport port-security static`	Set the port-security method as static.
`(config-if)#switchport port-security max 3`	Limit static secure MAC to 3 mac addresses.
`(config-if)#switchport port-security mac-address 0000.0000.aaaa vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode.
`(config-if)#switchport port-security mac-address 0000.0000.aaab vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode.
`(config-if)#switchport port-security mac-address 0000.0000.aaac vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode .

Verify the 3 secure static MAC addresses are added in interface ge1 using show running-config and also verify the port-security method should be static using below show commands.

Validation

```
SW1#show running-config interface ge1
interface ge1
 switchport
bridge-group 1
  switchport mode hybrid
 switchport hybrid allowed vlan all
 switchport port-security static
 switchport port-security maximum 3
 switchport port-security mac-address 0000.0000.aaaa vlanId 100
 switchport port-security mac-address 0000.0000.aaab vlanId 100
 switchport port-security mac-address 0000.0000.aaac vlanId 100
```


© 2021 IP Infusion Inc. Proprietary

```
SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
------+------------------+---------+------+------+-----------------
ge1     static              3        100          0000.0000.aaaa
                                        100          0000.0000.aaab
                                       100          0000.0000.aaac

SW1#show port-security interface ge1
Port Security Mode     : Static
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+----------------
 100          0000.0000.aaaa
 100          0000.0000.aaab
 100          0000.0000.aaac

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 0
Static (User-defined) Unicast MAC Address Count: 3
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         100                  ge1         0000.0000.aaaa    1     -
 1         100                  ge1         0000.0000.aaab    1     -
 1         100                  ge1         0000.0000.aaac    1     -

 SW1#show mac address-table bridge 1
 VLAN   MAC Address     Type      Ports     Port-security
------+--------------+---------+---------+-------------
 100   0000.0000.aaaa   static    ge1       Enable
 100   0000.0000.aaab   static    ge1       Enable
 100   0000.0000.aaac   static    ge1       Enable
SW1#
```

Configure one more static secure MAC address on interface ge1 and try to verify "`port security mac limit reached`" operator log message is displayed.

Start sending Layer-2 traffic with incremental source MAC of 100 and with VLAN 100 from IXIA1, and verify no dynamic secure MAC addresses are being learned using all the validation commands used.

Port Security using MC-LAG

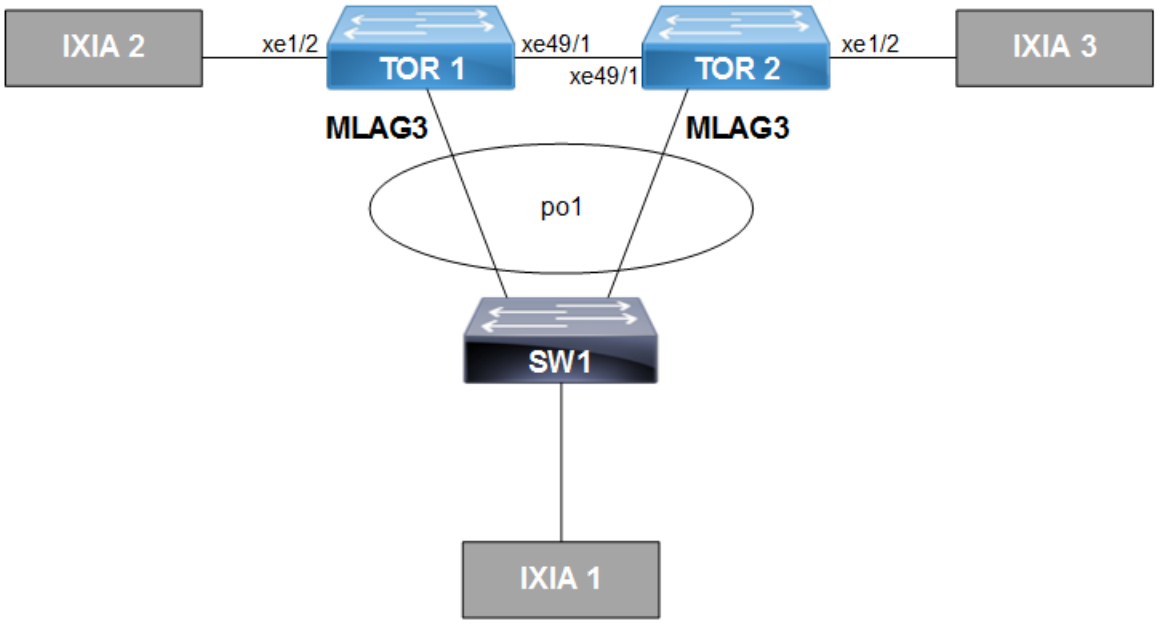


Figure 9-71: Port security with MC-LAG

TOR1

`#configgure termonal`	Enter configure mode
`(config)#bridge 1 protocol provider-rstp edge`	Create provider RSTP bridge
`(config)#vlan 2-10 type customer bridge 1 state enable`	Enabling customer vlan for bridge
`(config)#vlan 2-10 type service point-point bridge 1 state enable`	Enabling service vlan for bridge
`(config)#cvlan registration table map1 bridge 1`	Creating registration table
`(config-cvlan-registation)#cvlan 2 svlan 2`	Mapping CVLAN to SVLAN
`(config-cvlan-registation)#cvlan 10 svlan 2`	Mapping CVLAN to SVLAN
`(config-cvlan-registation)#exit`	Exit registration table mode
`(config)#interface mlag3`	Entering MLAG interface
`(config-if)#switchport`	Configuring interface as switchport
`(config-if)#exit`	Exit interface mode
`(config)#interface po1`	Entering dynamic lag interface
`(config-if)#switchport`	Configuring interface as switchport
`(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1and disabling spanning-tree
`(config-if)#switchport mode customer-edge hybrid`	Set the switching characteristics of this interface to customer edge hybrid
`(config-if)#switchport customer-edge hybrid vlan 2`	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN 2

© 2021 IP Infusion Inc. Proprietary

(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN all
(config-if)#mlag 3	Enabling mlag group number
(config-if)#exit	Exit interface mode
(config)#interface xe49/1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode provider-network	Set the switching characteristics of this interface to provider network
(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all VLAN
(config-if)#exit	Enter interface mode
(config)#interface xe3	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer edge hybrid
(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer edge hybrid and allow vlan 2
(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN all
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
(config-if)#exit	Exit interface mode
(config)#interface mlag3	Entering MLAG interface
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer edge hybrid
(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN 2
(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN all
(config-if)#switchport customer-edge vlan registration map1	Configuring the registration table mapping on MLAG interface
(config-if)#switchport port-security	Enabling port security
(config-if)#switchport port-security maximum 10	Limiting the maximum mac to 10
(config-if)#exit	Exit interface mode
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 2222.2222.2222	Domain address for the MLAG domain
(config-mcec-domain)#domain-system-number 1	Number to identify the node in a domain
(config-mcec-domain)#exit	Exit MCEC mode

(config)#intra-domain-link xe49/1	Intra domain line between MLAG domain
(config-if)#domain-priority 333	Domain priority for MCEC

TOR2

(config-if)#

#configure terminal	Enter configure mode
(config)#bridge 1 protocol provider-rstp edge	Create provider RSTP bridge
(config)#vlan 2-10 type customer bridge 1 state enable	Enabling customer VLAN for bridge
(config)#vlan 2-10 type service point-point bridge 1 state enable	Enabling service VLAN for bridge
(config)#cvlan registration table map1 bridge 1	Creating registration table
(config-cvlan-registation)#cvlan 2 svlan 2	Mapping CVLAN to SVLAN
(config-cvlan-registation)#cvlan 10 svlan 2	Mapping CVLAN to SVLAN
(config-cvlan-registation)#exit	Exit registration table mode
(config)#interface mlag3	Entering MLAG interface
(config-if)#switchport	Configuring interface as switchport
(config-if)#exit	Exit interface mode
(config)#interface po1	Entering dynamic lag interface
(config-if)#Switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer edge hybrid
(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN 2
(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN all
(config-if)#mlag 3	Enabling MLAG group number
(config-if)#exit	Exit interface mode
(config)#interface xe49/1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode provider-network	Set the switching characteristics of this interface to provider network
(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all VLAN
(config-if)#exit	Exit interface mode
(config)#interface xe3	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
bridge-group 1	Associate the interface with bridge group 1
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer edge hybrid

© 2021 IP Infusion Inc. Proprietary

(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN 2
(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN all
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
(config-if)#exit	Exit interface mode
(config)#interface mlag3	Entering MLAG interface
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer edge hybrid
(config-if)#switchport customer-edge hybrid vlan 2	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN 2
(config-if)#switchport customer-edge hybrid allowed vlanall	Set the switching characteristics of this interface to customer edge hybrid and allow VLAN all
(config-if)#switchport customer-edge vlan registration map1	Configuring the registration table mapping on MLAG interface
(config-if)#exit	Exit interface mode
mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 2222.2222.2222	Domain address for the MLAG domain
(config-mcec-domain)#domain-system-number 2	Number to identify the node in a domain
(config-mcec-domain)#intra-domain-link xe49/1	Intra domain line between MLAG domain
(config-mcec-domain)#domain-priority 333	Domain priority for MCEC

SW1

configure terminal	Enter configuration mode
(config)#bridge 1 protocol rstp vlan-bridge	Configuring the RSTP vlan bridge
(config)#interface po1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode hybrid	Set the switching characteristics of this interface hybrid
(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all vlan
(config-if)#exit	Exit interface mode
(config)#interface xe1/3	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode hybrid	Set the switching characteristics of this interface hybrid
(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all vlan

(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode
(config)#interface xe1/1	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disabling spanning-tree
(config-if)#switchport mode hybrid	Set the switching characteristics of this interface hybrid
(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all vlan
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode
(config)#interface xe3/3	Entering interface mode
(config-if)#switchport	Configuring interface as switchport
(config-if)#bridge-group 1	Associate the interface with bridge group 1and disabling spanning-tree
(config-if)#switchport mode hybrid	Set the switching characteristics of this interface hybrid
(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all VLAN

Validation

```
TOR1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1                2             mlag3        0000.0500.0200    1     54
 1                2             mlag3        0000.0500.0201    1     60
 1                2             mlag3        0000.0500.0202    1     54
 1                2             mlag3        0000.0500.0203    1     60
 1                2             mlag3        0000.0500.0204    1     54
 1                2             mlag3        0000.0500.0205    1     60
 1                2             mlag3        0000.0500.0207    1     60
 1                2             mlag3        0000.0500.0208    1     54
 1                2             mlag3        0000.0500.0209    1     60
 1                2             mlag3        0000.0500.020a    1     54
 1                2             mlag3        0000.0500.020b    1     60
 1                2             mlag3        0000.0500.020c    1     54
 1                2             mlag3        0000.0500.020d    1     60
 1                2             mlag3        0000.0500.020e    1     54
 1                2             mlag3        0000.0500.020f    1     60
 1                2             mlag3        0000.0500.0210    1     54
 1                2             mlag3        0000.0500.0211    1     60
 1                2             mlag3        0000.0500.0212    1     54
 1                2             mlag3        cc37.abbb.ed9b    1     40
```


© 2021 IP Infusion Inc. Proprietary

```
TOR1#sh port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
-------+------------------+---------+------+------+-----------------
Mlag3   dynamic             10
TOR1#
TOR1#show mac address-table count bridge 1 interface mlag3
MAC Entries for all vlans:
Dynamic Address Count: 20
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 20
TOR1#
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 10 RPVST+ Configuration

This chapter contains a complete example of an RPVST+ configuration.

Topology



Figure 10-72: RPVST+ configuration

Configuration

Switch 2

`#configure terminal`	Enter configure mode for the switch.
`(config)#bridge 1 protocol rpvst+`	Configure bridge 1 as an RPVST+ bridge.
`(config)#vlan 2-3 bridge 1`	Configure VLAN 2 and 3 and associate it to bridge 1.
`(config)#spanning-tree rpvst+ configuration`	Enter Rapid Per-VLAN Spanning Tree configuration mode.
`(config-rpvst+)#bridge 1 vlan 2`	Associate a configured VLAN with bridge 1.
`(config-rpvst+)#bridge 1 vlan 3`	Associate a configured VLAN with bridge 1,.
`(config-rvpst+)#exit`	Exit RPVST+ configuration mode.
`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#switchport`	Configure `eth1` as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface.
`(config-if)#switchport mode trunk`	Configure port as trunk.
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#bridge-group 1 vlan 2`	Configure bridge group to interface with VLAN 2.
`(config-if)#bridge-group 1 vlan 3`	Configure bridge group to interface with VLAN 3.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`.
`(config-if)#switchport`	Configure `eth2` as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface/
`(config-if)#switchport mode trunk`	Configure port as trunk
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#bridge-group 1 vlan 2`	Configure bridge group to interface with VLAN 2.
`(config-if)#bridge-group 1 vlan 3`	Configure bridge group to interface with VLAN3.
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

Switch 1

`#configure terminal`	Enter configure mode for the switch.
`(config)#bridge 1 protocol rpvst+`	Configure bridge 1 as an rpvst+ bridge.
`(config)#vlan 2-3 bridge 1`	Configure VLAN 2 and 3 and associate it to bridge 1.
`(config)#spanning-tree rpvst+ configuration`	Enter Rapid Per-VLAN Spanning Tree configuration mode.
`(config-rpvst+)#bridge 1 vlan 2`	Associate a configured VLAN with bridge 1.
`(config-rpvst+)#bridge 1 vlan 3`	Associate a configured VLAN with bridge 1.
`(config-rvpst+)#exit`	Exit RPVST+ configuration mode.
`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#switchport`	Configure `eth1` as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface.
`(config-if)#switchport mode trunk`	Configure port as trunk.
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#bridge-group 1 vlan 2`	Configure bridge group to interface with VLAN 2.
`(config-if)#bridge-group 1 vlan 3`	Configure bridge group to interface with VLAN3.
`(config-if)#exit`	Exit interface mode.

Switch 3

`#configure terminal`	Enter configure mode for the switch.
`(config)#bridge 1 protocol rpvst+`	Configure bridge 1 as an rpvst+ bridge
`(config)#vlan 2-3 bridge 1`	Configure VLAN 2 and 3 and associate it to bridge 1.
`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#switchport`	Configure `eth1` as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface.
`(config-if)#switchport mode trunk`	Configure port as trunk.
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#exit`	Exit interface mode.

Validation

Switch2

```
#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b7bfa7
% 1: Bridge Id 8002525400b7bfa7
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
```


© 2021 IP Infusion Inc. Proprietary

```
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b7bfa7
%   eth1: Designated Bridge 8002525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128
%   eth2: Configured External Priority 128
%   eth2: Designated Root 8002525400b7bfa7
%   eth2: Designated Bridge 8002525400b7bfa7
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%

#show spanning-tree rpvst+ interface eth1
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8001525400b7bfa7
% 1: Bridge Id 8001525400b7bfa7
% 1: last topology change Wed Mar 28 15:33:06 2018
% 1: 2 topology change(s)  - last topology change Wed Mar 28 15:33:06 2018

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 3
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 8001525400b7bfa7
%   eth1: Designated Bridge 8001525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 2 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth1: No portfast configured - Current  portfast off
```

```
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%
%
%   Instance        VLAN
%   0:              1
%   1:              2
%   2:              3



#show spanning-tree rpvst+ detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8001525400b7bfa7
% 1: Bridge Id 8001525400b7bfa7
% 1: last topology change Wed Mar 28 15:33:06 2018
% 1: 2 topology change(s)  - last topology change Wed Mar 28 15:33:06 2018

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 3
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 8001525400b7bfa7
%   eth1: Designated Bridge 8001525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 0
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 3
%   eth2: Designated Port Id 0x8004 - Priority 128  -
```


© 2021 IP Infusion Inc. Proprietary

```
%   eth2: Root 8001525400b7bfa7
%   eth2: Designated Bridge 8001525400b7bfa7
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%

% Instance  1:  Vlans: 2
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b7bfa7
%   eth1: Designated Bridge 8002525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0


% Instance  1:  Vlans: 2
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128
%   eth2: Configured External Priority 128
%   eth2: Designated Root 8002525400b7bfa7
%   eth2: Designated Bridge 8002525400b7bfa7
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1


% Instance  2:  Vlans: 3
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
```

```
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8003525400b7bfa7
%   eth1: Designated Bridge 8003525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0


% Instance  2:  Vlans: 3
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128
%   eth2: Configured External Priority 128
%   eth2: Designated Root 8003525400b7bfa7
%   eth2: Designated Bridge 8003525400b7bfa7
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 11 RSTP Configuration

This chapter contains a complete sample Rapid Spanning Tree Protocol (RSTP) configuration. RSTP provides rapid convergence of a spanning tree. It speeds up the reconfiguration of the tree after a change by using alternate ports.

Topology

The following example is a simple multi-bridge topology.

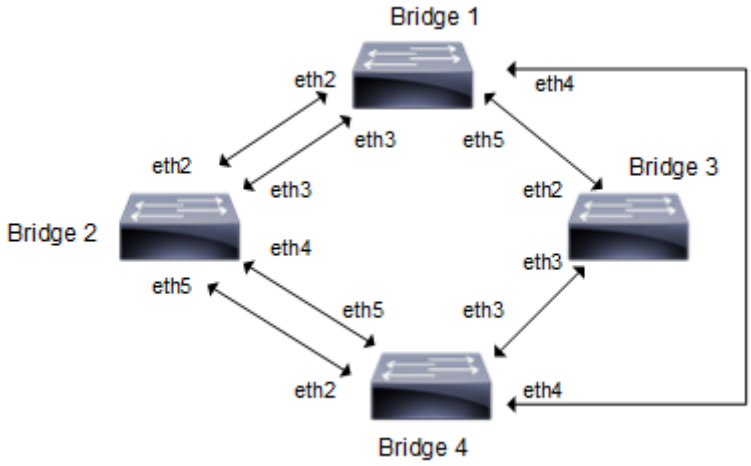


Figure 11-73: RSTP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Configuration

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol rstp`	Add a bridge (`1`) to the rapid spanning tree table
`Bridge1(config)#interface eth2`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.

`Bridge1(config)#interface eth5`	Enter interface mode
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol rstp`	Add a bridge (`2`) to the rapid spanning tree table
`Bridge2(config)#interface eth2`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth4`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol rstp`	Add a bridge `(3)` to the rapid spanning tree table
`Bridge3(config)#interface eth2`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config)#interface eth3`	Enter interface mode.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol rstp`	Add a bridge `(4)` to the rapid spanning tree table
`Bridge4(config)#interface eth2`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge3(config-if)#exit`	

Validation

show spanning-tree, show spanning-tree interface <if-name>

Bridge 1

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 200000 - Root Port 6 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8000525400046f549
% 1: Bridge Id 80005254009cb7e6
% 1: last topology change Tue Aug 11 02:25:01 2020
% 1: 30 topology change(s)  - last topology change Tue Aug 11 02:25:01 2020

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 8000525400046f549
%   eth2: Designated Bridge 8000525400751db5
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
```

```
%   eth2: forward-transitions 2
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 8000525400751db5
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 3
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8006 - Priority 128  -
%   eth4: Root 800052540046f549
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 6
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8004 - Priority 128  -
%   eth5: Root 800052540046f549
```


© 2021 IP Infusion Inc. Proprietary

```
%   eth5: Designated Bridge 800052540065fd8c
%   eth5: Message Age 1 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth5: forward-transitions 4
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
#
```

Bridge 2

```
#show spanning-tree
% 2: Bridge up - Spanning Tree Enabled  - topology change detected
% 2: Root Path Cost 200000 - Root Port 7 -  Bridge Priority 32768
% 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 2: Root Id 800052540046f549
% 2: Bridge Id 8000525400751db5
% 2: last topology change Tue Aug 11 02:25:00 2020
% 2: 22 topology change(s)  - last topology change Tue Aug 11 02:25:00 2020

% 2: portfast bpdu-filter disabled
% 2: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 8000525400751db5
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth2: forward-transitions 3
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 8000525400751db5
```

```
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 3
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Alternate - State
Discarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8007 - Priority 128  -
%   eth4: Root 800052540046f549
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 3
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Rootport - State
Forwarding
%   eth5: Designated Path Cost 0
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8004 - Priority 128  -
%   eth5: Root 800052540046f549
%   eth5: Designated Bridge 800052540046f549
%   eth5: Message Age 0 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   eth5: forward-transitions 2
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
#
```


© 2021 IP Infusion Inc. Proprietary

Bridge 3

```
#show spanning-tree
% 3: Bridge up - Spanning Tree Enabled  - topology change detected
% 3: Root Path Cost 200000 - Root Port 5 -  Bridge Priority 32768
% 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 3: Root Id 800052540046f549
% 3: Bridge Id 800052540065fd8c
% 3: last topology change Tue Aug 11 02:25:00 2020
% 3: 16 topology change(s)  - last topology change Tue Aug 11 02:25:00 2020

% 3: portfast bpdu-filter disabled
% 3: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 800052540065fd8c
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   eth2: forward-transitions 2
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Rootport - State
Forwarding
%   eth3: Designated Path Cost 0
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 800052540046f549
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 2
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
#
```

Bridge 4

```
#show spanning-tree
```

```
% 4: Bridge up - Spanning Tree Enabled  - topology change detected
% 4: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 4: Root Id 800052540046f549
% 4: Bridge Id 800052540046f549
% 4: last topology change Tue Aug 11 02:24:58 2020
% 4: 6 topology change(s)  - last topology change Tue Aug 11 02:24:58 2020

% 4: portfast bpdu-filter disabled
% 4: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Path Cost 0
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 800052540046f549
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Path Cost 0
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 800052540046f549
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 1
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8006 - Priority 128  -
%   eth4: Root 800052540046f549
```


© 2021 IP Infusion Inc. Proprietary

```
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 1
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated Path Cost 0
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8007 - Priority 128  -
%   eth5: Root 800052540046f549
%   eth5: Designated Bridge 800052540046f549
%   eth5: Message Age 0 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth5: forward-transitions 1
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
#
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 12 Spanning Tree Protocol Configuration

This chapter contains a complete sample Spanning Tree Protocol (STP) configuration.

Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops. Spanning tree also allows a network design to include redundant links to provide automatic backup paths if an active link fails, thus, eliminating the need to manually enable or disable the backup links.

Topology

The following example is a simple multi-bridge topology.

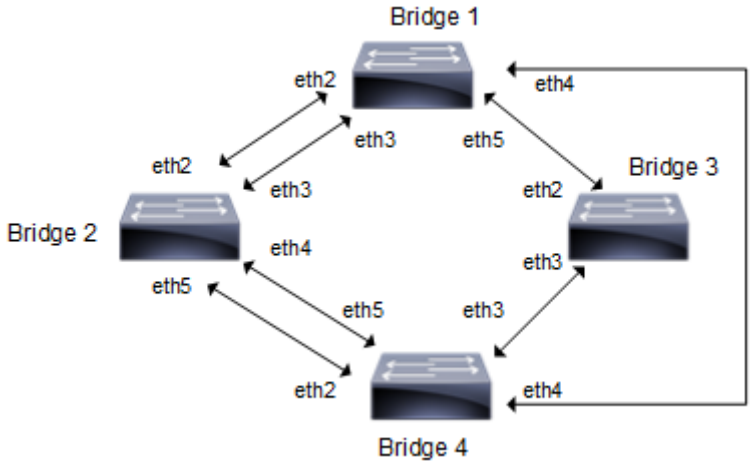


Figure 12-74: STP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Configurations

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol ieee`	Add a bridge `(1)` to the spanning tree table
`Bridge1(config)#interface eth2`	Enter interface mode.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.

`Bridge1(config)#interface eth5`	Enter interface mode
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol ieee`	Add a bridge (`2`) to the spanning tree table
`Bridge2(config)#interface eth2`	Enter interface mode.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth4`	Enter interface mode.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol ieee`	Add a bridge (`4`) to the spanning tree table
`Bridge4(config)#interface eth2`	Enter interface mode.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol ieee`	Add a bridge `(3)` to the spanning tree table
`Bridge3(config)#interface eth2`	Enter interface mode.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

`Bridge3(config)#interface eth3`	Enter interface mode.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.

Validation

show spanning-tree, show spanning-tree interface <if-name>

Bridge 1

```
#show spanning-tree
 1: Bridge up - Spanning Tree Enabled - topology change detected
 1: Root Path Cost 19 - Root Port 6 - Bridge Priority 32768
 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
 1: Root Id 800052540046f549
 1: Bridge Id 80005254009cb7e6
 1: last topology change Tue Aug 11 02:25:01 2020
 1: 30 topology change(s) - last topology change Tue Aug 11 02:25:01 2020
 1: portfast bpdu-filter disabled
 1: portfast bpdu-guard disabled
 eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 -State Blocked
 eth2: Designated Path Cost 19
 eth2: Configured Path Cost 19 - Add type Explicit ref count 1
 eth2: Designated Port Id 0x8004 - Priority 128 -
 eth2: Root 800052540046f549
 eth2: Designated Bridge 8000525400751db5
 eth2: Message Age 1 - Max Age 20
 eth2: Hello Time 2 - Forward Delay 15
 eth2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0
 eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - State blocked
 eth3: Designated Path Cost 19
 eth3: Configured Path Cost 19 - Add type Explicit ref count 1
 eth3: Designated Port Id 0x8005 - Priority 128 -
 eth3: Root 800052540046f549
 eth3: Designated Bridge 8000525400751db5
 eth3: Message Age 1 - Max Age 20
 eth3: Hello Time 2 - Forward Delay 15
 eth3: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change timer 0
 eth3: forward-transitions 3
 eth3: Restricted-role OFF
 eth3: No portfast configured - Current portfast off
 eth3: bpdu-guard default - Current bpdu-guard off
 eth3: bpdu-filter default - Current bpdu-filter off
 eth3: no root guard configured - Current root guard off
 eth3: Configured Link Type point-to-point - Current point-to-point
 eth3: No auto-edge configured - Current port Auto Edge off
 eth4: Port Number 6-Ifindex 6-Port Id 0x8006-Role Rootport-State Forwarding
 eth4: Designated Path Cost 0
 eth4: Configured Path Cost 19 - Add type Explicit ref count 1
 eth4: Designated Port Id 0x8006 - Priority 128 -
 eth4: Root 800052540046f549
 eth4: Designated Bridge 800052540046f549
 eth4: Message Age 0 - Max Age 20
 eth4: Hello Time 2 - Forward Delay 15
 eth4: Forward Timer 0 - Msg Age Timer 3-Hello Timer 0 - topo changen timer 0
 eth4: forward-transitions 6
 eth4: Restricted-role OFF
```

```
eth4: No portfast configured - Current portfast off
eth4: bpdu-guard default - Current bpdu-guard off
eth4: bpdu-filter default - Current bpdu-filter off
eth4: no root guard configured - Current root guard off
eth4: Configured Link Type point-to-point - Current point-to-point
eth4: No auto-edge configured - Current port Auto Edge off
eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - State Blocked
eth5: Designated Path Cost 19
eth5: Configured Path Cost 19 - Add type Explicit ref count 1
eth5: Designated Port Id 0x8004 - Priority 128 -
eth5: Root 800052540046f549
eth5: Designated Bridge 800052540065fd8c
eth5: Message Age 1 - Max Age 20
eth5: Hello Time 2 - Forward Delay 15
eth5: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change timer 0
eth5: forward-transitions 4
eth5: Restricted-role OFF
eth5: No portfast configured - Current portfast off
eth5: bpdu-guard default - Current bpdu-guard off
eth5: bpdu-filter default - Current bpdu-filter off
eth5: no root guard configured - Current root guard off
eth5: Configured Link Type point-to-point - Current point-to-point
eth5: No auto-edge configured - Current port Auto Edge off
```

Bridge 2

```
#show spanning-tree
 2: Bridge up - Spanning Tree Enabled - topology change detected
 2: Root Path Cost 19 - Root Port 7 - Bridge Priority 32768
 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
 2: Root Id 800052540046f549
 2: Bridge Id 8000525400751db5
 2: last topology change Tue Aug 11 02:25:00 2020
 2: 22 topology change(s) - last topology change Tue Aug 11 02:25:00 2020
 2: portfast bpdu-filter disabled
 2: portfast bpdu-guard disabled
 eth2: Port Number 4-Ifindex 4-Port Id 0x8004-Role Designated-State Forwarding
 eth2: Designated Path Cost 19
 eth2: Configured Path Cost 19 - Add type Explicit ref count 1
 eth2: Designated Port Id 0x8004 - Priority 128 -
 eth2: Root 800052540046f549
 eth2: Designated Bridge 8000525400751db5
 eth2: Message Age 1 - Max Age 20
 eth2: Hello Time 2 - Forward Delay 15
 eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
 eth2: forward-transitions 3
 eth2: Restricted-role OFF
 eth2: No portfast configured - Current portfast off
 eth2: bpdu-guard default - Current bpdu-guard off
 eth2: bpdu-filter default - Current bpdu-filter off
 eth2: no root guard configured - Current root guard off
 eth2: Configured Link Type point-to-point - Current point-to-point
 eth2: No auto-edge configured - Current port Auto Edge off
 eth3: Port Number 5-Ifindex 5-Port Id 0x8005-Role Designated-State Forwarding
 eth3: Designated Path Cost 19
 eth3: Configured Path Cost 19 - Add type Explicit ref count 1
 eth3: Designated Port Id 0x8005 - Priority 128 -
```


© 2021 IP Infusion Inc. Proprietary

```
eth3: Root 800052540046f549
eth3: Designated Bridge 8000525400751db5
eth3: Message Age 1 - Max Age 20
eth3: Hello Time 2 - Forward Delay 15
eth3: Forward Timer 0-Msg Age Timer 0-Hello Timer 0-topo change timer 0
eth3: forward-transitions 3
eth3: Restricted-role OFF
eth3: No portfast configured - Current portfast off
eth3: bpdu-guard default - Current bpdu-guard off
eth3: bpdu-filter default - Current bpdu-filter off
eth3: no root guard configured - Current root guard off
eth3: Configured Link Type point-to-point - Current point-to-point
eth3: No auto-edge configured - Current port Auto Edge off
eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 ---State Blocked
eth4: Designated Path Cost 0
eth4: Configured Path Cost 19 - Add type Explicit ref count 1
eth4: Designated Port Id 0x8007 - Priority 128 -
eth4: Root 800052540046f549
eth4: Designated Bridge 800052540046f549
eth4: Message Age 0 - Max Age 20
eth4: Hello Time 2 - Forward Delay 15
eth4: Forward Timer 0-Msg Age Timer 4-Hello Timer 0-topo change timer 0
eth4: forward-transitions 3
eth4: Restricted-role OFF
eth4: No portfast configured - Current portfast off
eth4: bpdu-guard default - Current bpdu-guard off
eth4: bpdu-filter default - Current bpdu-filter off
eth4: no root guard configured - Current root guard off
eth4: Configured Link Type point-to-point - Current point-to-point
eth4: No auto-edge configured - Current port Auto Edge off
eth5: Port Number 7-Ifindex 7-Port Id 0x8007-Role Rootport-State Forwarding
eth5: Designated Path Cost 0
eth5: Configured Path Cost 19 - Add type Explicit ref count 1
eth5: Designated Port Id 0x8004 - Priority 128 -
eth5: Root 800052540046f549
eth5: Designated Bridge 800052540046f549
eth5: Message Age 0 - Max Age 20
eth5: Hello Time 2 - Forward Delay 15
eth5: Forward Timer 0-Msg Age Timer 4-Hello Timer 0-topo change timer 0
eth5: forward-transitions 2
eth5: Restricted-role OFF
eth5: No portfast configured - Current portfast off
eth5: bpdu-guard default - Current bpdu-guard off
eth5: bpdu-filter default - Current bpdu-filter off
eth5: no root guard configured - Current root guard off
eth5: Configured Link Type point-to-point - Current point-to-point
eth5: No auto-edge configured - Current port Auto Edge off
```

Bridge 3

```
#show spanning-tree
 3: Bridge up - Spanning Tree Enabled - topology change detected
 3: Root Path Cost 19 - Root Port 5 - Bridge Priority 32768
 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
 3: Root Id 800052540046f549
 3: Bridge Id 800052540065fd8c
```

```
 3: last topology change Tue Aug 11 02:25:00 2020
 3: 16 topology change(s) - last topology change Tue Aug 11 02:25:00 2020
 3: portfast bpdu-filter disabled
 3: portfast bpdu-guard disabled
 eth2: Port Number 4-Ifindex 4-Port Id 0x8004-Role Designated-State Forwarding
 eth2: Designated Path Cost 19
 eth2: Configured Path Cost 19 - Add type Explicit ref count 1
 eth2: Designated Port Id 0x8004 - Priority 128 -
 eth2: Root 800052540046f549
 eth2: Designated Bridge 800052540065fd8c
 eth2: Message Age 1 - Max Age 20
 eth2: Hello Time 2 - Forward Delay 15
 eth2: Forward Timer 0-Msg Age Timer 0-Hello Timer 1-topo change timer 0
 eth2: forward-transitions 2
 eth2: Restricted-role OFF
 eth2: No portfast configured - Current portfast off
 eth2: bpdu-guard default - Current bpdu-guard off
 eth2: bpdu-filter default - Current bpdu-filter off
 eth2: no root guard configured - Current root guard off
 eth2: Configured Link Type point-to-point - Current point-to-point
 eth2: No auto-edge configured - Current port Auto Edge off
 eth3: Port Number 5-Ifindex 5-Port Id 0x8005-Role Rootport - State Forwarding
 eth3: Designated Path Cost 0
 eth3: Configured Path Cost 19 - Add type Explicit ref count 1
 eth3: Designated Port Id 0x8005 - Priority 128 -
 eth3: Root 800052540046f549
 eth3: Designated Bridge 800052540046f549
 eth3: Message Age 0 - Max Age 20
 eth3: Hello Time 2 - Forward Delay 15
 eth3: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change timer 0
 eth3: forward-transitions 2
 eth3: Restricted-role OFF
 eth3: No portfast configured - Current portfast off
 eth3: bpdu-guard default - Current bpdu-guard off
 eth3: bpdu-filter default - Current bpdu-filter off
 eth3: no root guard configured - Current root guard off
 eth3: Configured Link Type point-to-point - Current point-to-point
 eth3: No auto-edge configured - Current port Auto Edge off
```

Bridge 4

```
#show spanning-tree
 4: Bridge up - Spanning Tree Enabled - topology change detected
 4: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
 4: Root Id 800052540046f549
 4: Bridge Id 800052540046f549
 4: last topology change Tue Aug 11 02:24:58 2020
 4: 6 topology change(s) - last topology change Tue Aug 11 02:24:58 2020
 4: portfast bpdu-filter disabled
 4: portfast bpdu-guard disabled
 eth2: Port Number 4-Ifindex 4-Port Id 0x8004-Role Designated-State Forwarding
 eth2: Designated Path Cost 0
 eth2: Configured Path Cost 19 - Add type Explicit ref count 1
 eth2: Designated Port Id 0x8004 - Priority 128 -
 eth2: Root 800052540046f549
```


© 2021 IP Infusion Inc. Proprietary

```
eth2: Designated Bridge 800052540046f549
eth2: Message Age 0 - Max Age 20
eth2: Hello Time 2 - Forward Delay 15
eth2: Forward Timer 0-Msg Age Timer 0-Hello Timer 0-topo change timer 0
eth2: forward-transitions 1
eth2: Restricted-role OFF
eth2: No portfast configured - Current portfast off
eth2: bpdu-guard default - Current bpdu-guard off
eth2: bpdu-filter default - Current bpdu-filter off
eth2: no root guard configured - Current root guard off
eth2: Configured Link Type point-to-point - Current point-to-point
eth2: No auto-edge configured - Current port Auto Edge off
eth3: Port Number 5-Ifindex 5-Port Id 0x8005-Role Designated-State Forwarding
eth3: Designated Path Cost 0
eth3: Configured Path Cost 19 - Add type Explicit ref count 1
eth3: Designated Port Id 0x8005 - Priority 128 -
eth3: Root 800052540046f549
eth3: Designated Bridge 800052540046f549
eth3: Message Age 0 - Max Age 20
eth3: Hello Time 2 - Forward Delay 15
eth3: Forward Timer 0-Msg Age Timer 0-Hello Timer 0-topo change timer 0
eth3: forward-transitions 1
eth3: Restricted-role OFF
eth3: No portfast configured - Current portfast off
eth3: bpdu-guard default - Current bpdu-guard off
eth3: bpdu-filter default - Current bpdu-filter off
eth3: no root guard configured - Current root guard off
eth3: Configured Link Type point-to-point - Current point-to-point
eth3: No auto-edge configured - Current port Auto Edge off
eth4: Port Number 6-Ifindex 6-Port Id 0x8006-Role Designated-State Forwarding
eth4: Designated Path Cost 0
eth4: Configured Path Cost 19 - Add type Explicit ref count 1
eth4: Designated Port Id 0x8006 - Priority 128 -
eth4: Root 800052540046f549
eth4: Designated Bridge 800052540046f549
eth4: Message Age 0 - Max Age 20
eth4: Hello Time 2 - Forward Delay 15
eth4: Forward Timer 0-Msg Age Timer 0-Hello Timer 0-topo change timer 0
eth4: forward-transitions 1
eth4: Restricted-role OFF
eth4: No portfast configured - Current portfast off
eth4: bpdu-guard default - Current bpdu-guard off
eth4: bpdu-filter default - Current bpdu-filter off
eth4: no root guard configured - Current root guard off
eth4: Configured Link Type point-to-point - Current point-to-point
eth4: No auto-edge configured - Current port Auto Edge off
eth5: Port Number 7-Ifindex 7-Port Id 0x8007-Role Designated-State Forwarding
eth5: Designated Path Cost 0
eth5: Configured Path Cost 19 - Add type Explicit ref count 1
eth5: Designated Port Id 0x8007 - Priority 128 -
eth5: Root 800052540046f549
eth5: Designated Bridge 800052540046f549
eth5: Message Age 0 - Max Age 20
eth5: Hello Time 2 - Forward Delay 15
eth5: Forward Timer 0-Msg Age Timer 0-Hello Timer 0-topo change timer 0
eth5: forward-transitions 1
eth5: Restricted-role OFF
```

```
eth5: No portfast configured - Current portfast off
eth5: bpdu-guard default - Current bpdu-guard off
eth5: bpdu-filter default - Current bpdu-filter off
eth5: no root guard configured - Current root guard off
eth5: Configured Link Type point-to-point - Current point-to-point
eth5: No auto-edge configured - Current port Auto Edge off
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 13 VLAN Configuration

This chapter contains a complete VLAN configuration.

Configuring VLAN Tags

Topology

This shows configuring a VLAN bridge with VLAN tags on forwarding frames. Link between Bridge 1 and Bridge 2 is configured as VLAN 5 and link between Bridge 3 and Bridge 1 is configured as VLAN 10. Link between Bridge 2 and Bridge 3 is configured with VLAN 5 and VLAN 10.

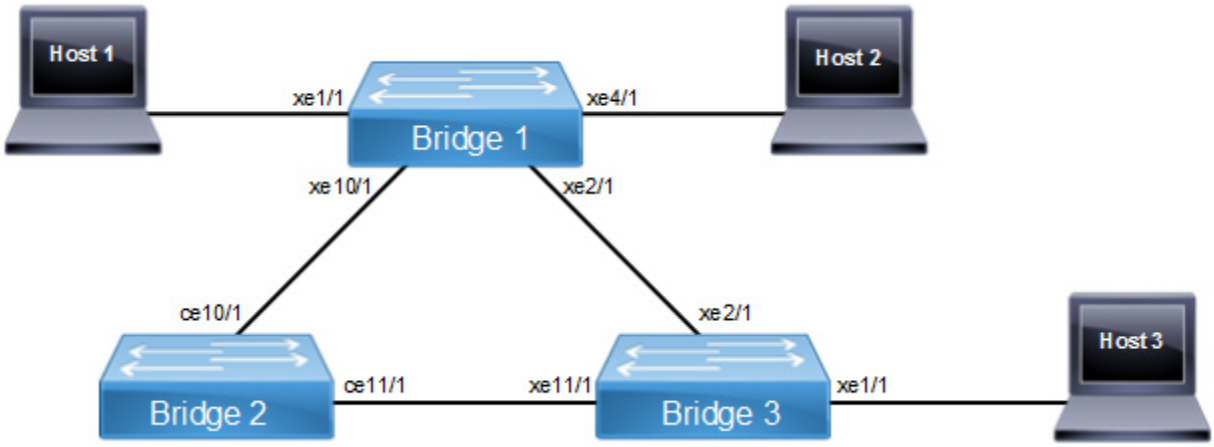


Figure 13-75: VLAN Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

`Bridge1#configure terminal`	Enter configuration mode
`Bridge1(config)#bridge 1 protocol ieee vlan-bridge`	Specify VLAN for bridge 1.
`Bridge1(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge1(config-vlan)#vlan 5 bridge 1 state enable`	Enable VLAN (5) on bridge 1.Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge1(config-vlan)#vlan 10 bridge 1 state enable`	Enable VLAN (10) on bridge 1. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge1(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge1(config)#interface xe1/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.

`Bridge1(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe2/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge1(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe4/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge1(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe10/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge1(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol ieee vlan-bridge`	Specify VLAN for bridge 2.
`Bridge2(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge2(config-vlan)#vlan 5 bridge 2 state enable`	Enable VLAN (5) on bridge 2. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge2(config-vlan)#vlan 10 bridge 2 state enable`	Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge2(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge2(config)#interface ce10/1`	Enter interface mode.
`Bridge2(config-if)#switchport`	
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge2(config-if)#switchport access vlan 5`	Enable VLAN port access by specifying the VLAN ID 5 on this interface.

© 2021 IP Infusion Inc. Proprietary

`Bridge2(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge2(config-if)#switchport`	Configure port as L2.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge2(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge2(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge2(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge2(config)#interface ce11/1`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure port as L2.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge2(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge2(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol ieee vlan-bridge`	Specify VLAN for bridge 3.
`Bridge3(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge3(config-vlan)#vlan 5 bridge 3 state enable`	Enable VLAN (5) on bridge 3. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge3(config-vlan)#vlan 10 bridge 3 state enable`	Enable VLAN (10) on bridge 3. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge3(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge3(config)#interface xe1/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge3(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge3(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge3(config)#interface xe2/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.

`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge3(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge3(config)#interface xe11/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge3(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.

Validation

Bridge 1

```
Bridge1#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 1 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 909
% 1: Root Id 8000001823304db6
% 1: Bridge Id 8000001823305244
% 1: 6 topology changes - last topology change Fri Apr 19 12:32:26 2019
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   xe1/1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 - designated
cost 1
%   xe1/1: Designated Port Id 0x8389 - state Forwarding -Priority 128
%   xe1/1: Designated root 8000001823304db6
%   xe1/1: Designated Bridge 8000001823305244
%   xe1/1: Message Age 1 - Max Age 20
%   xe1/1: Hello Time 2 - Forward Delay 15
%   xe1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   xe1/1: forward-transitions 1
%   xe1/1: No portfast configured - Current  portfast off
%   xe1/1: bpdu-guard  default  - Current bpdu-guard off
%   xe1/1: bpdu-filter default  - Current bpdu-filter off
%   xe1/1: no root guard configured     - Current root guard off
%
%   xe2/1: Port Number 909 - Ifindex 5005 - Port Id 0x838d - path cost 1 - designated
cost 0
%   xe2/1: Designated Port Id 0x838d - state Forwarding -Priority 128
%   xe2/1: Designated root 8000001823304db6
%   xe2/1: Designated Bridge 8000001823304db6
```


© 2021 IP Infusion Inc. Proprietary

```
%   xe2/1: Message Age 0 - Max Age 20
%   xe2/1: Hello Time 2 - Forward Delay 15
%   xe2/1: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 0 - topo change timer 0
%   xe2/1: forward-transitions 2
%   xe2/1: No portfast configured - Current  portfast off
%   xe2/1: bpdu-guard  default  - Current bpdu-guard off
%   xe2/1: bpdu-filter default  - Current bpdu-filter off
%   xe2/1: no root guard configured     - Current root guard off
%
%   xe4/1: Port Number 917 - Ifindex 5013 - Port Id 0x8395 - path cost 4 - designated
cost 1
%   xe4/1: Designated Port Id 0x8395 - state Forwarding -Priority 128
%   xe4/1: Designated root 8000001823304db6
%   xe4/1: Designated Bridge 8000001823305244
%   xe4/1: Message Age 1 - Max Age 20
%   xe4/1: Hello Time 2 - Forward Delay 15
%   xe4/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   xe4/1: forward-transitions 1
%   xe4/1: No portfast configured - Current  portfast off
%   xe4/1: bpdu-guard  default  - Current bpdu-guard off
%   xe4/1: bpdu-filter default  - Current bpdu-filter off
%   xe4/1: no root guard configured     - Current root guard off
%
%   xe10/1: Port Number 941 - Ifindex 5037 - Port Id 0x83ad - path cost 2 - designated
cost 1
%   xe10/1: Designated Port Id 0x83ad - state Forwarding -Priority 128
%   xe10/1: Designated root 8000001823304db6
%   xe10/1: Designated Bridge 8000001823305244
%   xe10/1: Message Age 1 - Max Age 20
%   xe10/1: Hello Time 2 - Forward Delay 15
%   xe10/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   xe10/1: forward-transitions 2
%   xe10/1: No portfast configured - Current  portfast off
%   xe10/1: bpdu-guard  default  - Current bpdu-guard off
%   xe10/1: bpdu-filter default  - Current bpdu-filter off
%   xe10/1: no root guard configured     - Current root guard off
%
B1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe2/1       0018.23cb.fbbc    1     300
 1         1                   xe10/1      cc37.ab97.37d8    1     300
 1         5                   xe1/1       0000.11bc.5dec    1     300
 1         10                  xe4/1       0000.2d50.205c    1     300
Bridge1#


Bridge1#show vlan all bridge 1
Bridge  VLAN ID     Name         State   H/W Status      Member ports
```

```
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Success    xe1/1(u) xe2/1(u) xe4/1(u)
                                                    xe10/1(u)
1       5       VLAN0005         ACTIVE  Success    xe1/1(t) xe10/1(t)
1       10      VLAN0010         ACTIVE  Success    xe2/1(t) xe4/1(t)


Bridge1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe2/1        0018.23cb.fbbc     1     300
 1         1                   xe10/1       cc37.ab97.37d8     1     300
 1         5                   xe1/1        0000.11bc.5dec     1     300
 1         10                  xe4/1        0000.2d50.205c     1     300
Bridge1#
```

Bridge 2

```
Bridge2#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 2         1                   ce10/1       0018.2326.166a     1     300
 2         1                   ce11/1       0018.23cb.fbe0     1     300
 2         1                   ce11/1       cc37.ab97.37d8     1     300
 2         5                   ce10/1       0000.11bc.5dec     1     300


Bridge2#show vlan all bridge 2
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
2       1       default          ACTIVE  Success    ce10/1(u) ce11/1(u)
2       5       VLAN0005         ACTIVE  Success    ce10/1(t) ce11/1(t)
2       10      VLAN0010         ACTIVE  Success    ce10/1(t) ce11/1(t)


Bridge2#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 2         1                   ce10/1       0018.2326.166a     1     300
 2         1                   ce11/1       0018.23cb.fbe0     1     300
 2         1                   ce11/1       cc37.ab97.37d8     1     300
 2         5                   ce10/1       0000.11bc.5dec     1     300
```


© 2021 IP Infusion Inc. Proprietary

Bridge 3

```
Bridge3# show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 3         1                   xe2/1        cc37.ab97.37d8     1     300
 3         5                   xe11/1       0000.11bc.5dec     1     300
 3         10                  xe2/1        0000.2d50.205c     1     300
Bridge3#sh vlan all bridge 3
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
3       1       default           ACTIVE  Success    xe1/1(u) xe2/1(u) xe11/1(u)
3       5       VLAN0005          ACTIVE  Success    xe1/1(t) xe11/1(t)
3       10      VLAN0010          ACTIVE  Success    xe1/1(t) xe2/1(t)


Bridge3#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 3         1                   xe2/1        cc37.ab97.37d8     1     300
 3         5                   xe11/1       0000.11bc.5dec     1     300
 3         10                  xe2/1        0000.2d50.205c     1     300
Bridge3#
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 14 VLAN Cross-Connect (XC)

Overview

VLAN cross connect creates a L2 bridge between two given endpoints on the same device. Once configured, every packets arriving at one of the endpoints with specific VLAN tag will be sent to another endpoint directly. In current implementation it matches VLAN tag as per configuration in device. If device is configured to match single tag then only outer most tagged will be matched whether packet is double tagged. If device is configured to match double tag then outer tag as well as inner tag will match If the packet is double tagge.

Note:

1. End point or source point could be a physical (Native Ethernet) port or logical port (po, vlan etc).
2. Same Vlan ID cannot be used in 2 cross connects.
3. Different type of L2, L3 and subscriber services are supported over cross.
4. The XC implementation will forward all packets and MAC address learning is disabled.

Topology

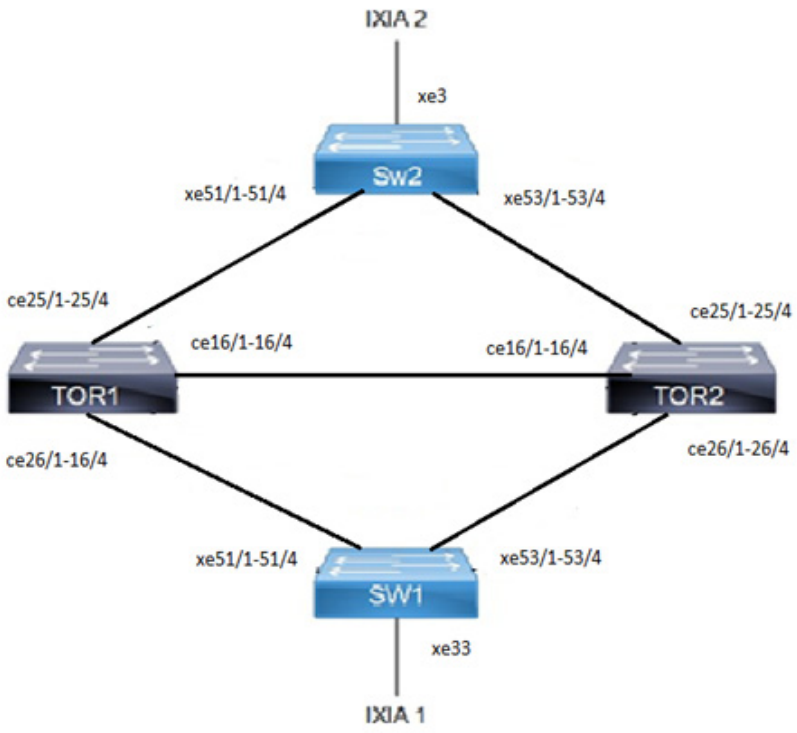


Figure 14-76: Cross-connect topology

Configuration - Single-tagged VLAN

TOR1

`#configure terminal`	Enter Configure mode.
`(config)#interface ce25/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#exit`	Exit interface mode
`(config)#interface ce16/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#exit`	Exit interface mode
`(config)#cross-connect VC1`	Create cross-connect (XC)
`(config-XC)# vlan ep1 ce25/1 ep2 ce16/1`	Add Endpoints to XC
`(config-VXC)# outer-vlan 100`	Outer-vlanId associated with the XC
`(config-VXC)#end`	Return to privilege mode

© 2021 IP Infusion Inc. Proprietary

TOR2

`#configure terminal`	Enter Configure mode.
`(config)#interface ce16/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#exit`	Exit interface mode
`(config)#interface ce26/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#exit`	Exit interface mode
`(config)#cross-connect VC1`	Create cross-connect (XC)
`(config-XC)# vlan ep1 ce16/1 ep2 ce26/1`	Add Endpoints to XC
`(config-VXC)# outer-vlan 100`	Outer-vlanId associated with the XC
`(config-VXC)#end`	Return to privilege mode

SW2

`#configure terminal`	Enter Configure mode.
`(config)#bridge 1 protocol mstp`	Add a bridge (1) to the multiple spanning tree table
`(config)#vlan database`	Enter the VLAN configuration mode
`(config-vlan)#vlan 100 bridge 1 state enable`	Enable the state of VLAN 100 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 100 on bridge 1
`(config-vlan)#exit`	Exit the VLAN configuration mode
`(config)#interface xe51/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`(config-if)#switchport mode trunk`	set the switching characteristics of the Layer 2 interface
`(config-if)#switchport trunk allowed vlan all`	Allow all VLANs to transmit and receive through the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe3`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`(config-if)#switchport mode trunk`	set the switching characteristics of the Layer 2 interface
`(config-if)#switchport trunk allowed vlan all`	Allow all VLANs to transmit and receive through the interface
`(config-if)#exit`	Exit interface mode

SW1

`#configure terminal`	Enter Configure mode.
`(config)#bridge 1 protocol mstp`	Add a bridge (1) to the multiple spanning tree table
`(config)#vlan database`	Enter the VLAN configuration mode
`(config-vlan)#vlan 100 bridge 1 state enable`	Enable the state of VLAN 100 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 100 on bridge 1
`(config-vlan)#exit`	Exit the VLAN configuration mode
`(config)#interface xe53/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`(config-if)#switchport mode trunk`	set the switching characteristics of the Layer 2 interface
`(config-if)#switchport trunk allowed vlan all`	Allow all VLANs to transmit and receive through the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe33`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`(config-if)#switchport mode trunk`	set the switching characteristics of the Layer 2 interface

© 2021 IP Infusion Inc. Proprietary

(config-if)#switchport trunk allowed vlan all	Allow all VLANs to transmit and receive through the interface
(config-if)#exit	Exit interface mode

Validation

TOR1

```
#show cross-connect
Cross-connect name : VC1
EP1:ce25/1              EP2:ce16/1         Admin Status:UP            OperStatus:UP
+=============================================================================================
+
| EP  | OVID     | IVID     | Rx packets  | Rx bytes   | Tx packets  | Tx bytes    |
+=============================================================================================
+
| EP1 |100       |     -    |6572258      |9858387000  |0            |0            |
| EP2 |100       |     -    |0            |0           |6572224      |9858336000   |
+=============================================================================================
+
Cross-connect summary Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

TOR2

```
#show cross-connect
Cross-connect name : VC1
EP1:ce16/1              EP2:ce26/1         Admin Status:UP            OperStatus:UP
+=============================================================================================
+
| EP  | OVID     | IVID     | Rx packets  | Rx bytes   | Tx packets  | Tx bytes    |
+=============================================================================================
+
| EP1 |100       |     -    |616588       |924882000   |0            |0            |
| EP2 |100       |     -    |0            |0           |618615       |927922500    |
+=============================================================================================
+
Cross-connect summary Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

Double-tagged VLAN

TOR1

`#configure terminal`	Enter Configure mode.
`(config)#interface ce25/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#exit`	Exit interface mode
`(config)#interface ce16/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#exit`	Exit interface mode
`(config)#cross-connect VC2`	Create cross-connect (XC)
`(config-XC)# vlan ep1 ce25/1 ep2 ce16/1`	Add Endpoints to XC
`(config-VXC)# outer-vlan 200-300 inner-vlan 20-30`	Outer-vlanId and Inner-vlanId with range associated with the XC
`(config-VXC)#end`	Return to privilege mode

TOR2

`#configure terminal`	Enter Configure mode.
`(config)#interface ce16/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#exit`	Exit interface mode
`(config)#interface ce26/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#exit`	Exit interface mode
`(config)#cross-connect VC2`	Create cross-connect (XC)
`(config-XC)# vlan ep1 ce16/1 ep2 ce26/1`	Add Endpoints to XC
`(config-VXC)# outer-vlan 200-300 inner-vlan 20-30`	Outer-vlanId and Inner-vlanId with range associated with the XC
`(config-VXC)#end`	Return to privilege mode

© 2021 IP Infusion Inc. Proprietary

SW2

`#configure terminal`	Enter Configure mode.
`(config)#bridge 1 protocol mstp`	Add a bridge (1) to the multiple spanning tree table
`(config)#vlan database`	Enter the VLAN configuration mode
`(config-vlan)#vlan 200-300 bridge 1 state enable`	Enable the state of VLANs 200-300 on bridge 1. Specifying an enable state allows forwarding of frames over VLANs 200-300 on bridge 1
`(config-vlan)#exit`	Exit the VLAN configuration mode
`(config)#interface xe51/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`(config-if)#switchport mode trunk`	set the switching characteristics of the Layer 2 interface
`(config-if)#switchport trunk allowed vlan all`	Allow all VLANs to transmit and receive through the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe3`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`(config-if)#switchport mode trunk`	set the switching characteristics of the Layer 2 interface
`(config-if)#switchport trunk allowed vlan all`	Allow all VLANs to transmit and receive through the interface
`(config-if)#exit`	Exit interface mode

© 2021 IP Infusion Inc. Proprietary

SW1

`#configure terminal`	Enter Configure mode.
`(config)#bridge 1 protocol mstp`	Add a bridge (1) to the multiple spanning tree table
`(config)#vlan database`	Enter the VLAN configuration mode
`(config-vlan)#vlan 200-300 bridge 1 state enable`	Enable the state of VLANs 200-300 on bridge 1. Specifying an enable state allows forwarding of frames over VLANs 200-300 on bridge 1
`(config-vlan)#exit`	Exit the VLAN configuration mode
`(config)#interface xe53/1`	Enter Interface mode
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`(config-if)#switchport mode trunk`	Set the switching characteristics of the Layer 2 interface
`(config-if)#switchport trunk allowed vlan all`	Allow all VLANs to transmit and receive through the interface
`(config-if)#exit`	Exit nterface mode
`(config)#interface xe33`	Enter Interface mode
`(config-if)#no shutdown`	Bring interface up
`(config-if)#switchport`	Configure interface as a layer 2 port
`(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`(config-if)#switchport mode trunk`	Set the switching characteristics of the Layer 2 interface
`(config-if)#switchport trunk allowed vlan all`	Allow all VLANs to transmit and receive through the interface
`(config-if)#exit`	Exit interface mode

Validation

TOR1

```
#show cross-connect
Cross-connect name : VC2
EP1:ce25/1              EP2:ce16/1         Admin Status:UP            OperStatus:UP
+=============================================================================================
+
| EP  | OVID     | IVID     | Rx packets  | Rx bytes    | Tx packets  | Tx bytes     |
+=============================================================================================
+
| EP1 |200-300   |20-30     |442089       |663133500    |0            |0             |
| EP2 |200-300   |20-30     |0            |0            |444123       |666184500     |
+=============================================================================================
+
Cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```


© 2021 IP Infusion Inc. Proprietary

TOR2

```
#show cross-connect
Cross-connect name : VC2
EP1:ce16/1              EP2:ce26/1         Admin Status:UP            OperStatus:UP
+=============================================================================================
+
| EP  | OVID     | IVID     | Rx packets  | Rx bytes   | Tx packets  | Tx bytes    |
+=============================================================================================
+
| EP1 |200-300   |20-30     |267607       |401410500   |0            |0            |
| EP2 |200-300   |20-30     |0            |0           |269640       |404460000    |
+=============================================================================================
+
Cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 15 Unidirectional Link Detection Configuration

This chapter shows a complete configuration to enable UDLD in a simple network topology.

The purpose of Unidirectional Link Detection protocol (UDLD) is to monitor the physical links and detect when a unidirectional link exists. Upon detection user can either block the port or notify the link status based on the network administrator's configuration.

UDLD works in two different modes:

- Normal mode
- Aggressive mode

Topology

Figure 15-77 shows the topology of the UDLD configuration.

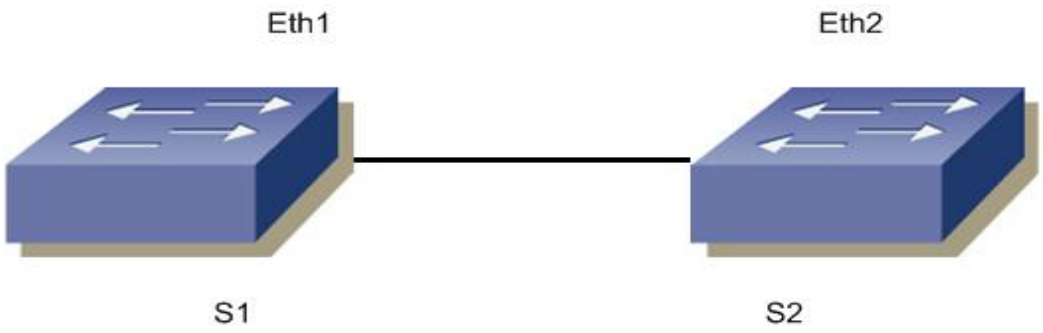


Figure 15-77: UDLD Configuration

S1

`#configure terminal`	Enter configure mode
`(config)#udld enable`	Enable UDLD globally
`(config)#udld message-time 7`	Configure message time for UDLD packets
`(config)#interface eth1`	Enter interface mode
`(config-if)#switchport`	Configure the interface as switch port
`(config-if)#udld state enable`	Enable UDLD on the interface
`(config-if)#udld mode normal`	Configure udld mode as normal or aggressive
`(config-if)#commit`	Commit config.
`(config-if)#exit`	Exit from the interface mode

S2

`#configure terminal`	Enter configure mode.
`(config)#udld enable`	Enable UDLD globally.
`(config)#udld message-time 7`	Configure message time for UDLD packets
`(config)#interface eth2`	Enter interface mode
`(config-if)#switchport`	Configure the interface as switch port.
`(config-if)#udld state enable`	Enable UDLD on the interface.
`(config-if)#udld mode normal`	Configure udld mode as normal or aggressive
`(config-if)#commit`	Commit config.
`(config-if)#exit`	Exit from the interface mode

Validation

```
#show udld
UDLD: Enable
Message Interval(sec) : 7

Port   UDLD Status      Mode      Link-Status
-----------------------------------------------
Eth1   Enable           Normal    Bi-directional
Eth2   Disable          Normal    Unknown
Eth3   Disable          Normal    Unknown
Eth4   Disable          Normal    Unknown
Eth5   Disable          Normal    Unknown
Eth6   Disable          Normal    Unknown
```

Once the links is made Uni-directional, the output of the command Show udld is as follows:

```
#show udld
UDLD: Enable
Message Interval(sec) : 7

Port   UDLD Status      Mode       Link-Status
-----------------------------------------------
Eth1   Enable           Normal     Unidirectional
Eth2   Disable          Normal     Unknown
Eth3   Disable          Normal     Unknown
Eth4   Disable          Normal     Unknown
Eth5   Disable          Normal     Unknown
Eth6   Disable          Normal     Unknown
```


© 2021 IP Infusion Inc. Proprietary

```
#sh running-config
udld Enable
udld message-time 7

#sh running-config in eth1
!
interface eth1
 switchport
 udld state Enable
!

#sh udld interface eth1
UDLD Status           : Enable
UDLD Mode             : Normal
Link-State            : Unknown
```

For aggressive mode, udld output is as follows:

```
#show udld
    UDLD  : Enable
    Message Interval(sec) : 7


Port   UDLD Status     Mode        Link-Status
-----------------------------------------------
eth1   Enable          Aggressive  Bi-Directional


#sh running config
udld Enable
udld message-time 7

#sh running-config in eth1
  interface eth1
switchport
udld mode Aggressive
udld state Enable
```

© 2021 IP Infusion Inc. Proprietary

Layer 2 Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Fundamental Layer 2 Commands*
- Chapter 2, *Bridge Commands*
- Chapter 3, *Spanning Tree Protocol Commands*
- Chapter 4, *RPVST+ Commands*
- Chapter 5, *Link Aggregation Commands*
- Chapter 6, *Multi-Chassis Link Aggregation Commands*
- Chapter 7, *VLAN and Private VLAN Commands*
- Chapter 8, *802.1x Commands*
- Chapter 9, *Link Layer Discovery Protocol Commands*
- Chapter 10, *Port Security Commands*
- Chapter 11, *VLAN Cross-Connect Commands*
- Chapter 12, *Unidirectional Link Detection Commands*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Fundamental Layer 2 Commands

This chapter describes fundamental Layer 2 commands.

- errdisable cause
- errdisable link-flap-setting
- errdisable timeout
- show errdisable details
- show interface errdisable status
- show running-config switch
- show tcp
- watch static-mac-movement

errdisable cause

Use this command to globally shut down a port when certain errors happen:

- BPDU guard puts an interface configured for Spanning Tree Protocol (STP) Port Fast into the ErrDisable state upon receipt of a STP BPDU to avoid a potential bridging loop.
- If one side of a link-access group (LAG) is configured as a static LAG and the other side as a dynamic LAG, the ports on the side receiving LACP BPDUs go into the ErrDisable state

Note: When link-flap ErrDisable is enabled globally, then all interfaces are enabled. Link-flap ErrDisable can be enabled globally, but disabled for a specific interface with the `no link-flap errdisable` command.

Note: Stp-Bpdu-Guard is enabled by default on the global level configuration.

Use `no` form of this command to not shut down a port when certain errors happen.

Command Syntax

```
errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap}
no errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap}
```

Parameters

`stp-bpdu-guard`	ErrDisable on stp-bpdu-guard
`lag-mismatch`	ErrDisable on lag-mismatch
`link-flap`	ErrDisable on link-flap

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable cause lag-mismatch
```


© 2021 IP Infusion Inc. Proprietary

errdisable link-flap-setting

Use this command to configure the link-flap errdisable feature:

- An interface should change state as up-down to complete one cycle of a link flap.
- The LED does not glow when an interface is in the errdisable state.
- Errdisable is supported only on physical interfaces.
- A LAG interface does not go into the errdisable state when all of its member ports are in the errdisable state
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. If the accumulated link flap count reaches the maximum flap count for a particular sliding window, a link flap error disable fault is triggered.

Note: Any previous flapping accumulated is flushed when you execute this command.

Command Syntax

```
errdisable link-flap-setting max-flaps <1-100> time <1-1800>
```

Parameters

<1-100>	Maximum flap count
<1-1800>	Sliding window size in seconds

Default

Five flaps in ten seconds:

Maximum flap count: 5

Sliding window size: 10 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable link-flap-setting max-flaps 5 time 20
```

errdisable timeout

Use this command to set the ErrDisable auto-recovery timeout interval.

Command Syntax

```
errdisable timeout interval <10-1000000>
```

Parameters

<10-1000000>	Timeout interval in seconds

Default

By default, zero: timer is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable timeout interval 1000
```


© 2021 IP Infusion Inc. Proprietary

show errdisable details

Use this command to display ErrDisable settings.

Command Syntax

```
show errdisable details
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show errdisable details
```

show interface errdisable status

Use this command to display ErrDisable conditions for an interface.

Command Syntax

```
show interface errdisable status
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface errdisable status
ge1 lag-mismatch-errdisable
ge2 stp-bpdu-guard-errdisable
```


© 2021 IP Infusion Inc. Proprietary

show running-config switch

Use this command to display the running system switch configuration.

Command Syntax

```
show running-config switch bridge
show running-config switch dot1x
show running-config switch gmrp
show running-config switch gvrp
show running-config switch lacp
show running-config switch lmi
show running-config switch mstp
show running-config switch radius-server
show running-config switch rpsvt+
show running-config switch rstp
show running-config switch ptp
show running-config switch stp
show running-config switch synce
show running-config switch vlan
```

Parameters

`bridge`	Display Bridge group information.
`dot1x`	Display 802.1x port-based authentication information.
`gmrp`	Display GARP Multicast Registration Protocol (GMRP) information.
`gvrp`	Display GARP VLAN Registration Protocol (GVRP) information.
`lacp`	Display Link Aggregation Control Protocol (LACP) information.
`lmi`	Display Ethernet Local Management Interface Protocol (LMI) information.
`mstp`	Display Multiple Spanning Tree Protocol (MSTP) information.
`radius-server`	Display RADIUS server information.
`rpvst+`	Display Rapid Per-VLAN Spanning Tree (rpvst+) information.
`rstp`	Display Rapid Spanning Tree Protocol (RSTP) information.
`ptp`	Display Precision time Protocol (PTP)
`stp`	Display Spanning Tree Protocol (STP) information.
`synce`	Display synce information.
`vlan`	Display values associated with a single VLAN.

Default

None

© 2021 IP Infusion Inc. Proprietary

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#show running-config switch stp
!
bridge 6 ageing-time 45
bridge 6 priority 4096
bridge 6 max-age 7
```


© 2021 IP Infusion Inc. Proprietary

show tcp

Use this command to display the Transmission Control Protocol (TCP) connections details.

Command Syntax

```
show tcp
```

Parameters

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show tcp
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 0.0.0.0:22            0.0.0.0:*              LISTEN
tcp        0      0 127.0.0.1:25          0.0.0.0:*              LISTEN
tcp        0      1 10.12.44.1:57740      127.0.0.1:705          CLOSE_WAIT
tcp       52      0 10.12.44.21:22        10.12.7.89:705         ESTABLISHED
tcp       85      0 10.12.44.21:57742     10.12.44.21:57738      ESTABLISHED
```

Table 1-91: Show tcp output

Entry	Description
Proto	Protocol – TCP
Recv-Q	Number of TCP packets in the Receive Queue.
Send-Q	Number of TCP packets in the Send-Q.
Local Address and port number	Local IP address and the port number.

Table 1-91: Show tcp output (Continued)

Entry	Description
Foreign Address and port number	Foreign (received) IP address and the port number.
State	Current state of TCP connections: ESTABLISHED SYN_SENT SYN_RECV FIN_WAIT1 FIN_WAIT2 TIME_WAIT CLOSE CLOSE_WAIT LAST_ACK LISTEN CLOSING UNKNOWN

© 2021 IP Infusion Inc. Proprietary

watch static-mac-movement

Use this command to watch if any MAC movement is detected over static MAC entries for a time period. Notification will be displaying if static MAC movement happens before the timer expires.

The counters can be validated with `show interface cpu counters queue-stats` for the L2 movement queue (`Tx pkts` and `Dropped pkts` columns).

Without enabling `watch static-mac-movement`, the statistics are reflected in the `Rx EGR Port Unavail` of show interface counters queue-drop-stats.

For VXLAN, `watch static-mac-movement` applies to all the MAC entries learned from the remote peer (remote dynamic or static remote), as these learned MACs are installed as static MAC entries in the hardware.

Command Syntax

```
watch static-mac-movement (<1-300>|)
```

Parameters

`<1-300>`	Timer value in seconds.

Default

By default, the timer is 10 seconds

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#watch static-mac-movement
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Bridge Commands

This chapter provides a description, syntax, and examples of the bridge commands. It includes the following commands:

- bridge acquire
- bridge address
- bridge ageing
- bridge forward-time
- bridge hello-time
- bridge mac-priority-override
- bridge max-age
- bridge max-hops
- bridge priority
- bridge shutdown
- bridge transmit-holdcount
- bridge-group
- bridge-group path-cost
- bridge-group priority
- clear allowed-ethertype
- clear mac address-table
- mac ageing display
- show allowed-ethertype
- show bridge
- show interface switchport
- show mac address-table count bridge
- show mac address-table bridge
- show mac-address-table bridge 1 learning
- switchport
- switchport allowed ethertype

© 2021 IP Infusion Inc. Proprietary

bridge acquire

Use this command to enable a bridge to learn station location information for an instance. This helps in making forwarding decisions.

Use the `no` parameter with this command to disable learning.

Command Syntax

```
bridge <1-32> acquire
no bridge <1-32> acquire
```

Parameter

`<1-32>`	Specify the bridge group ID.

Default

By default, learning is enabled for all instances.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 acquire
(config)#no bridge 3 acquire
```


© 2021 IP Infusion Inc. Proprietary

bridge address

Use this command to add a static forwarding table entry for the bridge.

Use the no parameter with this command to remove the entry for the bridge

Command Syntax

```
bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME
bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME vlan <2-4094>
bridge <1-32> address XXXX.XXXX.XXXX  (forward|discard) IFNAME vlan <2-4094> svlan
  <2-4094>
no bridge <1-32> address XXXX.XXXX.XXXX
no bridge <1-32> address XXXX.XXXX.XXXX vlan <2-4094>
no bridge <1-32> address XXXX.XXXX.XXXX vlan <2-4094> svlan <2-4094>
```

Parameters

`<1-32>`	Bridge identifier
`XXXX.XXXX.XXXX`	Media Access Control (MAC) address in HHHH.HHHH.HHHH format.
`forward`	Forward matching frames.
`discard`	Discard matching frames.
`IFNAME`	Interface on which the frame comes out.
`vlan`	Identity of the VLAN in the range of <2-4094>.
`svlan`	Identity of the SVLAN in the range of <2-4094>.

Defaul

By default, bridge address is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 1 address 0000.000a.0021 forward eth0
(config)#no bridge 1 address 0000.000a.0021
(config)#bridge 1 address 0011.2222.3333 forward xe5 vlan 23
(config)#no bridge 1 address 0011.2222.3333 vlan 23
(config)#bridge 1 address 0011.2222.3333 forward xe5 vlan 11 svlan 21
(config)#no bridge 1 address 0011.2222.3333 vlan 11 svlan 21
(config)#bridge 1 address 0011.2222.3334 discard xe6 vlan 12 svlan 22
(config)#no bridge 1 address 0011.2222.3334 vlan 12 svlan 22
```

bridge ageing

Use this command to specify the aging time for a learned MAC address. A learned MAC address persists until this specified time.

Note: On XGS devices, it takes up to two ageing cycles to remove the mac entry from hardware, hence the timeout will be anywhere between mac-ageing-time to two times the mac-ageing-time. For example, if the MAC ageing time is set to 100 seconds, MAC ageing can happen anywhere between 100 to 199 seconds.

Note: The bridge aging time affects the ARP entries which are dependent upon the MAC addresses in hardware. If a MAC address ages out, it causes the corresponding ARP entry to refresh.

Use the `no` form of this command to set the MAC address aging time to its default (300).

Command Syntax

```
bridge <1-32> ageing-time <10-572>
bridge <1-32> ageing disable
no bridge <1-32> ageing-time
no bridge <1-32> ageing-time (0|<10-1000000>))
```

Note: The `no bridge <1-32> ageing-time (0|<10-1000000>))` CLI is enabled when HAVE_DUNE is not enabled.

Parameters

`<1-32>`	Bridge group ID.
`<10-572>`	Aging time in seconds.
`disable`	Turn off MAC address aging completely.

Default

By default, the aging time is 300 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 ageing-time 1000
(config)#no bridge 3 ageing-time
```


© 2021 IP Infusion Inc. Proprietary

bridge forward-time

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances.

Use the `no` parameter with this command to restore the default value of 15 seconds.

Command Syntax

```
bridge <1-32> forward-time <4-30>
no bridge <1-32> forward-time
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<4-30>`	Specify the forwarding time delay in seconds.

Note: Care should be exercised if the value is to be made below 7 seconds.

Default

By default, value is 15 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 forward-time 6
(config)#no bridge 3 forward-time
```

bridge hello-time

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). A very low value of this parameter leads to excessive traffic on the network, while a higher value delays the detection of topology change.This value is used by all instances.

Configure the bridge instance name before using this command. The allowable range of values is 1-10 seconds. However, make sure that the value of hello time is always greater than the value of hold time (2 seconds by default).

Use the `no` parameter to restore the default value of the hello time.

Note: A Bridge shall enforce the following relationships for Hello-time, Max-age and Forward-delay.

- 2 × (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
- Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds)

Command Syntax

```
bridge <1-32> hello-time <1-10>
no bridge <1-32> hello-time
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<1-10>`	Specify the hello BPDU interval in seconds.

Default

By default, value is 2 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 3 hello-time 3

(config)#no bridge 3 hello-time
```


© 2021 IP Infusion Inc. Proprietary

bridge mac-priority-override

Use this command to set a MAC priority override.

Use the `no` parameter with this command to unset a MAC priority override.

Command Syntax

```
bridge <1-32> mac-priority-override mac-address MAC interface IFNAME vlan VLANID
  (static|static-priority-override|static-mgmt|static-mgmt-priority-overide)
  priority <0-7>
no bridge <1-32> mac-priority-override mac-address MAC interface IFNAME vlan VLANID
```

Parameters

`<1-32>`	Specify the bridge group ID.
`mac-address`	Enter a MAC address in HHHH.HHHH.HHHH format.
`interface`	Interface information
`vlan`	Add the values associated with a single VLAN
`static`	The MAC is a static entry
`static-mgmt`	The MAC is a Static Management
`static-mgmt-priority-overide`	The MAC is a Static Management with priority override
`static-priority-override`	The MAC is a static with priority override
`priority`	priority <0-7> priority value

Default

No default address is specified

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 mac-priority-override mac-address 1111.1111.1111 interface
eth1 vlan 2 static priority 2

(config)#no bridge 1 mac-priority-override mac-address 1111.1111.1111
interface eth1 vlan 2
```

bridge max-age

Use this command to set the maximum age for a bridge. This value is used by all instances.

Maximum age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of maximum age should be greater than twice the value of hello time plus 1, but less than twice the value of forward delay minus 1. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the maximum age.

Use the `no` parameter with this command to restore the default value of the maximum age.

Note: A Bridge shall enforce the following relationships for Hello-time, Max-age and Forward-delay.

- 2 × (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
- Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds)

Command Syntax

```
bridge <1-32> max-age <6-40>
no bridge <1-32> max-age
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<6-40>`	Specify the maximum time, in seconds, to listen for the root bridge <6-40>.

Default

By default, bridge maximum age is 20 seconds

Command Mode

Configure Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 max-age 12

(config)#no bridge 2 max-age
```


© 2021 IP Infusion Inc. Proprietary

bridge max-hops

Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST. Specifying the maximum hops for a BPDU prevents the messages from looping indefinitely in the network. When a bridge receives an MST BPDU that has exceeded the allowed maximum hops, it discards the BPDU.

Use the `no` parameter with this command to restore the default value.

Command Syntax

```
bridge <1-32> max-hops <1-40>
no bridge <1-32> max-hops
```

Parameters

`<1-32>`	Specify the bridge-group ID.
`<1-40>`	Specify the maximum hops for which the BPDU will be valid <1-40>.

Default

By default, maximum hops in an MST region are 20

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 3 max-hops 25

#configure terminal
(config)#no bridge 3 max-hops
```

bridge priority

Use this command to set the bridge priority for the common instance. Using a lower priority indicates a greater likelihood of the bridge becoming root. The priority values can be set only in increments of 4096.

Use the `no` form of the command to reset it to the default value.

Command Syntax

```
bridge (<1-32> | ) priority <0-61440>
no bridge (<1-32> | )priority
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<0-61440>`	Specify the bridge priority in the range of <0-61440>.

Default

By default, priority is 32768 (or hex 0x8000).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 priority 4096

(config)#no bridge 2 priority
```


© 2021 IP Infusion Inc. Proprietary

bridge shutdown

Use this command to disable a bridge.

Use the `no` parameter to reset the bridge.

Command Syntax

```
bridge shutdown <1-32>
bridge shutdown <1-32> ((bridge-blocked|bridge-forward)|)
no bridge shutdown <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.
`bridge-forward`	Put all ports of the bridge into forwarding state
`bridge-blocked`	Put all ports of the bridge into blocked state

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge shutdown 4
(config)#no bridge shutdown 4
```

bridge transmit-holdcount

Use this command to set the maximum number of transmissions of BPDUs by the transmit state machine.

Use the `no` parameter with this command to restore the default transmit hold-count value.

Command Syntax

```
bridge <1-32> transmit-holdcount <1-10>
no bridge <1-32> transmit-holdcount
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<1-10>`	Transmit hold-count value.

Default

By default, transmit hold-count is 6

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 transmit-holdcount 5

(config)#no bridge 1 transmit-holdcount
```


© 2021 IP Infusion Inc. Proprietary

bridge-group

Use this command to bind an interface with a bridge specified by the parameter.

Use the `no` parameter with this command to disable this command.

Command Syntax

```
bridge-group (<1-32>)
no bridge-group (<1-32>)
```

Parameters

`<1-32>`	Specify the bridge group ID.

Default

By default, bridge-group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 2

(config)#interface eth1
(config-if)#no bridge-group 2
```

bridge-group path-cost

Use this command to set the cost of a path associated with a bridge group. The lower the path cost, the greater the likelihood of the bridge becoming root.

Use the `no` parameter with this command to restore the default priority value.

Command Syntax

```
bridge-group <1-32> path-cost <1-200000000>
no bridge-group <1-32> path-cost
```

Parameters

`<1-32>`	Specify the bridge group ID.
`path-cost`	Specify the path-cost of a port.
`<1-200000000>`	Specify the cost to be assigned to the group.

Default

By default, bridge-group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 3 path-cost 123

(config-if)#no bridge-group 3 path-cost
```


© 2021 IP Infusion Inc. Proprietary

bridge-group priority

Use this command to set the port priority for a bridge. A lower priority indicates a greater likelihood of the bridge becoming root.

Command Syntax

```
bridge-group <1-32> priority <0-240>
no bridge-group <1-32> priority
```

Parameters

<1-32>	Specify the bridge group ID.
<0-240>	Specify the port priority range (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 4 priority 96

(config)#interface eth1
(config-if)#no bridge-group 4 priority
```

clear allowed-ethertype

Use this command to clear statistics for each ethertype per interfaces.

```
clear allowed-ethertype statistics (IFNAME|)
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear allowed-ethertype statistics xe54/1

#show allowed-ethertype statistics xe54/1
Interface xe54/1
arp: 0 Packets, 0 Bytes
ipv4: 0 Packets, 0 Bytes
ipv6: 0 Packets, 0 Bytes
dropped: 0 Packets, 0 Bytes
```


© 2021 IP Infusion Inc. Proprietary

clear mac address-table

Use this command to clear the filtering database for the bridge. This command can be issued to do the following:

- clear the filtering database
- clear all filtering database entries configured through CLI (static)
- clear all multicast filtering database entries
- clear all multicast filtering database entries for a given VLAN or interface
- clear all static or multicast database entries based on a mac address

Command Syntax

```
clear mac address-table (dynamic|static|multicast) bridge <1-32>
clear mac address-table (dynamic|static|multicast) (address MACADDR | interface
  IFNAME | vlan VID ) bridge <1-32>
clear mac address-table (dynamic|static|multicast) (address MACADDR | interface
  IFNAME | vlan VID ) (instance INST) bridge <1-32>
```

Parameters

`dynamic`	Clears all dynamic entries.
`multicast`	Clears all multicast filtering database entries.
`static`	Clears all entries configured through management.
`address`	Clear the specified MAC Address.
`MACADDR`	When filtering database, entries are cleared based on the MAC address.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`cvlan`	Clears all MAC address for the specified CVLAN. Value range is 1-4094.
`svlan`	Clears all mac address for the specified SVLAN. Value range is 1-4094.
`interface`	Clears all MAC address for the specified interface.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`instance`	Clears MSTP instance ID. Value range is <1-63>.
`vlan`	Clears all MAC address for the specified VLAN. Value range is 1-4094.
`bridge`	Clears the bridge group ID. Value range is 1-32.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to clear all filtering database entries configured through CLI:

```
#clear mac address-table static bridge 1
```

This example shows how to clear multicast filtering database entries:

```
#clear mac address-table multicast bridge 1
```

This example shows how to clear all filtering database entries for a given interface:

```
#clear mac address-table static interface eth0 bridge 1
```

This example shows how to clear multicast filtering database entries for a given VLAN.

```
#clear mac address-table multicast vlan 2 bridge 1
```

This example shows how to clear static filtering database entries for a given MAC address:

```
#clear mac address-table static address 0202.0202.0202 bridge 1
```

This example shows how to clear all filtering database entries learned through bridge operation for a given MAC address.

```
#clear mac address-table dynamic address 0202.0202.0202 bridge 1
```

 © 2021 IP Infusion Inc. Proprietary

mac ageing display

Use this command to enable the display of remaining age-time value for dynamically learnt mac address.

Note: When the mac ageing display is enabled the following points are applicable .

a. The mac ageing display should be enabled in non-scaled case (i.e less than 25% of table size) .

b. High cpu usage will occurs if mac-ageing-display is enabled in scaled case.

c. When enabled ,the appropriate ageing time for each entry will only be displayed after the first iteration of the ageing thread is complete which starts after 10 seconds of the cli commit .

d. For mac entries with no active traffic, the age of the entries will be displayed based on the timestamp when the entries were first learnt. if the entries learnt time is greater than the bridge-mac-age-time (default 300secs), the age of the mac entries will be displayed as zero.

Use the `no` form of this command to disable the display of MAC address aging timeout. When disabled the mac-address age will be the bridge-mac-age-time default 300secs.

Command Syntax

```
mac-ageing-display
no mac-ageing-display
```

Parameters

None

Default

By default, mac ageing display is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS DC Version 5.0.

Example

```
#configure terminal
(config)#mac-ageing-display
(config)#no mac-ageing-display
```

show allowed-ethertype

Use this command to show allowed and denied traffic statistics.

Note: Dropped slow protocol packets provides the count of slow protocol packets among the total dropped count. Total drop count is fetched from hardware and slow protocol packet count is fetched from software. Hence there can be one or two packet difference.

Command Syntax

```
show allowed-ethertype statistics (IFNAME|)
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show allowed-ethertype statistics
Interface po1
arp : 0 Packets, 0 Bytes
ipv4 : 511016709 Packets, 184897169366 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 220 Packets, 28160 Bytes
dropped slow protocol pkts : lacp 220, efm 0, others 0
Interface xe47
arp : 0 Packets, 0 Bytes
ipv4 : 169763534 Packets, 61427990740 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 0 Packets, 0 Bytes
Interface xe48
arp : 0 Packets, 0 Bytes
ipv4 : 0 Packets, 0 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 0 Packets, 0 Bytes
```


© 2021 IP Infusion Inc. Proprietary

show bridge

Use this command to display the filtering database for the bridge. The filtering database is used by a switch to store the MAC addresses that have been learned and which ports that MAC address was learned on.

Command Syntax

```
show bridge (ieee|rpvst+|mstp|)
```

Parameters

`ieee`	STP bridges.
`rpvst+`	RPVST+ bridges.
`mstp`	MSTP bridges.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1         1                   eth1         5254.0029.929c     1     0
 1         2                   eth1         5254.004c.dcc6     1     297
 1         1                   eth1         5254.004c.dcc6     1     291
```

Table 2-92 explains the show command output fields.

Table 2-92: show bridge output fields

Field	Description
Bridge	Bridge identifier.
VLAN, SVLAN, BVLAN	CVLAN, SVLAN, and BVLAN identifiers.
Port	Interface name.
MAC Address	Learned MAC address.
FWD	Whether frames for the MAC addresses are forwarded.
Time-out	How long the learned MAC address persists.

show interface switchport

Use this command to display the characteristics of the interface with the current VLAN.

Command Syntax

```
show interface switchport bridge <1-32>
```

Parameter

`bridge`	Bridge name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is an output of this command displaying the characteristics of this interface on bridge 2.

```
#show interface switchport bridge 2
 Interface name          : eth5
 Switchport mode         : access
 Ingress filter          : disable
 Acceptable frame types  : all
 Vid swap                : disable
 Default vlan            : 2
 Configured vlans        :    2
 Interface name          : eth4
 Switchport mode         : access
 Ingress filter          : disable
 Acceptable frame types  : all
 Vid swap                : disable
 Default vlan            : 1
 Configured vlans        :    1
```

Table 2-93 explains the show command output fields.

Table 2-93: show interface switchport output fields

Field	Description
Interface name	Display the name of interface.
Switchport mode	Port that used to connect between switches and access port.
Ingress filter	Ingress filtering examines all inbound packets and then permits or denies entry to the network.
Acceptable frame types	Type of acceptable frame in the interface.
VID swap	Displays the status of the VID swap.

© 2021 IP Infusion Inc. Proprietary

Table 2-93: show interface switchport output fields (Continued)

Field	Description
Default vlan	Default value for the VLAN.
Configured vlans	Displays the information on configured VLANs.

show mac address-table count bridge

Use this command to display a count of MAC entries from the filtering database.

Command Syntax

```
show mac address-table (local|remote) bridge <1-32> ({address MAC | interface
  IFNAME | vlan <1-4094> }|)
```

Parameter

`local`	MAC entries learned locally
`remote`	MAC entries learned from MLAG MAC sync
`<1-32>`	Bridge group
`MAC`	MAC address in HHHH.HHHH.HHHH format
`IFNAME`	Name of the interface
`<1-4094>`	VLAN identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac address-table count bridge 1
MAC Entries for all vlans:
Total MAC Addresses in Use: 3
```

Table 2-94 explains the show command output fields.

Table 2-94: show mac address-table count output fields

Field	Description
Multicast MAC Address Count	Number of multicast addresses.
Total MAC Addresses	Total number of addresses.

© 2021 IP Infusion Inc. Proprietary

show mac address-table bridge

Use this command to display MAC entries from the filtering database.

Command Syntax

```
show mac address-table (local|remote) bridge <1-32>({address MAC|interface
  FNAME|vlan <1-4094>}|)
show mac address-table count bridge <1-32>({(dynamic|multicast|static)|address
  MAC|interface IFNAME|vlan <1-4094>}|)
```

Parameter

`local`	MAC entries learned locally
`remote`	MAC entries learned from MLAG MAC sync
`<1-32>`	Bridge group
`dynamic`	Dynamic entries
`multicast`	Multicast entries
`static`	Static entries
`MAC`	MAC address in HHHH.HHHH.HHHH format
`IFNAME`	Name of the interface
`<1-4094>`	VLAN identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac address-table bridge 1 static interface ge14
 VLAN     MAC Address     Type      Ports
  ------+--------------+---------+---------+--------------
  1      3333.3333.3333   static    ge14

#show mac address-table bridge 1
 VLAN     MAC Address     Type      Ports
  ------+--------------+---------+---------+--------------
  1      3417.ebf6.0ace   dynamic   po1
  1      6400.6a8e.48ab   dynamic   po1
  1      a82b.b5b5.c37b   dynamic   po1
  200    0000.5e00.0101   dynamic   po1
  200    3417.ebf6.0ac5   dynamic   po1
  200    3417.ebf6.0ace   dynamic   po1
  200    6400.6a8e.48ab   dynamic   po1
  200    a82b.b5b5.c375   dynamic   po1
  200    a82b.b5b5.c37b   dynamic   po1
  800    0000.5e00.0102   dynamic   po1
  800    3417.ebf6.0ac5   dynamic   po1
```

© 2021 IP Infusion Inc. Proprietary

```
800     3417.ebf6.0ace   dynamic   po1
800     6400.6a8e.48ab   dynamic   po1
800     a82b.b5b5.c375   dynamic   po1
800     a82b.b5b5.c37b   dynamic   po1
```

Table 2-95 explains the show command output fields.

Table 2-95: show mac address-table output fields

Field	Description
VLAN	VLAN identifier.
MAC Address	Media Access Control address.
Type	Dynamic, multicast, or static.
Ports	Interface name.

© 2021 IP Infusion Inc. Proprietary

show mac-address-table bridge 1 learning

Use this command to display if we have disabled mac learning in any of the interfaces.

Command Syntax

show mac-address-table bridge <1-32> learning

Parameter

<1-32>	Bridge group
Learning	mac learning

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#no mac-address-table learning bridge 1 ?

interface     Interface
vlan              range(s): 2-5 10 or 2-5 7-19
OcNOS(config)#no mac-address-table learning bridge 1 interface xe1/1
OcNOS#show mac-address-table bridge 1 learning
!
no mac-address-table learning bridge 1 interface xe1/1
!
```

switchport

Use this command to set the mode of an interface to switched.

All interfaces are configured routed by default. To change the behavior of an interface from switched to routed, you must explicitly give the `no switchport` command.

Note: When you change the mode of an interface from switched to routed and vice-versa, all configurations for that interface are erased.

Use the `no` form of this command to set the mode to routed.

Command Syntax

```
switchport
no switchport
```

Parameters

None

Default

All interfaces are configured routed by default. To change the behavior of an interface from switched to routed, you must explicitly give the no switchport command.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport

(config)#interface eth0
(config-if)#no switchport
```


© 2021 IP Infusion Inc. Proprietary

switchport allowed ethertype

Use this command to allow a set of ethertype on the access port and deny remaining traffic.

Use the no command to remove ethertype configuration.

Command Syntax

```
switchport allowed ethertype {arp|ipv4|ipv6|mpls|WORD|log}
no switchport allowed ethertype ({arp|ipv4|ipv6|mpls|WORD|log}|)
```

Parameters

`arp`	Ethertype 0x0806.
`ipv4`	Ethertype 0x0800.
`ipv6`	Ethertype 0x086dd.
`mpls`	Ethertype 0x8847.
`WORD`	Any Ethertype value (0x600 - 0xFFFF).
`log`	Log unwanted ethertype packets.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport allowed ethertype arp ipv4 ipv6 log

(config-if)#no switchport allowed ethertype ipv4
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 Spanning Tree Protocol Commands

This chapter provides a description, syntax, and examples of the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and Provider RSTP commands.

- bridge cisco-interoperability
- bridge instance
- bridge instance priority
- bridge instance vlan
- bridge multiple-spanning-tree
- bridge protocol ieee
- bridge protocol mstp
- bridge protocol rstp
- bridge provider-rstp
- bridge rapid-spanning-tree
- bridge region
- bridge revision
- bridge spanning-tree
- bridge spanning-tree errdisable-timeout
- bridge spanning-tree force-version
- bridge spanning-tree pathcost
- bridge spanning-tree portfast
- bridge te-msti
- bridge te-msti vlan
- bridge-group instance
- bridge-group instance path-cost
- bridge-group instance priority
- bridge-group path-cost
- bridge-group priority
- bridge-group spanning-tree
- clear spanning-tree detected protocols
- clear spanning-tree statistics
- customer-spanning-tree customer-edge path-cost
- customer-spanning-tree customer-edge priority
- customer-spanning-tree forward-time
- customer-spanning-tree hello-time
- customer-spanning-tree max-age
- customer-spanning-tree priority
- customer-spanning-tree provider-edge path-cost
- customer-spanning-tree provider-edge priority

© 2021 IP Infusion Inc. Proprietary

- customer-spanning-tree transmit-holdcount
- debug mstp
- show debugging mstp
- show debugging mstp
- show debugging mstp
- show spanning-tree
- show spanning-tree mst
- show spanning-tree statistics
- snmp restart mstp
- spanning-tree autoedge
- spanning-tree edgeport
- spanning-tree edgeport
- spanning-tree guard
- spanning-tree instance restricted-role
- spanning-tree instance restricted-tcn
- spanning-tree link-type
- spanning-tree mst configuration
- spanning-tree restricted-domain-role
- spanning-tree restricted-role
- spanning-tree restricted-tcn
- spanning-tree te-msti configuration
- storm-control
- show strom-control

© 2021 IP Infusion Inc. Proprietary

bridge cisco-interoperability

Use this command to enable/disable Cisco interoperability for MSTP (Multiple Spanning Tree Protocol).

If Cisco interoperability is required, all OcNOS devices in the switched LAN must be Cisco-interoperability enabled. When OcNOS inter operates with Cisco, the only criteria used to classify a region are the region name and revision level. VLAN-to-instance mapping is not used to classify regions when interoperating with Cisco.

Command Syntax

```
bridge <1-32> cisco-interoperability (enable | disable)
```

Parameters

`<1-32>`	Specify the bridge group ID
`enable`	Enable Cisco interoperability for MSTP bridge
`disable`	Disable Cisco interoperability for MSTP bridge

Default

By default, cisco interoperability is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

To enable Cisco interoperability on a switch for a bridge:

```
#configure terminal
(config)#bridge 2 cisco-interoperability enable
```

To disable Cisco interoperability on a switch for a particular bridge:

```
#configure terminal
(config)#bridge 2 cisco-interoperability disable
```

© 2021 IP Infusion Inc. Proprietary

bridge instance

Use this command to add an MST instance to a bridge.

Use the `no` form of this command to delete an MST instance identifier from a bridge.

Command Syntax

```
bridge (<1-32> | backbone) instance (<1-63>)
no bridge (<1-32> | backbone) instance (<1-63>)
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	MST instance identifier.

Default

The bridge instance default is 1.

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 4 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3
...
(config-mst)#no bridge 4 instance 3
```


© 2021 IP Infusion Inc. Proprietary

bridge instance priority

Use this command to set the bridge instance priority.

Use the `no` form of this command to reset the priority to its default.

Command Syntax

```
bridge (<1-32> | backbone) instance <1-63> priority <0-61440>
no bridge (<1-32> | backbone) instance <1-63> priority
```

Parameters

`<1-32>`	Specify the bridge identifier.
`backbone`	Specifies the backbone bridge.
`<1-63>`	Specify the instance identifier.
`priority`	Specify the bridge priority for the instance. The lower the priority of the bridge, the better the chances is of the bridge becoming a root bridge or a designated bridge for the LAN. The priority values can be set only in increments of 4096. The default value is 32768.
`<0-61440>`	Specify the bridge priority.

Default

By default, bridge instance priority is 32768

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#bridge 4 instance 3 priority 1
```

bridge instance vlan

Use this command to simultaneously add multiple VLANs for the corresponding instance of a bridge.The VLANs must be created before being associated with an MST instance (MSTI). If the VLAN range is not specified, the MSTI will not be created.

Use the `no` form of this command to simultaneously remove multiple VLANs for the corresponding instance of a bridge.

Command Syntax

```
bridge (<1-32> | backbone) instance (<1-63>) vlan VLANID
no bridge (<1-32> | backbone) instance (<1-63>) vlan VLANID
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	MST instance identifier.
`VLANID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list. For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Default

The bridge instance VLAN ID Interfaces default-switch is VLAN100 100 ae0.0 ae1.0 ae2.0.

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

To associate multiple VLANs, in this case VLANs 10 and 20 to instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 1 instance 1 vlan 10,20
```

To associate multiple VLANs, in this case, VLANs 10, 11, 12, 13, 14, and 15 to instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 1 instance 1 vlan 10-15
```

To delete multiple VLANs, in this case, VLANs 10 and 11 from instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
```

 © 2021 IP Infusion Inc. Proprietary

```
(config-mst)#no bridge 1 instance 1 vlan 10,11
```

bridge multiple-spanning-tree

Use this command to enable MSTP globally on a bridge.

Use the `no` form of this command to disable MSTP globally on a bridge.

Command Syntax

```
bridge <1-32> multiple-spanning-tree enable
no bridge <1-32> multiple-spanning-tree enable (bridge-blocked|bridge-forward|)
```

Parameters

`<1-32>`	Bridge-group ID.
`bridge-blocked`	Put ports of the bridge in the blocked state (default).
`bridge-forward`	Put ports of the bridge in the forwarding state.

Default

By default, this feature is enabled.

For the `no` form of this command, `bridge-blocked` is the default.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 multiple-spanning-tree enable

#configure terminal
(config)#no bridge 2 multiple-spanning-tree enable bridge-forward
```


© 2021 IP Infusion Inc. Proprietary

bridge protocol ieee

Use this command to add a IEEE 802.1d Spanning Tree Protocol bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in interface mode.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol ieee (vlan-bridge|)
no bridge <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.
`vlan-bridge`	Specify this as a VLAN-aware bridge.

Default

The bridge protocol default value is 2 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 protocol ieee

(config)#bridge 4 protocol ieee vlan-bridge
```

bridge protocol mstp

Use this command to create a multiple spanning-tree protocol (MSTP) bridge of a specified parameter. This command creates an instance of the spanning tree and associates the VLANs specified with that instance.

The MSTP bridges can have different spanning-tree topologies for different VLANs inside a region of “similar” MSTP bridges. The multiple spanning tree protocol, like the rapid spanning tree protocol, provides rapid reconfiguration capability, while providing load balancing ability. A bridge created with this command forms its own separate region unless it is added explicitly to a region using the `region name` command.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol mstp (ring|)
no bridge <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.

Default

The bridge protocol mstp default value is 50 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 protocol mstp

#configure terminal
(config)#bridge 2 protocol mstp ring
```


© 2021 IP Infusion Inc. Proprietary

bridge protocol rstp

Use this command to add an IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in Interface mode.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol rstp
bridge <1-32> protocol rstp (vlan-bridge|)(ring|)
no bridge <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.
`ring`	(Optional) Add an RSTP bridge for a ring topology.
`vlan-bridge`	(Optional) Adds a VLAN-aware bridge.

Default

By default, bridge protocol rstp is enabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 protocol rstp

#configure terminal
(config)#bridge 3 protocol rstp vlan-bridge
```

bridge provider-rstp

Use this command to enable Provider Rapid Spanning Tree Protocol (Provider RSTP) globally on a bridge.

Use the `no` form of this command to disable Provider RSTP globally on a bridge.

Command Syntax

```
bridge <1-32> provider-rstp enable
no bridge <1-32> provider-rstp enable (bridge-blocked|bridge-forward|)
```

Parameters

`<1-32>`	Bridge group ID.
`bridge-blocked`	Put ports of the bridge in the blocked state (default).
`bridge-forward`	Put ports of the bridge in the forwarding state.

Default

By default, this feature is enabled.

For the `no` form of this command, `bridge-blocked` is the default.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 provider-rstp enable

#configure terminal
(config)#no bridge 1 provider-rstp enable bridge-block
```


© 2021 IP Infusion Inc. Proprietary

bridge rapid-spanning-tree

Use this command to enable Rapid Spanning Tree Protocol (RSTP) globally on a bridge.

Use the `no` form of the command to disable RSTP globally on a bridge.

Command Syntax

```
bridge <1-32> rapid-spanning-tree enable
no bridge <1-32> rapid-spanning-tree enable (bridge-blocked|bridge-forward|)
```

Parameters

`<1-32>`	Bridge group ID.
`bridge-blocked`	Put ports of the bridge in the blocked state (default).
`bridge-forward`	Put ports of the bridge in the forwarding state.

Default

By default, this feature is enabled.

For the `no` form of this command, `bridge-blocked` is the default.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 rapid-spanning-tree enable

#configure terminal
(config)#no bridge 2 rapid-spanning-tree enable bridge-forward
```

bridge region

Use this command to create an MST region and specify its name. MST bridges of a region form different spanning trees for different VLANs.

Use the `no` form of the command to disable the Rapid Spanning Tree protocol on a region.

Command Syntax

```
bridge <1-32> region REGION_NAME
no bridge <1-32> region
```

Parameters

`<1-32>`	Specify the bridge group ID.
`REGION_NAME`	Specify the name of the region.

Default

By default, each MST bridge starts with the region name as its bridge address. This means each MST bridge is a region by itself, unless specifically added to one.

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 3 region myRegion

(config)#spanning-tree mst configuration
(config-mst)#no bridge 3 region
```


© 2021 IP Infusion Inc. Proprietary

bridge revision

Use this command to specify the number for configuration information.

Command Syntax

```
bridge <1-32> revision <0-65535>
```

Parameters

<1-32>	Specify the bridge group ID in the range of <1-32>.
<0-65535>	Specify a revision number in the range of <0-65535>.

Default

By default, revision number is 0

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 3 revision 25
```

bridge spanning-tree

Use this command to enable Spanning Tree Protocol (STP) globally on a bridge.

Use the `no` form of this command to disable STP globally on the bridge.

Command Syntax

```
bridge <1-32> spanning-tree enable
no bridge <1-32> spanning-tree enable (bridge-blocked|bridge-forward|)
```

Parameters

`<1-32>`	Bridge group ID.
`bridge-blocked`	Put ports of the bridge in the blocked state (default).
`bridge-forward`	Put ports of the bridge in the forwarding state.

Default

By default, this feature is enabled.

For the `no` form of this command, `bridge-blocked` is the default.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 spanning-tree enable

#configure terminal
(config)#no bridge 2 spanning-tree enable bridge-forward
```


© 2021 IP Infusion Inc. Proprietary

bridge spanning-tree errdisable-timeout

Use this command to enable the error-disable-timeout facility, which sets a timeout for ports that are disabled due to the BPDU guard feature.

The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port. This command associates a timer with the feature such that the port gets enabled back without manual intervention after a set interval.

Use the `no` parameter to disable the error-disable-timeout facility.

Command Syntax

```
bridge <1-32> spanning-tree errdisable-timeout enable
bridge <1-32> spanning-tree errdisable-timeout interval <10-1000000>
no bridge <1-32> spanning-tree errdisable-timeout enable
no bridge <1-32> spanning-tree errdisable-timeout interval
```

Parameters

`<1-32>`	Specify the bridge group ID.
`enable`	Enable the timeout mechanism for the port to be enabled back
`interval`	Specify the interval after which port shall be enabled.
`<10-1000000>`	Specify the error-disable-timeout interval in seconds.

Default

By default, the port is enabled after 300 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 spanning-tree errdisable-timeout enable

#configure terminal
(config)#bridge 4 spanning-tree errdisable-timeout interval 34
```

bridge spanning-tree force-version

Use this command to set the version for the bridge. A version identifier of less than a value of 2 enforces the spanning tree protocol. Although the command supports an input range of 0-4, for RSTP, the valid range is 0-2. When the force-version is set for a bridge, all ports of the bridge have the same spanning tree version set.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the no parameter with this command to disable the version for the bridge.

Command Syntax

```
bridge <1-32> spanning-tree force-version <0-4>
no bridge <1-32> spanning-tree force-version
```

Parameters

`<1-32>`	Specify the bridge group ID.
`force-version`	Specify a force version identifier:
`0`	STP
`1`	Not supported
`2`	RSTP
`3`	MSTP

Default

By default, spanning tree force version is 0

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

Set the value to enforce the spanning tree protocol:

```
#configure terminal
(config)#bridge 1 spanning-tree force-version 0

(config)#no bridge 1 spanning-tree force-version
```


© 2021 IP Infusion Inc. Proprietary

bridge spanning-tree pathcost

Use this command to set a spanning-tree path cost method.

If the short parameter is used, the switch uses a value for the default path cost a number in the range 1 through 65,535. If the long parameter is used, the switch uses a value for the default path cost a number in the range 1 through 200,000,000. Refer to the show spanning-tree to view the administratively configured and current running pathcost method running on a bridge.

Use the no option with this command to return the path cost method to the default setting.

Command Syntax

```
bridge <1-32> spanning-tree pathcost method (short|long)
no bridge <1-32> spanning-tree pathcost method
```

Parameters

`<1-32>`	Specify the bridge group ID.
`method`	Method used to calculate default port path cost.
`long`	Use 16-bit based values for default port path costs.
`short`	Use 32-bit based values for default port path costs.

Default

By default, path cost method for STP is short and for MSTP/RSTP is long.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 spanning-tree pathcost method short

(config)#no bridge 1 spanning-tree pathcost method
```

bridge spanning-tree portfast

Use this command to set the portfast BPDU (Bridge Protocol Data Unit) guard or filter for the bridge.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the `no` parameter with this command to disable the BPDU filter for the bridge.

BPDU Filter

All ports that have their BPDU filter set to default take the same value of BPDU filter as that of the bridge. The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures that PortFast-enabled ports do not transmit or receive any BPDUs.

BPDU Guard

When the BPDU guard feature is set for a bridge, all portfast-enabled ports of the bridge that have the BPDU guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed. You can either bring the port back up manually by using the `no shutdown` command, or configure the errdisable-timeout feature to enable the port after the specified time interval.

Command Syntax

```
bridge <1-32> spanning-tree portfast bpdu-guard
bridge <1-32> spanning-tree portfast bpdu-filter
no bridge <1-32> spanning-tree portfast bpdu-guard
no bridge <1-32> spanning-tree portfast bpdu-filter
```

Parameters

`<1-32>`	Specify the bridge group ID.
`bpdu-filter`	Specify to filter the BPDUs on portfast enabled ports.
`bpdu-guard`	Specify to guard the portfast ports against BPDU receive.

Default

By default, portfast for STP is enabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 spanning-tree portfast bpdu-filter

#configure terminal
(config)#bridge 1 spanning-tree portfast bpdu-guard
```


© 2021 IP Infusion Inc. Proprietary

bridge te-msti

Use this command to enable or disable a Multiple Spanning Tree Instance (MSTI).

The te-msti always refers to the MST instance indexed by the pre-defined macro constant MSTP_TE_MSTID internally. This is the only MST instance which supports the disabling of spanning trees.

Use the no form of this command to remove the configuration.

Command Syntax

```
bridge (<1-32> | backbone) te-msti
no bridge (<1-32> | backbone) te-msti
```

Parameters

<1-32>	Specify the bridge group ID.
backbone	Identity of the backbone bridge group.
te-msti	MSTI to be the traffic engineering MSTI instance.

Default

By default, bridge te-msti is disabled

Command Mode

TE-MSTI Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#bridge 2 te-msti

(config-te-msti)#no bridge 2 te-msti
```

bridge te-msti vlan

Use this command to enable or disable a Multiple Spanning Tree Instance (MSTI). When an MSTI is shutdown (disabled) each VLAN in the MSTI is set to the forwarding state on all bridge ports which the VLAN as a member of. When and MSTI is enabled (no shutdown), normal MSTP operation is started for the MSTI.

The t`e-msti` always refers to the MST instance indexed by the pre-defined macro constant `MSTP_TE_MSTID` internally. This is the only MST instance which supports the disabling of spanning trees. All VLANs that do not want spanning tree topology computation need to be assigned to this `te-msti` instance.

This command is intended for supporting Traffic Engineering (TE) Ethernet tunnels. All VLANs allocated for traffic engineering should be assigned to one MSTI. That MSTI can in turn shutdown the spanning tree operation so that each VLAN path through the network can be manually provisioned.

Use the `no` form of this command to remove the configuration.

Command Syntax

```
bridge (<1-32> | backbone) te-msti vlan <1-4094>
no bridge (<1-32> | backbone) te-msti vlan <1-4094>
```

Parameters

`<1-32>`	Specify the bridge group ID.
`backbone`	Identity of the backbone bridge group.
`vlan`	Specify a VLAN.
`<1-4094>`	Specify a VLAN identifier to be associated.

Note: This designated instance is defined in 802.1Qay clause 8.9 to be 0xFFE.

Default

By default, te-msti vlan is vlan1.

Command Mode

TE-MSTI Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#bridge 2 te-msti vlan 10
(config-te-msti)#no bridge 2 te-msti vlan 10
```


© 2021 IP Infusion Inc. Proprietary

bridge-group instance

Use this command to assign a Multiple Spanning Tree (MST) instance to a port.

Use the `no` form of this command to remove the interface from the MST instance.

Command Syntax

```
bridge-group (<1-32> | backbone) instance (<1-63> | te-msti)
no bridge-group (<1-32> | backbone) instance (<1-63> | te-msti)
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	Multiple spanning tree instance identifier.
`te-msti`	Traffic engineering MSTI instance.
	For Provider Backbone Bridging (PBB), bridge-group <1-32> refers to the I-component or PB bridge while the <backbone> bridge group refers to the B-component. Usually for a BEB (Backbone Edge Bridge) device, the backbone bridge-group is used for traffic engineering.
	For a PB (Provider Bridge) device used as BCB (Backbone Core Bridge), bridge group <1-32> is used for traffic engineering.

Default

By default, the bridge port remains in the listening and learning states for 15 seconds before transitional to the forwarding state.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#bridge-group 1
(config-if)#bridge-group 1 instance te-msti
```

bridge-group instance path-cost

Use this command to set a path cost for a multiple spanning tree instance.

Before you can give this command, you must explicitly add an MST instance to a port using the `bridge-group instance` command.

Use the `no` form of this command to set the path cost to its default which varies depending on bandwidth.

Command Syntax

```
bridge-group (<1-32> | backbone) instance <1-63> path-cost <1-200000000>
no bridge-group ( <1-32> | backbone) instance <1-63> path-cost
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Specify the backbone bridge.
`<1-63>`	Set the MST instance identifier.
`<1-200000000>`	Path cost for a port (a lower path cost means greater likelihood of becoming root).

Default

Assuming a 10 Mb/s link speed, the default value is 200,000.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3 vlan 3
(config-mst)#exit
(config)#interface eth1
(config-if)#bridge-group 4 instance 3
(config-if)#bridge-group 4 instance 3 path-cost 1000
```


© 2021 IP Infusion Inc. Proprietary

bridge-group instance priority

Use this command to set the priority of a multiple spanning tree instance.

The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

Command Syntax

```
bridge-group (<1-32>) instance (<1-63>) priority <0-240>
no bridge-group (<1-32>) instance (<1-63>) priority
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	Multiple spanning tree instance identifier.
`<0-240>`	Port priority. A lower value means greater likelihood of becoming root. Set the port priority in increments of 16.

Default

By default, the port priority is 128

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth2
(config-if)#bridge-group 2
(config-if)#bridge-group 2 instance 4
(config-if)#bridge-group 2 instance 4 priority 64
```

bridge-group path-cost

Use this command to set the cost of a path. Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the `bridge-group instance` command.

Use the `no` parameter with this command to restore the default cost value of the path which varies depending on the bandwidth.

Command Syntax

```
bridge-group <1-32> path-cost <1-200000000>
no bridge-group <1-32> path-cost
```

Parameters

`<1-32>`	Specify the bridge group ID.
`path-cost`	Specify the cost of path for a port.
`<1-200000000>`	Specify the cost of the path (a lower cost means a greater likelihood of the interface becoming root).

Default

Assuming a 10 Mb/s link speed, the default value is 200,000.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3 vlan 3
(config-mst)#exit
(config)#interface eth1
(config-if)#bridge-group 4
(config-if)#bridge-group 4 path-cost 1000
```


© 2021 IP Infusion Inc. Proprietary

bridge-group priority

Use this command to set the port priority for a bridge group.

The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

Command Syntax

```
bridge-group (<1-32> | backbone) priority <0-240>
no bridge-group (<1-32> | backbone) priority
```

Parameters

`<1-32>`	Specify the bridge group ID.
`backbone`	Backbone bridge.
`<0-240>`	Specify the port priority (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, port priority for each instance is 128

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#bridge-group 4 priority 80
```

bridge-group spanning-tree

Use this command to enable or disable spanning-tree on an interface.

Command Syntax

```
bridge-group <1-32> spanning-tree (disable|enable)
```

Parameters

`<1-32>`	Bridge group ID.
`disable`	Disable spanning tree on the interface.
`enable`	Enable spanning tree on the interface.

Default

By default, spanning-tree is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth1
(config-if)#bridge-group 1 spanning-tree enable
```


© 2021 IP Infusion Inc. Proprietary

clear spanning-tree detected protocols

Use this command to clear the detected protocols for a specific bridge or interface. This command begins the port migration as per IEEE 802.1w-2001, Section 17.26. After issuing this command, the migration timer is started on the port, only if the force version is RSTP or MSTP (greater versions of RSTP).

Command Syntax

```
clear spanning-tree detected protocols bridge <1-32>
```

Parameters

<1-32>	Specify the bridge group ID.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear spanning-tree detected protocols bridge 2
```

clear spanning-tree statistics

Use this command to clear all STP BPDU statistics.

Command Syntax

```
clear spanning-tree statistics bridge <1-32>
clear spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <1-4094>)
  bridge <1-32>
clear spanning-tree statistics (interface IFNAME| (instance (<1-63>)| vlan <2-
  4094>)) bridge <1-32>
```

Parameters

<1-32>	Specify the bridge identifier.
IFNAME	Specify the name of the interface on which protocols have to be cleared.
<1-63>	MST instance ID.
<1-4094>	VLAN identifier where spanning tree is located <2-4094>

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear spanning-tree statistics bridge 32
```


© 2021 IP Infusion Inc. Proprietary

customer-spanning-tree customer-edge path-cost

Use this command to set the cost of a path associated with a customer edge port on a customer edge spanning tree.

Use the `no` form of this command to remove the cost of a path associated with a customer edge port on a customer edge spanning tree.

Command Syntax

```
customer-spanning-tree customer-edge path-cost <1-200000000>
no customer-spanning-tree customer-edge path-cost
```

Parameters

`path-cost`	Specify the path-cost of a port.
`<1-200000000>`	Specify the cost to be assigned to the group.

Default

Assuming a 10 Mb/s link speed, the default value is 200,000

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree customer-edge path-cost 1000
```

customer-spanning-tree customer-edge priority

Use this command to set the port priority for a customer-edge port in the customer spanning tree.

Command Syntax

```
customer-spanning-tree customer-edge priority <0-240>
```

Parameters

`priority`	Specify the port priority.
`<0-240>`	Specify the port priority range (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree customer-edge priority 100
```


© 2021 IP Infusion Inc. Proprietary

customer-spanning-tree forward-time

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances.

Use the `no` form of this command to restore the default value of 15 seconds.

Command Syntax

```
customer-spanning-tree forward-time <4-30>
no customer-spanning-tree forward-time
```

Parameters

`<4-30>`	Specify the forwarding time delay in seconds.

Note: Care should be exercised if the value is set to less than 7 seconds.

Default

By default, priority is 15 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree forward-time 6

(config-if)#no customer-spanning-tree forward-time
```

customer-spanning-tree hello-time

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). Avoid a very low value of this parameter as this can lead to excessive traffic on the network; a higher value delays the detection of topology change. This value is used by all instances.

Use the `no` option with this command to restore the default value of the hello-time.

Command Syntax

```
customer-spanning-tree hello-time <1-10>
no customer-spanning-tree hello-time
```

Parameters

`<1-10>`	Specify the hello BPDU interval in seconds.

Default

By default, level is 2 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree hello-time 3

(config-if)#no customer-spanning-tree hello-time
```


© 2021 IP Infusion Inc. Proprietary

customer-spanning-tree max-age

Use this command to set the max-age for a bridge.

Max-age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of max-age should be greater than twice the value of hello-time plus one, but less than twice the value of forward delay minus one. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by a root can be propagated to the leaf nodes without exceeding the max-age.

Use the `no` parameter with this command to restore the default value of max-age.

Command Syntax

```
customer-spanning-tree max-age <6-40>
no customer-spanning-tree max-age
```

Parameters

`<6-40>`	Specify the maximum time in seconds to listen for the root bridge.

Default

By default, bridge max-age is 20 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree max-age 12

(config-if)#no customer-spanning-tree max-age
```

customer-spanning-tree priority

Use this command to set the bridge priority for the spanning tree on a customer edge port. Using a lower priority indicates a greater likelihood of the bridge becoming root. This command must be used to set the priority of the customer spanning tree running on the customer edge port.

Use the `no` form of the command to reset it to the default value.

Command Syntax

```
customer-spanning-tree priority <0-61440>
no customer-spanning-tree priority
```

Parameters

`<0-61440>`	Specify the bridge priority in the range <0-61440>. Priority values can be set only in increments of 4096.

Default

By default, priority is 61440

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree priority 4096

(config-if)#no customer-spanning-tree priority
```


© 2021 IP Infusion Inc. Proprietary

customer-spanning-tree provider-edge path-cost

Use this command to set the cost of a path associated with a provider edge port on a customer edge spanning tree.

Use the `no` form of this command to remove the cost of a path associated with a provider edge port on a customer edge spanning tree.

Command Syntax

```
customer-spanning-tree provider-edge svlan <1-4094> path-cost <1-200000000>
no customer-spanning-tree provider-edge svlan <1-4094> path-cost
```

Parameters

`<1-4094>`	Specify the SVLAN identifier of provider edge port.
`<1-200000000>`	Specify the cost to be assigned to the group.

Default

Assuming a 10 Mb/s link speed, the default value is 200,000

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree provider-edge svlan 2 path-cost 1000

(config-if)#no customer-spanning-tree provider-edge svlan 2 path-cost
```

customer-spanning-tree provider-edge priority

Use this command to set the port priority for a provider-edge port in the customer spanning tree.

Command Syntax

```
customer-spanning-tree provider-edge svlan <1-4094> priority <0-240>
```

Parameters

<1-4094>	Specify the SVLAN identifier of provider edge port.
<0-240>	Specify the port priority (a lower priority means greater likelihood of the interface becoming root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree provider-edge svlan 2 priority 0
```


© 2021 IP Infusion Inc. Proprietary

customer-spanning-tree transmit-holdcount

Use this command to set the transmit-holdcount for a bridge.

Use the `no` parameter with this command to restore the default value of `transmit-holdcount`.

Command Syntax

```
customer-spanning-tree transmit-holdcount <1-10>
no customer-spanning-tree transmit-holdcount
```

Parameters

`<1-10>`	Specify the maximum number that can be transmitted per second.

Default

By default, bridge transmit hold count is 6

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree transmit-holdcount 3

(config-if)#no customer-spanning-tree transmit-holdcount
```

debug mstp

Use this command to turn on, and turn off, debugging and echoing data to the console, at various levels.

Note: This command enables MSTP, RSTP, and STP debugging.

Use the `no` parameter with this command to turn off debugging.

Command Syntax

```
debug mstp all
debug mstp cli
debug mstp packet rx
debug mstp packet tx
debug mstp protocol
debug mstp protocol detail
debug mstp timer
debug mstp timer detail
no debug mstp all
no debug mstp cli
no debug mstp packet rx
no debug mstp packet tx
no debug mstp protocol
no debug mstp protocol detail
no debug mstp timer
no debug mstp timer detail
```

Parameters

`all`	Echoes all spanning-tree debugging levels to the console.
`cli`	Echoes spanning-tree commands to the console.
`packet`	Echoes spanning-tree packets to the console.
`rx`	Received packets.
`tx`	Transmitted packets.
`protocol`	Echoes protocol changes to the console.
`detail`	Detailed output.
`timer`	Echoes timer start to the console.
`detail`	Detailed output.

Command Mode

Exec, Privileged Exec, and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

© 2021 IP Infusion Inc. Proprietary

Examples

```
#configure terminal
(config)#debug mstp all
(config)#debug mstp cli
(config)#debug mstp packet rx
(config)#debug mstp protocol detail
(config)#debug mstp timer
```

show debugging mstp

Use this command to display the status of debugging of the MSTP system.

Command Syntax

```
show debugging mstp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging mstp
MSTP debugging status:
MSTP debugging status:
 MSTP timer debugging is on
 MSTP protocol debugging is on
 MSTP detailed protocol debugging is on
 MSTP cli echo debugging is on
 MSTP transmitting packet debugging is on
 MSTP receiving packet debugging is on
#
```


© 2021 IP Infusion Inc. Proprietary

show spanning-tree

Use this command to show the state of the spanning tree for all STP or RSTP bridge-groups, including named interface and VLANs.

Command Syntax

```
show spanning-tree
show spanning-tree interface IFNAME
show spanning-tree mst
show spanning-tree mst config
show spanning-tree mst interface IFNAME
show spanning-tree mst detail
show spanning-tree mst detail interface IFNAME
show spanning-tree mst instance (<1-63>) interface IFNAME
show spanning-tree mst instance (<1-63> | te-msti)
show spanning-tree statistics bridge <1-32>
show spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <2-4094>)
  bridge <1-32>
show spanning-tree statistics (interface IFNAME | (instance (<1-63>) | vlan <1-
  4094>)) bridge <1-32>
show spanning-tree vlan range-index
```

Parameters

`interface`	Display interface information
`mst`	Display MST information
`statistics`	Display statistics of the BPDUs
`vlan range-index`	Display a VLAN range-index value
`config`	Display configuration information
`detail`	Display detailed information
`instance`	Display instance information
`<1-63>`	Specify the instance identifier
`te-msti`	Display Traffic Engineering MSTI instance
`<1-32>`	Specify the bridge identifier
`IFNAME`	Display the interface name
`<2-4094>`	Specify a VLAN identifier, associated with the instance

Command Mode

Exec mode and Privileged Exec mode

© 2021 IP Infusion Inc. Proprietary

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command displaying spanning tree information.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%eth2: Ifindex 5 - Port Id 8005 - Role Designated - State Forwarding
%eth2: Designated Path Cost 0
%eth2: Configured Path Cost 200000 - Add type Explicit ref count 1
%eth2: Designated Port Id 8005 - Priority 128 -
%eth2: Root 80000002b328530a
%eth2: Designated Bridge 80000002b328530a
%eth2: Message Age 0 - Max Age 20
%eth2: Hello Time 2 - Forward Delay 15
%eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%eth2: forward-transitions 4
%eth2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%eth2: No portfast configured - Current portfast off
%eth2: portfast bpdu-guard default - Current portfast bpdu-guard off
%eth2: portfast bpdu-filter default - Current portfast bpdu-filter off
%eth2: no root guard configured- Current root guard off
%eth2: Configured Link Type point-to-point - Current point-to-point
%eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
%eth1: Designated Path Cost 0
%eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
%eth1: Designated Port Id 8004 - Priority 128 -
%eth1: Root 80000002b328530a
%eth1: Designated Bridge 80000002b328530a
%eth1: Message Age 0 - Max Age 20
%eth1: Hello Time 2 - Forward Delay 15
%eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%eth1: forward-transitions 4
%eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%eth1: No portfast configured - Current portfast off
%eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
%eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
%eth1: no root guard configured- Current root guard off
%eth1: Configured Link Type point-to-point - Current point-to-point
%
%
```

 © 2021 IP Infusion Inc. Proprietary

The following is a sample output of this command displaying the state of the spanning tree for interface `eth1`.

```
#show spanning-tree interface eth1
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
% eth1: Designated Path Cost 0
% eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
% eth1: Designated Port Id 8004 - Priority 128 -
% eth1: Root 80000002b328530a
% eth1: Designated Bridge 80000002b328530a
% eth1: Message Age 0 - Max Age 20
% eth1: Hello Time 2 - Forward Delay 15
% eth1: forward-transitions 4
% eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
% eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
% eth1: no root guard configured- Current root guard off
```

Table 3-96 Explains the show command output fields.

Table 3-96: show spanning-tree interface output fields

Field	Description
Bridge up	A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments.
Root Path Cost	Root cost for the interface.
Root Port	Interface that is the current elected root port for this bridge.
Bridge Priority	Used for the common instance.
Forward Delay	Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hello Time	Configured number of seconds between transmissions of configuration BPDUs.
Max Age	Maximum age of received protocol BPDUs.
Port Id	Logical interface identifier configured to participate in the MSTP instance.
Role Designated	Designated role for the packets in the interface.
State Forwarding	State of the forwarding packets in the interface.

Field	Description
Designated Path Cost	Designated cost for the interface.
Configured Path Cost	Configured cost for the interface.
Designated Port Id	Port ID of the designated port for the LAN segment this interface is attached to.
Priority	Specify the port priority.
Message Age	Number of seconds elapsed since the most recent BPDU was received.
Forward Timer	The forward delay timer is the time interval that is spent in the listening and learning state.
Msg Age Timer	The message age contains the length of time that has passed since the root bridge initially originated the BPDU.
Received RSTP	Number of times the received the RSTP.
Send RSTP	Number of times transmitted the RSTP.

© 2021 IP Infusion Inc. Proprietary

show spanning-tree mst

Use this command to display the filtering database values. This command displays the number of instances created, and VLANs associated with it.

Command Syntax

```
show spanning-tree mst
show spanning-tree mst config
show spanning-tree mst detail
show spanning-tree mst detail interface IFNAME
show spanning-tree mst instance (<1-63>) interface IFNAME
show spanning-tree mst instance (<1-63> | te-msti)
show spanning-tree mst interface IFNAME
```

Parameters

`config`	Display configuration information.
`detail`	Display detailed information.
`interface`	Display interface information.
`instance`	Display instance information.
`<1-63>`	Specify the instance identifier.
`te-msti`	Traffic Engineering MSTI instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000002b328530a
% 1: CIST Reg Root Id 80000002b328530a
% 1: CIST Bridge Id 80000002b328530a
% 1: 2 topology change(s) - last topology change Wed Nov 19 22:43:21 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
```

```
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec%
% Instance VLAN
% 0:         1
% 2:         3-4
```

Table 3-97 Explains the show command output fields.

Table 3-97: show spanning-tree mst output fields

Field	Description
Bridge up	A network bridge is networking process that creates a single aggregate network from multiple communication networks or network segments.
CIST Root Path Cost	Calculated cost to reach the regional root bridge from the bridge where the command is entered.
CIST Root Port	Interface that is the current elected CIST root port for this bridge.
CIST Bridge	A CIST bridge is networking process that creates a single aggregate network from multiple communication networks.
Priority	Specify the port priority.
Forward Delay	Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hello Time	Configured number of seconds between transmissions of configuration BPDUs.
Max Age	Maximum age of received protocol BPDUs.
Max-hops	Configured maximum number of hops a BPDU can be forwarded in the MSTP region.

© 2021 IP Infusion Inc. Proprietary

show spanning-tree statistics

Use this command to display detailed BPDU statistics for a spanning tree instance.

Command Syntax

```
show spanning-tree statistics bridge <1-32>
show spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <2-4094>)
  bridge <1-32>
show spanning-tree statistics (interface IFNAME | (instance (<1-63>) | vlan <1-
  4094>)) bridge <1-32>
```

Parameters

`<1-32>`	Bridge identifier.
`<1-63>`	MST instance identifier.
`IFNAME`	Displays the interface name.
`<2-4094>`	Specify a VLAN identifier, associated with the instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, bridge-group 1 is configured for IEEE on the eth2 interface.

```
#show spanning-tree statistics interface eth2 bridge 1

% BPDU Related Parameters
% ----------------------
% Port Spanning Tree                : Enable
% Spanning Tree Type                : Spanning Tree Protocol
% Current Port State                : Learning
% Port ID                           : 8004
% Port Number                       : 4
% Path Cost                         : 200000
% Message Age                       : 0
% Designated Root                   : 00:02:b3:d5:91:ec
% Designated Cost                   : 0
% Designated Bridge                 : 00:02:b3:d5:91:ec
% Designated Port Id                : 8005
% Top Change Ack                    : FALSE
% Configure Pending                    : FALSE

% PORT Based Information & Statistics
% ----------------------------------
% Configure Bpdu's xmitted              : 0
% Configure Bpdu's received             : 22
% TCN Bpdu's xmitted                : 0
```

```
% TCN Bpdu's received                : 8
% Forward Trans Count                : 0

% STATUS of Port Timers
% ---------------------
% Hello Time Configured               : 2
% Hello timer                        : ACTIVE
% Hello Time Value                   : 1
% Forward Delay Timer                : ACTIVE
% Forward Delay Timer Value          : 1
% Message Age Timer                  : ACTIVE
% Message Age Timer Value            : 19
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0

% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 14
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 15
% Next State                         : Blocked
% Topology Change Time               : 0


% Other Bridge information & Statistics
  -------------------------------------
% STP Multicast Address              : 01:80:c2:00:00:00
% Bridge Priority                    : 32768
% Bridge Mac Address                 : 00:02:b3:d5:98:3f
% Bridge Hello Time                  : 2
% Bridge Forward Delay               : 15
% Topology Change Initiator          : 0
% Last Topology Change Occurred       : Wed Dec 31 16:00:00 1969
% Topology Change                    : FALSE
% Topology Change Detected           : FALSE
% Topology Change Count              : 0
% Topology Change Last Recvd from    : 00:00:00:00:00:00
```

Table 3-98 Explains the show command output fields.

Table 3-98: show spanning-tree statistics output fields

Field	Description
BPDU Related Parameters	Details of the BPDU related parameters.
PORT Based Information & Statistics	Information of the port and interface for which the statistics are being displayed.

© 2021 IP Infusion Inc. Proprietary

Field	Description
STATUS of Port Timers	Status of the port timers.
Other Port-Specific Info	Specific information about the port.
Other Bridge information & Statistics	Information about bridge and statistics being displayed.

snmp restart mstp

Use this command to restart SNMP in Multiple Spanning Tree Protocol (MSTP).

Command Syntax

```
snmp restart mstp
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart mstp
```


© 2021 IP Infusion Inc. Proprietary

spanning-tree autoedge

Use this command to assist in automatic identification of the edge port.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
spanning-tree autoedge
no spanning-tree autoedge
```

Default

By default, spanning-tree autoedge is disabled

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree autoedge
```

spanning-tree edgeport

Use this command to set a port as an edge-port and to enable rapid transitions.

Use the `no` parameter with this command to set a port to its default state (not an edge-port) and to disable rapid transitions.

Note: This command is an alias to the `spanning-tree portfast` command. Both commands can be used interchangeably.

Command Syntax

```
spanning-tree edgeport
no spanning-tree edgeport
```

Default

By default, spanning-tree edgeport is disabled

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree edgeport
```


© 2021 IP Infusion Inc. Proprietary

spanning-tree guard

Use this command to enable the root guard feature for the port. This feature disables reception of superior BPDUs.

The root guard feature makes sure that the port on which it is enabled is a designated port. If the root guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

Use the `no` parameter with this command to disable the root guard feature for the port.

Command Syntax

```
spanning-tree guard root
no spanning-tree guard root
```

Parameters

`root`	Set to disable reception of superior BPDUs

Default

By default, spanning-tree guard root is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree guard root
```

spanning-tree instance restricted-role

Use this command to set the restricted role value for the instance to TRUE.

Use the `no` parameter with this command to set the restricted role value for the instance to FALSE.

Command Syntax

```
spanning-tree instance <1-63> restricted-role
no spanning-tree instance <1-63> restricted-role
```

Parameters

`<1-63>`	Specify the instance ID range.

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree instance 2 restricted-role
```


© 2021 IP Infusion Inc. Proprietary

spanning-tree instance restricted-tcn

Use this command to set the restricted TCN value for the instance to TRUE.

Command Syntax

```
spanning-tree instance <1-63> restricted-tcn
no spanning-tree instance <1-63> restricted
```

Parameters

<1-63>	Specify the instance ID range.

Default

By default, restricted TCN value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree instance 2 restricted-tcn
```

spanning-tree link-type

Use this command to enable or disable point-to-point or shared link types.

RSTP has a backward-compatible STP mode, `spanning-tree link-type shared`. An alternative is the `spanning-tree force-version 0`.

Use the `no` parameter with this command to disable rapid transition.

Command Syntax

```
spanning-tree link-type auto
spanning-tree link-type point-to-point
spanning-tree link-type shared
no spanning-tree link-type
```

Parameters

`auto`	Sets to either point-to-point or shared based on duplex state.
`point-to-point`	Enables rapid transition.
`shared`	Disables rapid transition.

Default

By default, spanning-tree link-type is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree link-type point-to-point

(config-if)#no spanning-tree link-type
```


© 2021 IP Infusion Inc. Proprietary

spanning-tree mst configuration

Use this command to enter the Multiple Spanning Tree Configuration mode.

Command Syntax

```
spanning-tree mst configuration
```

Parameters

None

Default

No default value is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#
```

spanning-tree bpdu-filter

Use this command to set the BPDU filter value for individual ports. When the `enable` or `disable` parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the `default` parameter is used with this command, the bridge level BPDU filter configuration takes effect for the port.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the `no` parameter with this command to revert the port BPDU filter value to default.

Command Syntax

```
spanning-tree bpdu-filter (enable|disable|default)
no spanning-tree bpdu-filter
```

Parameters

`default`	Sets the bpdu-filter to the default level.
`disable`	Disables the BPDU-filter.
`enable`	Enables the BPDU-filter.

Default

By default, spanning-tree bpdu-filter is default option

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree bpdu-filter enable

(config-if)#no spanning-tree bpdu-filter
```


© 2021 IP Infusion Inc. Proprietary

spanning-tree bpdu-guard

Use this command to enable or disable the BPDU Guard feature on a port.

This command supersedes the bridge level configuration for the BPDU Guard feature. When the `enable` or `disable` parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the `default` parameter is used with this command, the bridge-level BPDU Guard configuration takes effect.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the no parameter with this command to set the BPDU Guard feature on a port to default.

Command Syntax

```
spanning-tree bpdu-guard (enable|disable|default)
no spanning-tree bpdu-guard
```

Parameters

`default`	Sets the BPDU-guard to the default level.
`disable`	Disables the BPDU-guard.
`enable`	Enables the BPDU-guard.

Default

By default, spanning-tree bpdu-guard is default

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree bpdu-guard enable

(config-if)#no spanning-tree bpdu-guard
```

spanning-tree restricted-domain-role

Use this command to set the restricted-domain-role value of the port to TRUE.

Use the `no` parameter with this command to set the restricted-domain-role value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-domain-role
no spanning-tree restricted-domain-role
```

Parameters

None

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-domain-role
```


© 2021 IP Infusion Inc. Proprietary

spanning-tree restricted-role

Use this command to set the restricted-role value of the port to TRUE.

Use the `no` parameter with this command to set the restricted-role value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-role
no spanning-tree restricted-role
```

Parameters

None

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-role
```

spanning-tree restricted-tcn

Use this command to set the restricted TCN value of the port to TRUE.

Use the `no` parameter with this command to set the restricted TCN value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-tcn
no spanning-tree restricted-tcn
```

Parameters

None

Default

By default, restricted TCN value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-tcn
```


© 2021 IP Infusion Inc. Proprietary

spanning-tree te-msti configuration

This command is used to put the terminal into the `te-msti` configuration mode.

After creating a bridge instance and adding VLAN to that bridge instance, use this command to enter `te-msti` configuration mode.

Command Syntax

```
spanning-tree te-msti configuration
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#
```

storm-control

Use this command to set the rising threshold level for broadcast, multicast, or destination lookup failure traffic. The storm control action occurs when traffic utilization reaches this level.

Storm control is used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

Storm-control is a physical interface property and when configured on port-channel storm-control is applied on each physical member port and therefore the actual value is the configured value multiplied by the number of active member interfaces.

Use the `no` form of this command to disable storm control.

Note: Minimum granularity for storm-control is 64kbps.

Command Syntax

```
storm-control (broadcast|multicast|dlf) (level LEVEL | <0-1000000000>
  (kbps|mbps|gbps))
no storm-control (broadcast|multicast|dlf)
```

Parameters

`broadcast`	Broadcast rate limiting.
`multicast`	Multicast rate limiting.
`dlf`	Destination lookup failure limiting.
`level`	Sets the percentage of the threshold.
`LEVEL`	The percentage of the threshold; percentage of the maximum speed (pps) of the interface <0.0000-1000.0000>.
`<0-1000000000>`	Sets absolute threshold value <0-1000000000>
`kbps`	specifies the units of Kilobits per second.
`mbps`	specifies the units of Megabits per second.
`gbps`	specifies the units of Gigabits per second.

Note: Use value for absolute threshold value parameter in multiples of 64 kbps. Whether the unit of measure is kbps, mbps, or gbps, the value must be divisible by 64 (such as "99.968 mbps").

Default

By default, storm control is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
```


© 2021 IP Infusion Inc. Proprietary

```
(config-if)#storm-control broadcast level 30

(config)#interface eth0
(config-if)#storm-control multicast level 30

(config)#interface eth0
(config-if)#storm-control multicast 64 mbps

(config)#interface eth0
(config-if)#no storm-control multicast

OcNOS(config-if)#storm-control multicast 50 kbps
%% Value applicable in hardware is 64.000 kbps

OcNOS(config-if)#storm-control multicast 0 kbps

OcNOS(config-if)#storm-control multicast 64 kbps

OcNOS(config-if)#storm-control multicast 100 kbps
%% Value applicable in hardware is 64.000 kbps

OcNOS(config-if)#storm-control multicast 130 kbps
%% Value applicable in hardware is 128.000 kbps

OcNOS(config-if)#storm-control multicast 130 mbps
%% Value applicable in hardware is 129.984 mbps
(config)#int xe1/1
(config-if)#switchport
(config-if)#storm-control multicast 100 mbps
%% Value applicable in hardware is 99.968 mbps

#show storm-control xe1/1
*The hardware applicable value is displayed
Port          BcastLevel    McastLevel    DlfLevel      Discards
xe1/1         100.0000%     99.968 mbps   100.0000%     0

#show run int xe1/1
!
interface xe1/1
 switchport
 storm-control multicast 100 mbps

(config-if)#int po4
(config-if)#switchport
#show storm-control po4
*The hardware applicable value is displayed
Port          BcastLevel    McastLevel    DlfLevel      Discards
po4           219.968 mbps  100.0000%     100.0000%     0
#
```

Note:

- The warning message appears only for the applicable value in multiples ok 64 kbps.
- show running-config command displays the value that was entered by user.

- show storm-control displyas the actual configured value. If the configured value is from 1-64 kbps, the configured vlaue is treated as 64, similarly from 100-127 value the configured value is dropped to 64 kbps.
- For example, values configured from
  1-64 kbps becomes 64 kbps,
  100 kbps becomes 64 kbps,
  130 kbps becomes 128 kbps,
  200 kbps becomes 192 kbps so on.

© 2021 IP Infusion Inc. Proprietary

show strom-control

Use the command to verify the BUM rate limit configured.

Note: Drop statistics for BUM rate limiting is not supported on Qumran.

Command Syntax

```
show storm-control (INTERFACE-NAME|)
```

Example

```
OcNOS#sh storm-control xe2
*The hardware applicable value is displayed
Port          BcastLevel    McastLevel    DlfLevel      Discards
xe2           100.0000%     100.0000%     100.0000%     0
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 RPVST+ Commands

This chapter contains the commands used for Rapid Per VLAN Spanning Tree (RPVST+). RPVST+ enables a bridge to inter-operate with Cisco RPVST+ switches.

RPVST+ uses the Multiple Spanning Tree Protocol (MSTP) with a single VLAN for each Multiple Spanning Tree instance (MSTI). The MST bridges can have different spanning-tree topologies for different VLANs inside a region of similar MST bridges. MSTP, like the Rapid Spanning Tree Protocol (RSTP), provides rapid reconfiguration capabilities and supports load balancing.

This chapter includes the following commands:

- bridge vlan
- bridge vlan priority
- bridge-group vlan
- bridge protocol rpvst+
- bridge rapid-pervlan-spanning-tree
- show spanning-tree rpvst+
- spanning-tree rpvst+ configuration
- spanning-tree vlan restricted-role
- spanning-tree vlan restricted-tcn

© 2021 IP Infusion Inc. Proprietary

bridge vlan

This command creates or deletes a mapping between an MSTI (Multiple Spanning Tree Instance) and a VLAN for RPVST+ operation. There can be only one VLAN per MST instance if the bridge is configured to run in RPVST+ mode.

The VLAN must have already been created. Spanning tree is enabled on each configured VLAN, and one instance of spanning-tree runs on each configured VLAN.

Use the `no` form of the command to disable this functionality.

Command Syntax

```
bridge <1-32> vlan <2-4094>
no bridge <1-32> vlan <2-4094>
```

Parameters

`<1-32>`	Bridge identifier.
`<2-4094>`	VLAN identifier.

Command Mode

RPVST+ configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree rpvst+ configuration
(config-rpvst+)#bridge 1 vlan 2
(config-rpvst+)#no bridge 1 vlan 2
```


© 2021 IP Infusion Inc. Proprietary

bridge vlan priority

This command sets the priority value for the spanning-tree on the bridge. The lower the priority of the VLAN on a bridge, the better the chances of the bridge becoming a root bridge, or a designated bridge for the VLAN.

Use the `no` form of this command to set the priority to its default (32,768).

Command Syntax

```
bridge <1-32> vlan <2-4094> priority <0-61440>
no bridge <1-32> vlan <2-4094> priority
```

Parameters

`<1-32>`	Bridge identifier.
`<2-4094>`	VLAN identifier.
`<0-61440>`	Bridge priority for the common instance. Set the priority in increments of 4096. A lower priority indicates greater likelihood of becoming root.

Default

By default, priority for each VLAN is 32,768

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 vlan 2 priority 80
(config)#no bridge 1 vlan 10 priority
```

© 2021 IP Infusion Inc. Proprietary

bridge-group vlan

Use this command to assign a Rapid Per-VLAN Spanning Tree (RPVST+) instance to a port.

RPVST+ uses port priority as a tiebreaker to determine which port should forward frames for a particular LAN, or which port should be the root port for a VLAN. A lower value implies a better priority. In the case of the same priority, the interface index serves as the tiebreaker, with a lower-numbered interface being preferred over others.

Use the `no` parameter with this command to remove an RPVST+ instance from this port.

Command Syntax

```
bridge-group <1-32> vlan <2-4094>
bridge-group <1-32> vlan <2-4094> path-cost <1-200000000>
bridge-group <1-32> vlan <2-4094> priority <0-240>
no bridge-group <1-32> vlan <2-4094>
no bridge-group <1-32> vlan <2-4094> path-cost
no bridge-group <1-32> vlan <2-4094> priority
```

Parameters

`<1-32>`	Bridge group identifier.
`<2-4094>`	VLAN identifier.
`<1-200000000>`	Cost of a path associated with the interface.
`<0-240>`	Port priority. A lower priority indicates greater likelihood of the interface becoming a root. Set the priority only in increments of 16.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 1 vlan 10

(config)#interface eth1
(config-if)#bridge-group 1 vlan 10 path-cost 1000

(config-if)#no bridge-group 1 vlan 10 path-cost

(config)#interface eth1
(config-if)#bridge-group 1 vlan 10 priority 240

(config-if)#no bridge-group 1 vlan 10 priority
```


© 2021 IP Infusion Inc. Proprietary

bridge protocol rpvst+

Use this command to enable Rapid Per-VLAN Spanning Tree on a bridge.

Command Syntax

```
bridge <1-32> protocol rpvst+
```

Parameter

<1-32>	Bridge identifier.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 1 protocol rpvst+
```

bridge rapid-pervlan-spanning-tree

Use this command to enable Rapid Per-VLAN Spanning Tree (RPVST+) globally on a bridge.

Use the `no` form of this command to disable RPVST+ globally on a bridge.

Command Syntax

```
bridge <1-32> rapid-pervlan-spanning-tree enable
no bridge <1-32> rapid-pervlan-spanning-tree enable (bridge-blocked|bridge-
  forward|)
```

Parameters

`<1-32>`	Bridge identifier.
`bridge-blocked`	Put ports of the bridge in the blocked state (default).
`bridge-forward`	Put ports of the bridge in the forwarding state.

Default

By default, this feature is enabled.

For the `no` form of this command, `bridge-blocked` is the default.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 rapid-pervlan-spanning-tree enable

(config)#no bridge 1 rapid-pervlan-spanning-tree enable bridge-forward
```


© 2021 IP Infusion Inc. Proprietary

show spanning-tree rpvst+

Use this command to display RPVST information.

Command Syntax

```
show spanning-tree rpvst+
show spanning-tree rpvst+ config
show spanning-tree rpvst+ detail
show spanning-tree rpvst+ detail interface IFNAME
show spanning-tree rpvst+ interface IFNAME
show spanning-tree rpvst+ vlan <1-4094>
show spanning-tree rpvst+ vlan <1-4094> interface IFNAME
```

Parameters

`config`	Display configuration information.
`detail`	Display detailed information.
`IFNAME`	Display interface information.
`<1-4094>`	Display VLAN information

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following displays output of this command without any parameters.

```
#show spanning-tree rpvst+
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8001525400b092de
% 1: Bridge Id 8001525400b092de
% 1: last topology change Wed Mar 28 02:31:50 2018
% 1: 1 topology change(s)  - last topology change Wed Mar 28 02:31:50 2018

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 2
%   eth1: Designated Port Id 0x8003 - Priority 128  -
```

```
%   eth1: Root 8001525400b092de
%   eth1: Designated Bridge 8001525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 3 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%
%
%   Instance        VLAN
%   0:              1, 4-10
%   1:              2
%   2:              3
```

The following displays output of this command with the `config` parameter.

```
#show spanning-tree rpvst+ config
%
%  RPVST Configuration Information for bridge 1 :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : Default
%  Revision Level : 0
%  Digest         : 0xB41829F9030A054FB74EF7A8587FF58D
%-------------------------------------------------------

#show spanning-tree rpvst+ detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8001525400b092de
% 1: Bridge Id 8001525400b092de
% 1: last topology change Wed Mar 28 02:31:50 2018
% 1: 1 topology change(s)  - last topology change Wed Mar 28 02:31:50 2018

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 2
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 8001525400b092de
```

 © 2021 IP Infusion Inc. Proprietary

```
%   eth1: Designated Bridge 8001525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%

% Instance  1:  Vlans: 2
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b092de
%   eth1: Designated Bridge 8002525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b092de
% 1: Bridge Id 8002525400b092de
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b092de
%   eth1: Designated Bridge 8002525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%

%
#show spanning-tree rpvst+ vlan 2 interface eth1
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b092de
```

```
% 1: Bridge Id 8002525400b092de
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b092de
%   eth1: Designated Bridge 8002525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```


© 2021 IP Infusion Inc. Proprietary

spanning-tree rpvst+ configuration

Use this command to enter RPVST+ configuration mode after creating a bridge and adding a VLAN to that bridge.

Internally, an RSTP Instance is created for each configured VLAN.

Command Syntax

```
spanning-tree rpvst+ configuration
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#spanning-tree rpvst+ configuration
(config-rpvst+)#
```

spanning-tree vlan restricted-role

Use this command to restrict the role of the interface.

Use the `no` form of this command to not restrict the role of the interface.

Command Syntax

```
spanning-tree vlan <2-4094> restricted-role
no spanning-tree vlan <2-4094> restricted-role
```

Parameters

`<2-4094>`	VLAN identifier.

Default

The default is to not restrict the role of the interface

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree vlan 10 restricted-role
```


© 2021 IP Infusion Inc. Proprietary

spanning-tree vlan restricted-tcn

Use this command to restrict propagating topology change notifications (TCNs) from the interface.

Use the `no` form of this command to not restrict propagating TCNs from the interface.

Command Syntax

```
spanning-tree vlan <2-4094> restricted-tcn
no spanning-tree vlan <2-4094> restricted_tcn
```

Parameters

`<2-4094>`	VLAN identifier.

Default

The default is to not restrict propagating TCNs

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree vlan 10 restricted-tcn
(config-if)#no spanning-tree vlan 10 restricted_tcn
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 Link Aggregation Commands

This chapter describes the link aggregation commands.

- channel-group mode
- clear lacp
- debug lacp
- interface po
- interface sa
- lacp destination-mac
- lacp force-up
- lacp port-priority
- lacp system-priority
- lacp timeout
- port-channel load-balance
- port-channel min-bandwidth - dynamic LAG min-bandwidth
- port-channel min-links - dynamic LAG min-links
- port-channel min-bandwidth - static LAG min-bandwidth
- port-channel min-links - static LAG min-linksn
- show debugging lacp
- show etherchannel
- show lacp sys-id
- show lacp-counter
- show port etherchannel
- show static-channel-group
- show static-channel load-balance
- snmp restart lacp
- static-channel-group

© 2021 IP Infusion Inc. Proprietary

channel-group mode

Use this command to add an interface to an existing link aggregation group.

After you execute this command, the interface loses its properties and takes the properties of the aggregated interface.

Use the `no` parameter with this command to remove an interface from a dynamic link aggregation group. When you remove an interface from a LAG, the interface acquires the default interface properties.

Command Syntax

```
channel-group <1-16383> mode (active|passive)
no channel-group
```

Parameters

`<1-16383>`	Specify a channel group number (with DRNI).
`mode`	Specify a channel mode.
`active`	Enable LACP negotiation.
`passive`	Disable LACP negotiation.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#channel-group 1 mode active
(config-if)#exit

#sh run in po1
!
interface po1
 switchport
 port-channel load-balance src-dst-mac
```

The is an example of `no channel-group`:

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#no channel-group
(config-if)#exit

#sh run in xe1
!
interface xe1
!
#sh run in po1
!
```


© 2021 IP Infusion Inc. Proprietary

```
interface po1
 switchport
 port-channel load-balance src-dst-mac
!
```

clear lacp

Use this command to clear the counters of all LACP aggregators or a given LACP aggregator.

Command Syntax

```
clear lacp <1-16383> counters
clear lacp counters
```

Parameters

`<1-16383>`	Clears a channel-group number.

Command Mode

Exec mode and Pr<1-16383>ivileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear lacp 2 counters
```


© 2021 IP Infusion Inc. Proprietary

debug lacp

Use this command to enable LACP debugging.

Use the `no` parameter with this command to disable debugging.

Command Syntax

```
debug lacp (event|cli|timer|packet|sync|ha|all|rx|tx)
no debug lacp (event|cli|timer|packet|sync|ha|allrx|tx)
undebug all
```

Parameters

`all`	Enables all LACP debugging.
`cli`	Echo commands to console.
`event`	Sets the debug options for LACP events.
`ha`	Echo High availability events to console.
`packet`	Sets the debug option for LACP packets.
`sync`	Echo synchronization to console.
`timer`	Echo timer expiry to console.
`rx`	Echo receiving of lacpdus to console.
`tx`	Echo transmission of lacpdus to console.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug lacp all
```

© 2021 IP Infusion Inc. Proprietary

interface po

Use this command to create a dummy dynamic link aggregate interface (by default an L3 LAG interface).

Use the `no` form of this command to remove a dynamic link aggregate group and also it remove the properties of the po from all member ports.

Note: Switchport/routed mode needs to be set for the PO before adding member ports to it.

Command Syntax

```
interface po<1-16383>
no interface po<1-16383>
```

Parameters

`<1-16383>`	Channel group number

Default

By default, interface po is L3 LAG interface

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface po1
(config-if)#switchport
(config-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

interface sa

Use this command to create a dummy static link aggregate interface (by default an L3 LAG interface) and to add an interface to an existing static link aggregation group.

Use the `no` form of this command to remove a static link aggregate group and also remove the properties of the po from all member ports.

Command Syntax

```
interface sa<1-16383>
no interface sa<1-16383>
```

Parameters

`<1-16383>`	Channel group number.

Default

By default, interface sa is L3 LAG interface

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface sa1
(config-if)#switchport
(config-if)#exit
```

lacp destination-mac

Use this command to set the address type to use for sending LACPDUs (Link Aggregation Control Protocol Data Units).

Note: The interface must be an aggregation port.

Use the `no` form of this command to set the address type to its default (multicast group address).

Command Syntax

```
lacp destination-mac  (customer-bridge-group-address | multicast-group-address |
  non-tmpr-group-address)
no lacp destination-mac
```

Parameters

`customer-bridge-group-address`

Customer bridge group address

`multicast-group-address`

Multicast group address (default)

`non-TPMR-group-address`

Non-Two-Port Media Access Control Relay (TPMR) group address

Default

By default, lacp destination-mac is multicast-group-address

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#interface eth1
(config-if)#lacp destination-mac customer-bridge-group-address
```


© 2021 IP Infusion Inc. Proprietary

lacp force-up

Use this command to make a port immediately begin forwarding packets and not wait for an LACPDU. After you execute this command, the member port is forcefully up even if LACP is not in sync (only if no other member in the aggregator is in sync).

If a force-up port stops receiving LACPDUs, the port ignores the time-out and remains in operation.

This command can be configured on one member interface of a port channel.

Note: This command can only be given after executing the channel-group mode command on an interface. Force-up mode is not supported for LACP passive mode.

Note: For MC-LAG, only configure a force-up port on either on the master node or the slave node to prevent traffic drops/loops.

Use the `no` form of this command to disable force-up mode.

Command Syntax:

```
lacp force-up
```

```
no lacp force-up
```

Parameters

None

Default

By default, LACP force-up mode is disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#channel-group 1 mode active
(config-if)#lacp force-up
(config-if)#exit
```

lacp port-priority

Use this command to set the priority of a channel. Channels are selected for aggregation based on their priority with the higher priority (numerically lower) channels selected first.

Use the `no` parameter with this command to set the priority of port to the default value (32768).

Command Syntax

```
lacp port-priority <1-65535>
no lacp port-priority
```

Parameters

`<1-65535>`	Specify the LACP port priority.

Default

By default, lacp port priority is 32768

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#lacp port-priority 34
```


© 2021 IP Infusion Inc. Proprietary

lacp system-priority

Use this command to set the LACP system priority. This priority determines the system responsible for resolving conflicts in the choice of aggregation groups.

Note: A lower numerical value has a higher priority.

Use the `no` parameter with this command to set the system priority to its default value (32768).

Command Syntax

```
lacp system-priority <1-65535>
no lacp system-priority
```

Parameters

`<1-65535>`	System priority.

Default

By default, system priority is 32768

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#lacp system-priority 6700
```

lacp timeout

Use this command to set either a short or long timeout value on a port. The timeout value is the number of seconds before invalidating a received LACP data unit (DU).

Command Syntax

```
lacp timeout (short|long)
```

Parameters

`short`	LACP short timeout. 3 seconds.
`long`	LACP long timeout. 90 seconds.

Note: Short: With this mode, BPDU will be sent at Fast_Periodic_Time of 1 second interval. It will timeout, before invalidating received LACPDU, after 3xFast_Periodic_Time(3seconds),

Long: With this mode, BPDU will be sent at Slow_Periodic_Time of 30 seconds intervals. It will timeout, before invalidating received LACPDU, after 3xSlow_Periodic_Time(90seconds)

Default

By default, lacp timeout is long

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following sets the LACP short timeout on a port.

```
#configure terminal
(config)#interface eth0
(config-if)#lacp timeout short
```


© 2021 IP Infusion Inc. Proprietary

port-channel load-balance

Use this command to configure LACP port-channel load-balancing and set port-selection criteria (PSC) for an interface.

Use the `no` option with this command to remove the load-balancing configuration and unset PSC.

Command Syntax

```
port-channel load-balance (dst-mac|src-mac|src-dst-mac|dst-ip|src-ip|src-dst-
  ip|dst-port|src-port|src-dst-port|rtag7)
no port-channel load-balance
```

Parameters

`dst-ip`	Destination IP address-based load balancing.
`dst-mac`	Destination MAC address-based load balancing.
`dst-port`	Destination TCP/UDP address-based load balancing.
`src-dst-ip`	Source and Destination IP address-based load balancing.
`src-dst-mac`	Source and Destination MAC address-based load balancing.
`src-dst-port`	Source and Destination TCP/UDP address-based load balancing.
`src-ip`	Source IP address-based load balancing.
`src-mac`	Source MAC address-based load balancing.
`src-port`	Source port address-based load balancing.
`rtag7`	Hashing based on packet type. IP - IP/Layer4 header, L2 - Layer2 header packet.

Default

By default load balance is src-dst-ip for L3 port and src-dst-mac for L2 port.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel load-balance src-dst-mac
```

port-channel min-bandwidth - dynamic LAG min-bandwidth

Use this command to set the minimum number of aggregated bandwidth that need to be up in the LAG(PO) interface. When the minimum number of bandwidth are configured for a LAG(PO), if the active links bandwidth for that interface become less than the configured value, then the whole LAG(PO) is brought down. When the number of active links bandwidth become the same or more than the configured value, then the whole LAG is restored.

Use the no form of this command to remove the minimum number of aggregated bandwidth that need to be up in the LAG interface.

Note: The minimum number of aggregated bandwidth should be same across both ends of an aggregation interface. If not configured, then on one of the nodes the LAG port will be treated as up and on the other as down and traffic will be discarded.

Note: When a LAG port is moved to the down state because it does not have the minimum number of required bandwidth up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.

Note: The port-channel min-links - dynamic LAG min-links feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Command Syntax

```
port-channel min-bandwidth <1-1000>g
no port-channel min-bandwidth
```

Parameters

`<1-1000>g`	for 1 to 1000 gigabits/s

Default

By default, port channel min- bandwidth is disabled.

Command Mode

Interface mode

Applicability

This command was introduced from OcNOS version 1.3.8

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel min-bandwidth 10g
```


© 2021 IP Infusion Inc. Proprietary

port-channel min-links - dynamic LAG min-links

Use this command to set the minimum number of aggregated links that need to be up in the LAG(PO) interface. When the minimum number of links are configured for a LAG(PO), if the active links for that interface become less than the configured value, then the whole LAG(PO) is brought down. When the number of active links become the same or more than the configured value, then the whole LAG is restored.

Use the no form of this command to remove the minimum number of aggregated links that need to be up in the LAG interface.

Note: The minimum number of aggregated links should be same across both ends of an aggregation interface. If not configured, then on one of the nodes the LAG port will be treated as up and on the other as down and traffic will be discarded.

Note: When a LAG port is moved to the down state because it does not have the minimum number of required links up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.

Note: The show debugging lacp feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Command Syntax

```
port-channel min-links <2-32>
no port-channel min-links
```

Parameters

<2-32>	Minimum number of links

Default

By default, port channel min-link is disabled.

Command Mode

Interface mode

Applicability

This command was introduced from OcNOS version 1.3.8

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel min-links 10
(config-if)#exit
```

port-channel min-bandwidth - static LAG min-bandwidth

Use this command to set the minimum number of aggregated bandwidth that need to be up in the LAG(SA) interface. When the minimum number of bandwidth are configured for a LAG(SA), if the active links bandwidth for that interface become less than the configured value, then the whole LAG(SA) is brought down. When the number of active links bandwidth become the same or more than the configured value, then the whole LAG is restored.

Use the no form of this command to remove the minimum number of aggregated bandwidth that need to be up in the LAG interface.

Note: The minimum number of aggregated bandwidth should be same across both ends of an aggregation interface. If not configured, then on one of the nodes the LAG port will be treated as up and on the other as down and traffic will be discarded.

Note: When a LAG port is moved to the down state because it does not have the minimum number of required bandwidth up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.

Note: The port-channel min-links - static LAG min-links feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Command Syntax

```
port-channel min-bandwidth <1-1000>g
no port-channel min-bandwidth
```

Parameters

`<1-1000>g`	for 1 to 1000 gigabits/s

Default

By default, port channel min- bandwidth is disabled.

Command Mode

Interface mode

Applicability

This command was introduced from OcNOS version 1.3.8

Example

```
#configure terminal
(config)#interface sa1
(config-if)#port-channel min-bandwidth 10g
```


© 2021 IP Infusion Inc. Proprietary

port-channel min-links - static LAG min-links

Use this command to set the minimum number of aggregated links that need to be up in the LAG(SA) interface. When the minimum number of links are configured for a LAG(SA), if the active links for that interface become less than the configured value, then the whole LAG(SA) is brought down. When the number of active links become the same or more than the configured value, then the whole LAG is restored.

Use the no form of this command to remove the minimum number of aggregated links that need to be up in the LAG interface.

Note: The minimum number of aggregated links should be same across both ends of an aggregation interface. If not configured, then on one of the nodes the LAG port will be treated as up and on the other as down and traffic will be discarded.

Note: When a LAG port is moved to the down state because it does not have the minimum number of required links up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.

Note: The port-channel min-bandwidth - static LAG min-bandwidth feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Command Syntax

```
port-channel min-links <2-32>
no port-channel min-links
```

Parameters

<2-32>	Minimum number of links

Default

By default, port channel min-link is disabled.

Command Mode

Interface mode

Applicability

This command was introduced from OcNOS version 1.3.8

Example

```
#configure terminal
(config)#interface sa1
(config-if)#port-channel min-links 10
(config-if)#exit
```

show debugging lacp

Use this command to display the status of the debugging of the LACP system.

Command Syntax

```
show debugging lacp
```

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging lacp

LACP debugging status:
LACP timer debugging is on
```


© 2021 IP Infusion Inc. Proprietary

show etherchannel

Use this command to display information about link aggregation groups.

Command Syntax

```
show etherchannel
show etherchannel <1-16383>
```

With MLAG:

```
show etherchannel (<1-16383>|) detail
show etherchannel (<1-16383>|) load-balance
show etherchannel (<1-16383>|) summary
```

Without MLAG:

```
show etherchannel (<1-16383>|) detail
show etherchannel (<1-16383>|) load-balance
show etherchannel (<1-16383>|) summary
```

Parameters

`<1-16383>`	Specify channel-group number.
`detail`	Specify detailed etherchannel information.
`load-balance`	Specify load balancing.
`summary`	Specify Etherchannel summary information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show etherchannel summary
% Aggregator po1 185
% Aggregator Type: Layer3
% Admin Key: 0001 - Oper Key 0001
%   Link: eth3 (5) sync: 0
-------------------------------------
% Aggregator po4 186
% Admin Key: 0004 - Oper Key 0004
%   Link: eth2 (4) sync: 0
-------------------------------------
% Aggregator po5 187
% Admin Key: 0005 - Oper Key 0005
%   Link: eth1 (3) sync: 0


#show etherchannel detail
% Aggregator po1 185
```

```
% Aggregator Type: Layer3
%  Mac address: 08:00:27:36:f5:7d
%  Admin Key: 0001 - Oper Key 0001
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0001
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 0
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth3 (5) sync: 0
%  Collector max delay: 5
-------------------------------------------------
% Aggregator po4 186
%  Mac address: 08:00:27:76:0c:57
%  Admin Key: 0004 - Oper Key 0004
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0004
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth2 (4) sync: 0
%  Collector max delay: 5
-------------------------------------------------
% Aggregator po5 187
%  Mac address: 08:00:27:2f:d5:ae
%  Admin Key: 0005 - Oper Key 0005
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0005
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 0
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth1 (3) sync: 0
%  Collector max delay: 5
```

Table 5-99 explains the show command output fields.

Table 5-99: show etherchannel detail output

Field	Description
Aggregator	Link aggregators name and ID number.
Mac address	Unique MAC address for link identification.
Admin Key	LACP administrative key – automatically configured value on each port configured to use LACP.
Oper Key	LACP operator key on Partner – automatically configured value on each port configured to use LACP.
Actor LAG ID	LAG ID consisting of MAC address plus aggregator ID number for this Actor.
Receive link count	The number of link received from the peer LAG.
Transmit link count	The number of links contained transmitted to the peer LAG.
Individual	The individual physical network interfaces or ports contained in the LAG.
Ready	The number of links in the active state on this Actor.
Partner LAG ID	Partner LAG ID consisting of MAC address plus aggregator ID number.
Link	Interface and ID number of the link.

© 2021 IP Infusion Inc. Proprietary

Table 5-99: show etherchannel detail output (Continued)

Field	Description
sync	MAC address synchronization enables a MC-LAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.
Collector max delay	Maximum period of wait time between sending of two subsequent Ethernet frames on a link.

show lacp sys-id

Use this command to display the LACP system identifier and priority.

Command Syntax

```
show lacp sys-id
```

Parameters

`sys-id`	Display LACP system ID and priority

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lacp sys-id
% System 8000,00-0e-0c-83-37-27
```


© 2021 IP Infusion Inc. Proprietary

show lacp-counter

Use this command to display the packet traffic on all ports of all present LACP aggregators, or a given LACP aggregator.

Command Syntax

```
show lacp-counte
show lacp-counter <1-16383>
```

Parameters

<1-16383>	Channel-group number

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lacp-counter 555

Port      LACPDUs         Marker          Pckt err
        Sent    Recv    Sent    Recv    Sent    Recv
```

show port etherchannel

Use this command to display details about a PO and its members' interfaces or to display details of a single member interface of a PO.

Command Syntax

```
show port etherchannel IFNAME
```

Parameters

IFNAME	Interface name

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show port etherchannel ce29/1
LAG ID                        : 0x8000,cc-37-ab-a0-89-ca,0x0002
Partner oper LAG ID           : 0x8000,a8-2b-b5-38-1e-48,0x0004
Aggregator ID                 : 100002
  LACP link info              : ce29/1 - 10001
  Periodic Transmission
  machine state               : Slow periodic
  Receive machine state       : Current
  Mux machine state           : Collecting/Distributing
  Actor Info :
  ===========
  Actor Port priority         : 0x8000 (32768)
  Admin key                   : 0x0002 (2) Oper key: 0x0002 (2)
  Physical admin key          : (2)
  Actor Oper state            : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Actor Admin state           : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
  Partner Info:
  ============
  Partner oper port           : 10009
  Partner link info           : admin port 0
  Partner admin LAG ID        : 0x0000-00:00:00:00:0000
  Partner system priority     : admin:0x0000 - oper:0x8000
  Partner port priority       : admin:0x0000 - oper:0x8000
  Partner oper state          : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Partner admin state         : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0


#show port etherchannel po2
LAG ID                        : 0x8000,cc-37-ab-a0-89-ca,0x0002
Partner oper LAG ID           : 0x8000,a8-2b-b5-38-1e-48,0x0004
Aggregator ID                 : 100002
  LACP link info              : ce29/1 - 10001
  Periodic Transmission
  machine state               : Slow periodic
```


© 2021 IP Infusion Inc. Proprietary

```
Receive machine state      : Current
Mux machine state          : Collecting/Distributing
Actor Info :
===========
Actor Port priority        : 0x8000 (32768)
Admin key                  : 0x0002 (2) Oper key: 0x0002 (2)
Physical admin key         : (2)
Actor Oper state           : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Actor Admin state          : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
Partner Info:
============
Partner oper port          : 10009
Partner link info          : admin port 0
Partner admin LAG ID       : 0x0000-00:00:00:00:0000
Partner system priority    : admin:0x0000 - oper:0x8000
Partner port priority      : admin:0x0000 - oper:0x8000
Partner oper state         : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner admin state        : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0

LACP link info             : ce30/1 - 10005
Periodic Transmission
machine state              : Slow periodic
Receive machine state      : Current
Mux machine state          : Collecting/Distributing
Actor Info :
===========
Actor Port priority        : 0x8000 (32768)
Admin key                  : 0x0002 (2) Oper key: 0x0002 (2)
Physical admin key         : (2)
Actor Oper state           : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Actor Admin state          : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
Partner Info:
============
Partner oper port          : 10013
Partner link info          : admin port 0
Partner admin LAG ID       : 0x0000-00:00:00:00:0000
Partner system priority    : admin:0x0000 - oper:0x8000
Partner port priority      : admin:0x0000 - oper:0x8000
Partner oper state         : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner admin state        : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
```

Note: Most of the output of this command is duplicated in the show etherchannel command (see also the 802.3ad specificiation). The output of the `show port etherchannel` command is primarily a list of state machine values. An explanation of the state machine bits follows. See Figure 5-78.

Table 5-100 explains the show command output fields.

Table 5-100: show port etherchannel detailed output

Entry	Description
Actor/Partner state	The Actor's and Partner's state variables, encoded as individual bits within a single octet.
ACT	LACP_Activity is encoded in bit 0. Active LACP is encoded as a 1; Passive LACP as a 0.

Table 5-100: show port etherchannel detailed output (Continued)

Entry	Description
TIM	LACP_Timeout is encoded in bit 1. Short Timeout is encoded as a 1; Long Timeout as a 0.
AGG	Aggregability is encoded in bit 2. Aggregatable is encoded as a 1; Individual is encoded as a 0.
SYN	Synchronization is encoded in bit 3. In_Sync is encoded as a 1; Out_Of_Sync is encoded as a 0.
COL	Collecting is encoded in bit 4. True is encoded as a 1; False is encoded as a 0.
DIS	Distributing is encoded in bit 5. True is encoded as a 1; False is encoded as a 0.
DEF	Defaulted is encoded in bit 6.
EXP	Defaulted is encoded in bit 7.

Bits 7 and 8 are reserved; these are ignored on receipt and transmitted as zero. However, the received value of these bits is recorded on receipt to accurately reflect the actor's view of the partner's state in outgoing PDUs.

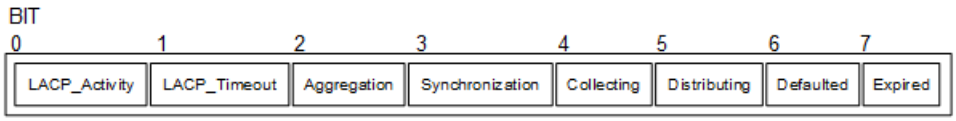


Figure 5-78: Diagram of state machine octet

© 2021 IP Infusion Inc. Proprietary

show static-channel-group

Use this command to display the types of load-balancing port selection criteria (PSC) used on configured static aggregators.

Command Syntax

```
show static-channel-group  (<1-16383>|)
```

Parameters

<1-16383>	Specify channel-group number.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is an example of the output of this command:

```
#show  static-channel-group 1
% Static Aggregator: sa1
% Member:
   eth1
```

show static-channel load-balance

Use this command to display information about static channel groups.

Command Syntax

```
show static-channel (<1-16383>|) load-balance
```

Parameters

<1-16383>	Specify static-channel-group number.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is an example of the output of this command:

```
#show static-channel load-balance
% Static Aggregator: sa5
Source and Destination Mac address
-----------------------------------------
% Static Aggregator: sa3
Source and Destination Mac address
-----------------------------------------
% Static Aggregator: sa1
Source and Destination Mac address

#show static-channel 1 load-balance
% Static Aggregator: sa1
Source and Destination Mac address
```


© 2021 IP Infusion Inc. Proprietary

snmp restart lacp

Use this command to restart SNMP in LACP.

Command Syntax

```
snmp restart lacp
```

Parameters

None

Default

By default, snmp restart lacp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#snmp restart lacp
```

static-channel-group

Use this command to create a static link aggregation group or to add an interface to an existing link aggregation group.

Use the `no` form of this command to remove an interface from a static link aggregation group without removing the static link aggregation group itself.

Command Syntax

```
static-channel-group <1-16383>
```

```
no static-channel-group
```

Parameter

`<1-16383>`	Channel group number.

Default

By default, static channel group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#static-channel-group 1
(config-if)#exit

#sh run in sa1
!
interface sa1
 switchport
 port-channel load-balance src-dst-mac
```

This is an example of `no static-channel-group`:

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#no static-channel-group
(config-if)#exit

#sh run in xe1
!
interface xe1
!
#sh run in sa1
!
interface sa1
 switchport
```


© 2021 IP Infusion Inc. Proprietary

```
 port-channel load-balance src-dst-mac
!
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 6 Multi-Chassis Link Aggregation Commands

This chapter describes the Multi-Chassis Link Aggregation commands.

Multi-Chassis Link Aggregation is also called MC-LAG, MLAG, or Distributed Resilient Network Interconnect (DRNI). In this document, it is called MC-LAG.

- clear mcec statistics
- debug mcec
- domain-address
- domain hello timeout
- domain priority
- domain-system-number
- intra-domain-link
- intra-domain-peer
- mcec domain configuration
- mlag
- mode
- show mcec statistics
- show mlag detail
- show mlag domain
- show mlag phy-digest
- show spanning-tree mlag operational-config
- show spanning-tree mlag sync-detail
- switchover type

© 2021 IP Infusion Inc. Proprietary

clear mcec statistics

Use this command to clear the statistics related to hello and information PDUs in the MCEC domain.

Command Syntax

```
clear mcec statistics
```

Parameters

None

Command Mode

Privileged exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#clear mcec statistics
```


© 2021 IP Infusion Inc. Proprietary

debug mcec

Use this command to view debugging logs for MC-LAG.

Use the `no` form of this command to remove debugging logs for MC-LAG.

Command Syntax

```
debug mcec (timer|event|hello|info|cli|mac-sync|all)
no debug mcec (timer|event|hello|info|cli|mac-sync|all)
```

Parameters

`all`	ALL
`cli`	CLI
`event`	Event
`hello`	Hello
`info`	Info
`mac-sync`	Mac Sync
`timer`	Timer

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug mcec all
#no debug mcec all
```

domain-address

Use this command to configure domain address, which helps to identify the mcec domain.

Use the `no` form of this command to remove the domain address.

Command Syntax

```
domain-address <domain-id>
no domain-address
```

Parameters

```
domain-id  domain address in HHHH.HHHH.HHHH format
```

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-address 1111.2222.3333
```


© 2021 IP Infusion Inc. Proprietary

domain hello timeout

Use this command to specify the domain hello-timeout value.

Command Syntax

```
domain-hello-timeout (long|short)
```

Parameters

`long`	Long Timeout
`short`	Short Timeout

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-hello-timeout long
```

domain priority

Use this command to specify the priority value associated with mcec domain.

Use the `no` form of this command to remove the priority value associated with mcec domain.

Command Syntax

```
domain-priority <1-65535>
no domain-priority
```

Parameters

`<1-65535>`	Priority Value

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-priority 2
```


© 2021 IP Infusion Inc. Proprietary

domain-system-number

Use this command to configure domain system number, which uniquely identifies domain system in mcec domain.

Use the `no` form of this command to configure domain system number.

Command Syntax

```
domain-system-number <1-2>
no domain-system-number
```

Parameters

`<1-2>`	Domain System Number

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-system-number 2
```

intra-domain-link

Use this command to map an interface as intra domain link that connects the domain system with its neighbor in a mcec domain.

Use the no form of this command to unmap the interface configured as intra domain link that connects the domain system with its neighbor in a mcec domain.

Command Syntax

```
intra-domain-link <IFNAME>
no intra-domain-link
```

Parameters

IFNAME	Interface name

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#intra-domain-link eth2
```


© 2021 IP Infusion Inc. Proprietary

intra-domain-peer

Use this command to map an interface as intra domain peer that connects the domain system with its neighbor in a mcec domain.

Use the `no` form of this command to unmap the interface configured as intra domain peer that connects the domain system with its neighbor in a mcec domain.

Command Syntax

```
intra-domain-peer A.B.C.D source-address A.B.C.D (vrf VRF_NAME|)
no intra-domain-peer
```

Parameters

`Peer Address`	Peer/Target IPv4 address
`A.B.C.D`	IPv4 address.
`Source Address`	Source IPv4 address
`A.B.C.D`	IPv4 address.
`vrf-IFNAME`	VRF Interface name

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS-SP version 3.0.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#intra-domain-peer 1.1.1.1 source-address 2.2.2.2 vrf
myvrf
```

mcec domain configuration

Use this command to enter MCEC Domain configuration mode to configure mcec domain information.

Command Syntax

```
mcec domain configuration
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#
```


© 2021 IP Infusion Inc. Proprietary

mlag

Use this command to map a port-channel to an MC-LAG instance.

Note: The MC-LAG port-channel (interface) must be created before mapping.

Note: All MC-LAG nodes must use the same MAC table size.

Use the `no` form of this command to un-map the port channel from the MC-LAG instance.

Command Syntax

```
mlag <1-255>
no mlag
```

Parameters

`<1-255>`	MC-LAG identifier

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3 and updated for static channel groups in OcNOS version 1.3.6.

Example

```
#config terminal
(config)#interface mlag1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport mode trunk allowed vlan all
(config-if)#exit
(config)#interface sa1
(config-if)#switchport
 (config-if)#mlag 1
(config-if)#exit

#configure terminal
(config)#interface sa1
(config-if)#no mlag
```

mode

Use this command to set the MC-LAG mode.

Use the no form of this command to turn off this feature.

Command Syntax

```
mode (active-active | active-standby)
no mode (active-active | active-standby)
```

Parameters

`active-active`	The interface is the active interface that carries the traffic
`active-standby`	The interface is ready to transition to the active state should a failure occur in the other node

Default

`active-active`

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#
(config)#interface mlag1
(config-if)#mode active-active

(config)#
(config)#interface mlag1
(config-if)#mode active-standby
```


© 2021 IP Infusion Inc. Proprietary

show mcec statistics

Use this command to display all the statistics related to hello and info pdu's in mcec domain.

Command Syntax

```
show mcec statistics
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh mcec statistics
Unknown MCCPDU received on the system : 0

-----------------------------------
IDP xe49
-----------------------------------
Valid RX Hello PDUs : 109
Valid TX Hello PDUs : 201
Valid RX Info PDUs: 23
Valid TX Info PDUs : 28
Valid RX Mac Sync PDUs : 5
Valid TX Mac Sync PDUs : 4
Valid RX Dhcps Sync PDUs : 2
Valid TX Dhcps Sync PDUs : 1


MLAG 1
Valid RX Info PDUs : 5
Valid TX Info PDUs : 7
```

Table 6-102 Shows the output details.

Table 6-101: Show mcec statistics details

Entry	Description
RX Hello PDUs	Total number of received hello PDUs.
TX Hello PDUs	Total number of transmitted hello PDUs.
RX Info PDUs	Total number of received Info PDUs.
TX Info PDUs	Total number of transmitted Info PDUs.

Table 6-101: Show mcec statistics details

Entry	Description
RX Mac Sync PDUs	Total number of received Mac Sync PDUs.
TX Mac Sync PDUs	Total number of transmitted Mac Sync PDUs.
RX Dhcps Sync PDUs	Total number of received Dhcps Sync PDUs
TX Dhcps Sync PDUs	Total number of transmitted Dhcps Sync PDUs

© 2021 IP Infusion Inc. Proprietary

show mlag detail

Use this command to display details about MC-LAG configuration and status.

Command Syntax

```
show mlag <1-255> detail
```

Parameters

<1-255>	MC-LAG group number

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3 and updated for static channel groups in OcNOS version 1.3.6.

Examples

```
#sh mlag 1 detail

MLAG-17
Mapped Aggregator : po1
Admin Key : 32769
Oper Key: 16385
Physical properties Digest : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

Neigh Admin Key: 16385
Neigh Physical Digest: dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
Info RCV State : Current
Info Periodic Time State : Standby
Mlag Sync                : IN_SYNC
Mode                     : Active
```

Table 6-102 Shows the output details.

Table 6-102: Show mlag output details

Entry	Description
Mapped Aggregator	Map the output of the aggregator in the interface which is active transformation.
Admin Key	Administrative key: automatically configured value on each port configured to use MC-LAG.
Oper Key	MLAG operator key on partner: automatically configured value on each port configured to use MC-LAG.
Physical properties Digest	Physical properties of the digest.
Neigh Admin Key	Neigh administrative key: automatically configured value on each port configured to use MC-LAG.

Table 6-102: Show mlag output details

Entry	Description
Neigh Physical Digest	Neighbor physical properties of the digest.
Info RCV State	Details of the RCV.
Info Periodic Time State	A simple state space formulation of a general digital periodic time series.
Mlag Sync	MAC address synchronization: enables a MC-LAG partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its partner’s.

© 2021 IP Infusion Inc. Proprietary

show mlag domain

Use this command to display MC-LAG configuration and status.

Command Syntax

```
show mlag domain (summary|details)
```

Parameters

summary	Summary
details	Details

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3 and updated for static channel groups in OcNOS version 1.3.6.

Examples

```
#show mlag domain summary

------------------------------------
Domain Configuration
------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : sa5
Domain Adjacency                : UP

------------------------------------
MLAG Configuration
------------------------------------

MLAG-1
  Mapped Aggregator             : sa1
  Physical properties Digest    : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57
cc
  Total Bandwidth               : 40g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active

MLAG-2
  Mapped Aggregator             : sa2
  Physical properties Digest    : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5
c8

  Total Bandwidth               : 40g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active
```

```
# show mlag domain details
-----------------------------------
Domain Configuration
-----------------------------------
Domain System Number           : 1
Domain Address                 : 1111.2222.3333
Domain Priority                : 32768
Intra Domain Interface         : sa5

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP
-----------------------------------
MLAG Configuration
-----------------------------------
MLAG-1
  Mapped Aggregator            : sa1
  Admin Key                    : 16385
  Oper Key                     : 16385
  Physical properties Digest   : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57
cc

  Neigh Admin Key              : 32769
  Neigh Physical Digest        : d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57
cc
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Total Bandwidth              : 40g
  Mlag Sync                    : IN_SYNC

MLAG-2
  Mapped Aggregator            : sa2
  Admin Key                    : 16386
  Oper Key                     : 16386
  Physical properties Digest   : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5
c8
  Neigh Admin Key              : 32770
  Neigh Physical Digest        : ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5
c8

  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Total Bandwidth              : 40g
  Mlag Sync                    : IN_SYNC
```

Table 6-103 Shows the output details.

Table 6-103: Show mlag summary details

Entry	Description
Domain System Number	Number to identify the node in domain.
Domain Address	Domain address for the MC-LAG domain.

© 2021 IP Infusion Inc. Proprietary

Table 6-103: Show mlag summary details

Entry	Description
Domain Priority	Domain priority for the MC-LAG domain.
Intra Domain Interface	Intra domain interface between MC-LAG domains.
Domain Adjacency	Domain adjacency details and configuration.
Physical properties Digest	physical properties of the digest algorithm.
Total Bandwidth	Total bandwidth available on the interface.
Domain System Number	Number of the domain system.
Domain Address	Domain address for the MC-LAG domain.
Domain Priority	Domain priority for the MC-LAG domain.
Intra Domain Interface	Details of the intra domain in the interface.
Hello RCV State	State of the hello RCV in the interface.
Hello Periodic Timer State	State of the hello periodic timer in the interface.
Domain Sync	Detail of the domain configuration synchronization.
Mapped Aggregator	Map the output of the aggregator in the interface which is active transformation.
Admin Key	Administrative key:automatically configured value on each port configured to use MC-LAG.
Oper Key	MLAG operator key on partner:automatically configured value on each port configured to use MC-LAG.
Physical properties Digest	Physical properties of the digest.
Neigh Admin Key	Neighbot administrative key: automatically configured value on each port configured to use MC-LAG.
Neigh Physical Digest	Neighbor physical properties of the digest.
Info RCV State	Details of the RCV.
Info Periodic Time State	A simple state space formulation of a general digital periodic time series.
Mlag Sync	MAC address synchronization: enables a MC-LAG partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its partner’s.

show mlag phy-digest

Use this command to display the physical interface properties considered for the physical digest.

Command Syntax

```
show mlag phy-digest
```

Parameters

None

Command Mode

Privilege exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#show mlag phy-digest

==========================================
mlag 1 mapped to interface po1
==========================================

Properties considered for physical digest

  mtu              : 1500
  duplex mode      : full
  hardware type    : 9
 port type    : L2(switchport)
 pvid      : 2000
  Native vlan id   : 0
  vlan port mode   : customer-edge

 stored digest  : 1 ef 71 4b 7f 37 5b 6a
          a5 8c e1 2f 95 9a fe cf
```


© 2021 IP Infusion Inc. Proprietary

show spanning-tree mlag operational-config

Use this command to display the operational information for MC-LAG.

Command Syntax

```
show spanning-tree mlag operational-config
```

Parameters

None

Command Mode

Privilege exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#show spanning-tree mlag operational-config
 Operational Configuration
----------------------------------------
 Bridge Priority       : 32768
 Pathcost method       : Long

 Interface             : mlag1
Pathcost       : 1000
 Priority              : 0
```

show spanning-tree mlag sync-detail

Use this command to display the spanning-tree properties shared with the domain peer node.

Command Syntax

```
show spanning-tree mlag sync-detail
```

Parameters

None

Command Mode

Privilege exec mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#show spanning-tree mlag sync-detail
 Domain Digest Parameters
----------------------------------------
 Max Age             : 20
 BPDU Filter         : Disabled
 BPDU Guard          : Disabled
 Hello time          : 2
 Forward Delay       : 15
 Force Version       : 2
 Err-disable status  : Disabled
 Err-disable timeout : 300
 MSTP Enabled        : Enabled
 MSTP Bridge Forward : Disabled

 Interface Digest parameters
----------------------------
  Port Name              : mlag1
  Admin Root Guard       : Disabled
 Admin Edge port    : Disabled
 Portfast configuration : Disabled
  Restricted TCN         : Disabled
  Admin BPDU filter      : Default
  Admin BPDU guard       : Default
```


© 2021 IP Infusion Inc. Proprietary

switchover type

Use this command to set the MC-LAG switchover type.

Use the `no` form of this command to turn off switchover.

Command Syntax

```
switchover type revertive <1-255>
switchover type non-revertive
no switchover type (revertive | non-revertive)
```

Parameters

`revertive`	If a failure happens that triggers a switchover, after failure recovery the initially-active node becomes active again
`<1-255>`	Switch back to the initially-active node this many seconds after failure recovery
`non-revertive`	Do not switch back to the initially-active node after failure recovery

Default

`revertive`	in 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#
(config)#interface mlag1
(config-if)#switchover type revertive 20

(config)#
(config)#interface mlag1
(config-if)#switchover type non-revertive
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 7 VLAN and Private VLAN Commands

This chapter has the commands used to manage VLANs and private VLANs.

- private-vlan association
- private-vlan community
- private-vlan isolated
- private-vlan primary
- show dtag vlan
- show vlan access-map
- show vlan
- show vlan brief
- show vlan classifier
- switchport access
- switchport hybrid
- switchport mode
- switchport mode access ingress-filter
- switchport mode hybrid acceptable-frame-type
- switchport mode hybrid ingress-filter
- switchport mode trunk ingress-filter
- switchport trunk allowed
- switchport trunk allowed vlan dtag
- switchport trunk native
- switchport mode private-vlan
- switchport private-vlan host-association
- switchport private-vlan mapping
- feature vlan classifier
- vlan classifier activate
- vlan classifier group
- vlan classifier rule ipv4
- vlan classifier rule mac
- vlan classifier rule proto
- vlan database
- vlan dtag
- vlan state
- vlan VLAN_RANGE bridge

© 2021 IP Infusion Inc. Proprietary

private-vlan association

Use this command to associate a secondary VLAN to a primary VLAN. Only one isolated VLAN can be associated to a primary VLAN. Multiple community VLANs can be associated to a primary VLAN.

Use the `no` form of this command to remove association of all the secondary VLANs to a primary VLAN.

Command Syntax

```
private-vlan association add VLAN_RANGE
private-vlan association remove VLAN_RANGE
no private-vlan association
```

Parameters

`add`	Add a VLAN to private VLAN list.
`remove`	Removes values associated with a single VLAN.
`VLAN_RANGE`	Specify VLAN ID 1-4094 or range(s): 1-5, 10 or 2-5,7-19 of the private VLANs to be configured

Default

By default, functionality is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan association add 3-4
(config-vlan)#private-vlan association remove 3-4
(config-vlan)#no private-vlan association
```


© 2021 IP Infusion Inc. Proprietary

private-vlan community

Use this command to set a VLAN type for a private (community) VLAN.

Use the `no` form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> community bridge <1-32>
no private-vlan <2-4094> bridge <1-32>
```

Parameters

`<2-4094>`	Specify a private VLAN identifier.
`bridge`	Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 4 community bridge 1
```

private-vlan isolated

Use this command to create an isolated private VLAN.

Use the `no` form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> isolated bridge <1-32>
no private-vlan <2-4094> bridge <1-32>
```

Parameters

`<2-4094>`	Specify a private VLAN identifier.
`bridge`	Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 3 isolated bridge 1
```


© 2021 IP Infusion Inc. Proprietary

private-vlan primary

Use this command to create a primary VLAN.

Use the `no` form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> primary bridge <1-32>
no private-vlan <2-4094> bridge <1-32>
```

Parameters

`<2-4094>`	Specify a private VLAN identifier.
`bridge`	Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 2 primary bridge 1
```

show dtag vlan

Use this command to display information about VLAN double tagging.

Command Syntax

```
show dtag vlan DTAG_VLAN_ID
```

Parameters

DTAG-VLAN-IDs	Outer-VLAN identifier and inner-VLAN identifier in the format 100.200, where 100 is the outer tag and 200 is the inner tag

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show dtag vlan 2000.3001
```

Table 7-104 explains the output.

Table 7-104: show dtag vlan output

Field	Description
Bridge	Bridge number
VLAN ID	VLAN identifier
Name	Double tag-VLAN identifers
State	VLAN state: ACTIVE, SUSPEND, or INVALID
H/W Status	Hardware status: UP or DOWN
Member ports	Interfaces that are part of the VLAN and whether untagged (u) or tagged (t)

© 2021 IP Infusion Inc. Proprietary

show vlan access-map

Use this command to display information for VLAN access maps.

Command Syntax

```
show vlan access-map
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vlan access-map
Vlan access-map myMap 10
       match ip: myMap
       action: drop
```

show vlan

Use this command to display information about static, dynamic or all VLANs.

Command Syntax

```
show vlan (all|static|dynamic|auto) bridge <1-32>
```

Parameters

`<1-32>`	Displays the bridge group ID.
`all`	Displays all VLANs (static and dynamic).
`static`	Displays static VLANs.
`dynamic`	Displays dynamic VLANs.
`auto`	Displays auto configured VLANs.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh vlan all bridge 1
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Up         xe2(u) xe10(u)
1       2       vlan2            ACTIVE  Up         xe10(t)
1       10      VLAN0010         ACTIVE  Up         xe2(t) xe10(t)
1       20      VLAN0020         ACTIVE  Up         xe2(t) xe10(t)
1       30      VLAN0030         ACTIVE  Up         xe10(t)
1       40      VLAN0040         ACTIVE  Up         xe10(t)
1       50      VLAN0050         ACTIVE  Up         xe10(t)
1       60      VLAN0060         ACTIVE  Up         xe10(t)
#
```

Table 7-105 Explains the show command output fields.

Table 7-105: show vlan output fields

Field	Description
Bridge	Number of bridge in the interface.
VLAN ID	VLAN identifier of the VLAN listed.
Name	Name of the VLAN.
State	Indicates whether the physical link is operational and can pass packets.

© 2021 IP Infusion Inc. Proprietary

Field	Description
H/W Status	Indicates that the hardware is operational.
Member ports	The tagged interfaces to which a VLAN is associated.

show vlan brief

Use this command to display brief VLAN information for all bridges.

Command Syntax

```
show vlan (brief | <2-4094>)
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from this command when using the `all` parameter.

```
#show vlan brief

Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
=============== ======= ================ ======= ==============================
1               1       default          ACTIVE  eth2(u)


0               1       default          ACTIVE
0               2       new              ACTIVE
```

Table 7-106 Explains the show command output fields.

Table 7-106: show vlan brief output fields

Field	Description
Bridge	Number of bridge in the interface.
VLAN ID	VLAN identifier of the VLAN listed.
Name	Name of the VLAN.
State	Indicates whether the physical link is operational and can pass packets.
H/W Status	Indicates that the hardware is operational.
Member ports	The tagged interfaces to which a VLAN is associated.

© 2021 IP Infusion Inc. Proprietary

show vlan classifier

Use this command to display information on configured VLAN classifier groups, interfaces configured for a VLAN group or all the groups, or all configured VLAN classifier rules.

If either a group ID or rule ID is not specified, all configured VLAN classifier rules are shown. If either a group ID or rule ID is specified, a specific configured VLAN classifier rule is shown.

Command Syntax

```
show vlan classifier group interface IFNAME
show vlan classifier group (<1-16>|)
show vlan classifier rule(<1-256>|)
```

Parameters

`group`	Displays group activated information.
`<1-16>`	Displays the group ID
`interface`	Displays interface information.
`interface`	Displays interface group information.
`group`	Displays group activated information.
`<1-16>`	Displays the group ID.
`rule`	Displays VLAN classifier rule ID.
`<1-256>`	Displays rule ID information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example displays groups for VLAN classifier groups:

```
#show vlan classifier group 1
vlan classifier group 1 add rule 1
```

This example displays interfaces for all VLAN classifier groups:

```
#show vlan classifier interface group
vlan classifier group 1 interface fe2
vlan classifier group 1 interface fe3
vlan classifier group 2 interface fe5
vlan classifier group 3 interface fe7
```

This example displays interfaces for VLAN classifier group 1:

```
#show vlan classifier interface group 1
vlan classifier group 1 interface fe2
vlan classifier group 1 interface fe3
```

This example displays interfaces for VLAN classifier rule 1:

```
#show vlan classifier rule 1
vlan classifier rule 1 mac 222.2222.2222 vlan 2
```


© 2021 IP Infusion Inc. Proprietary

switchport access

Use this command to change the default VLAN on the current interface.

Note: IP Infusion Inc. does not recommend using VLAN identifier 1 because of interoperability issues with other vendors' equipment.

Use the `no` parameter to remove an existing VLAN.

Command Syntax

```
switchport access vlan <2-4094>
no switchport access vlan
```

Parameter

`<2-4094>`	Specify the VLAN identifier.

Default

The switchport access vlan default value is 3968.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows the steps of a typical VLAN session, creating and destroying a VLAN.

```
#configure terminal
(config)#interface eth0
(config-if)#switchport access vlan 3

(config)#interface eth0
(config-if)#no switchport access vlan
```

switchport hybrid

Use this command to set the switching characteristics of the interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.

For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Use the `no` parameter to turn off allowed hybrid switching.

Command Syntax

```
switchport hybrid allowed vlan all
switchport hybrid vlan <2-4094>
switchport hybrid allowed vlan none
switchport hybrid allowed vlan except VLAN_ID
switchport hybrid allowed vlan remove VLAN_ID
switchport hybrid allowed vlan add VLAN_ID egress-tagged (enable|disable)
no switchport hybrid
no switchport hybrid vlan
```

Parameters

`all`	Allow all VLANs to transmit and receive through the interface.
`none`	Allow no VLANs to transmit and receive through the interface.
`except`	Allow all VLANs except these VLANs to transmit and receive through the interface.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`remove`	Remove these VLANs from the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`add`	Add these VLANs to the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`egress-tagged`	Whether to tag outgoing frames.
`enable`	Enable egress tagging for outgoing frames.
`disable`	Disable egress tagging for outgoing frames.

Default

By default, switchport hybrid is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

© 2021 IP Infusion Inc. Proprietary

Examples

The following shows adding a single VLAN to the member set.

```
(config-if)#switchport hybrid allowed vlan add eg
switchport hybrid allowed vlan add 2 egress-tagged enable
```

The following shows adding a range of VLANs to the member set.

```
(config-if)#switchport hybrid allowed vlan add eg
switchport hybrid allowed vlan add 2-4 egress-tagged enable
```

switchport mode

Use this command to set the switching characteristics of the Layer 2 interface.

Command Syntax

```
switchport mode (access|hybrid|trunk|provider-network|customer-edge
|customer-network|private-vlan)
```

Parameters

`access`	Access.
`hybrid`	Hybrid.
`trunk`	Trunk.
`provider-network`	Provider network.
`customer-network`	Customer network.

Default

By default, switchport hybrid is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode access
```


© 2021 IP Infusion Inc. Proprietary

switchport mode access ingress-filter

Use this command to set the switching characteristics of the interface to access mode, and classify untagged frames only. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode access ingress-filter (enable|disable)
```

Parameters

`ingress-filter`	Set the ingress filtering for the received frames.
`enable`	Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode access ingress-filter enable
```

switchport mode hybrid acceptable-frame-type

Use this command to set the interface acceptable frame types. This processing occurs after VLAN classification.

Use `no` form of this command to unconfigure the interface acceptable frames.

Command Syntax

```
switchport mode hybrid acceptable-frame-type (all|vlan-tagged)
no switchport hybrid
```

Parameters

`all`	Set all frames can be received
`vlan-tagged`	Accept only classified frames that belong to the port's member set.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/ trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode hybrid acceptable-frame-type vlan-tagged
```


© 2021 IP Infusion Inc. Proprietary

switchport mode hybrid ingress-filter

Use this command to set the switching characteristics of the interface as hybrid, and classify both tagged and untagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode hybrid ingress-filter (enable|disable)
```

Parameters

`enable`	Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode hybrid ingress-filter enable
```

switchport mode trunk ingress-filter

Use this command to set the switching characteristics of the interface as trunk, and specify only tagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode trunk ingress-filter (enable|disable)
```

Parameters

`ingress-filter`	Set the ingress filtering for the received frames.
`enable`	Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode trunk ingress-filter enable
```


© 2021 IP Infusion Inc. Proprietary

switchport trunk allowed

Use this command to set the switching characteristics of the interface to trunk.

For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Use the `no` parameter to remove all VLAN identifiers configured on this port.

Command Syntax

```
switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add VLAN_ID
switchport trunk allowed vlan except VLAN_ID
switchport trunk allowed vlan remove VLAN_ID
no switchport trunk
```

Parameters

`all`	Allow all VLANs to transmit and receive through the interface.
`none`	Allow no VLANs to transmit and receive through the interface.
`add`	Add these VLANs to the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`except`	All VLANs except these VLANs are part of the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`remove`	Remove these VLANs from the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following shows adding a single VLAN to the port's member set.

```
(config)#interface eth0
(config-if)#switchport trunk allowed vlan add 2
```

The following shows adding a range of VLANs to the port's member set.

```
(config)#interface eth0
(config-if)#switchport trunk allowed vlan add 2-4
```


© 2021 IP Infusion Inc. Proprietary

switchport trunk allowed vlan dtag

Use this command to maintain a mapping between the double-tagged logical interfaces with the physical interfaces for the purpose of enabling VLAN-translation on the port alone.

An example of when to use this command is in a GPON application, where an S-tag uniquely identifies an OLT channel partition and a C-tag uniquely identifies a subscriber/service on that channel partition.

Command Syntax

```
switchport trunk allowed vlan add dtag DTAG-VLAN-IDs
switchport trunk allowed vlan remove dtag DTAG-VLAN-IDs
```

Parameters

`add`	Add a mapping
`remove`	Remove a mapping
`DTAG-VLAN-IDs`	Outer-VLAN identifier and inner-VLAN identifier in the format 100.200, where 100 is the outer tag and 200 is the inner tag

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#int mlag1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan add 100,2000
(config-if)#switchport trunk allowed vlan add dtag 2000.3001
```

switchport trunk native

Use this command to configure native VLANs for this port. The native VLAN is used for classifying the incoming untagged packets.

Use the `no` parameter to revert the native VLAN to the default VLAN identifier 1.

Command Syntax

```
switchport trunk native vlan VLAN_ID
no switchport trunk native vlan
```

Parameter

`VLAN_ID`	VLAN identifier(s) <1-4094>. You can specify a single VLAN, or a VLAN list. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces in between the hyphens or commas.

Default

The default is that ingress filtering is off and all frame types are classified and accepted.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport trunk native vlan 2

(config)#interface eth0
(config-if)#no switchport trunk native vlan
```


© 2021 IP Infusion Inc. Proprietary

switchport mode private-vlan

Use this command to make a layer2 port as a host port or promiscuous port.

Use the `no` form of this command to remove the configuration.

Command Syntax

```
switchport mode private-vlan (host | promiscuous)
no switchport mode private-vlan (host | promiscuous)
```

Parameters

`host`	This port type can communicate with all other host ports assigned to the same community VLAN, but it cannot communicate with the ports in the same isolated VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN.
`promiscuous`	A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN

Default

By default, switchport mode private-vlan is host.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode private-vlan host
(config)#interface eth1
(config-if)#switchport mode private-vlan promiscuous
(config)#interface eth2
(config-if)#no switchport mode private-vlan promiscuous
```

switchport private-vlan host-association

Use this command to associate a primary VLAN and a secondary VLAN to a host port. Only one primary and secondary VLAN can be associated to a host port.

Use the `no` form of this command to remove the association.

Command Syntax

```
switchport private-vlan host-association <2-4094> add <2-4094>
no switchport private-vlan host-association
```

Parameters

`<2-4094>`	VLAN identifier of the primary VLAN.
`add`	Adds the secondary VLAN.
`<2-4094>`	VLAN identifier of the secondary VLAN (either isolated or community).

Default

By default, switchport mode private-vlan value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport private-vlan host-association 2 add 3

#configure terminal
(config)#interface eth0
(config-if)#no switchport private-vlan host-association
```


© 2021 IP Infusion Inc. Proprietary

switchport private-vlan mapping

Use this command to associate a primary VLAN and a set of secondary VLANs to a promiscuous port.

Use the `no` form of this to remove all the association of secondary VLANs to primary VLANs for a promiscuous port.

Command Syntax

```
switchport private-vlan mapping <2-4094> add VLAN_ID
switchport private-vlan mapping <2-4094> remove VLAN_ID
no switchport private-vlan mapping
```

Parameters

`<2-4094>`	VLAN identifier of the primary VLAN.
`add`	Adds the secondary VLAN.
`remove`	Removes the secondary VLAN.
`VLAN_ID`	VLAN identifier <2-4094> of the secondary VLAN (either isolated or community).

Default

By default, switchport mode private-vlan mapping value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport private-vlan mapping 2 add 3-4
(config-if)#switchport private-vlan mapping 2 remove 3-4

(config-if)#no switchport private-vlan mapping
```

feature vlan classifier

Use this command to enable the feature VLAN classifier.

Use `no` form of this command to disable the feature VLAN classifier.

Command Syntax

```
feature vlan classifier
no feature vlan classifier
```

Parameters

`classifier`	VLAN Classifier Service

Default

By default, feature vlan classifier is enable

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#feature vlan classifier
(config)#no feature vlan classifier
```


© 2021 IP Infusion Inc. Proprietary

vlan classifier activate

Use this command to activate the VLAN classifier.

Use no form of this command to deactivate the VLAN classifier.

Command Syntax

```
vlan classifier activate <1-16> vlan <2-4096>
no vlan classifier activate <1-16>
```

Parameters

<1-16>	Indicates the VLAN classifier activate identifier.
<2-4094>	VLAN identifier of the primary VLAN.

Default

By default, vlan classifier activate value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth2
(config-if)#vlan classifier activate 1 vlan 2

(config-if)#no vlan classifier activate 1
```

vlan classifier group

Use this command to create a subnet-based VLAN classifier group. A group indicates a VLAN classifier group ID.

Command Syntax

```
vlan classifier group <1-16> (add | delete) rule <1-256>
no vlan classifier group <1-16>
```

Parameters

`add`	Adds a rule to a group.
`delete`	Deletes a rule from a group.
`rule`	Indicates the VLAN classifier rule identifier `<1-256>`.

Default

By default, vlan classifier group value is 1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier group 1 delete rule 1
(config)#no vlan classifier group 2
```


© 2021 IP Infusion Inc. Proprietary

vlan classifier rule ipv4

Use this command to create a subnet-based VLAN classifier rule and map it to a specific VLAN. If the source IP address matches the IP subnet specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> ipv4 A.B.C.D/M
no vlan classifier rule <1-256>
```

Parameters

A.B.C.D/M	Indicates the IPv4 address classification. Enter the address in A.B.C.D/M format.

Default

By default, vlan classifier rule is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 ipv4 20.20.20.2/24
(config)#no vlan classifier rule 2
```

vlan classifier rule mac

Use this command to create a subnet-based VLAN classifier rule and map it to a specific VLAN.

If the source IP address matches the IP subnet specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> mac WORD
no vlan classifier rule <1-256>
```

Parameters

WORD	Indicate the Mac address classification. Enter the address in HHHH.HHHH.HHHH format.

Default

By default, vlan classifier rule value is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 mac fe80::22e::b5ff:fee8:6/64
(config)#no vlan classifier rule 2
```


© 2021 IP Infusion Inc. Proprietary

vlan classifier rule proto

Use this command to create a subnet-based VLAN classifier rule for a protocol and map it to a specific VLAN. If the source IP address matches the IP subnet specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> proto (ip|ipv6|ipx|x25|arp|rarp|atalkddp|atalkaarp|
  atmmulti|atmtransport|pppdiscovery|pppsession|xeroxpup|xeroxaddrtrans|g8bpqx25|
  ieeepup|ieeeaddrtrans|dec|decdnadumpload|decdnaremoteconsole|decdnarouting|
  declat|decdiagnostics|deccustom|decsyscomm|<0-65535>)
no vlan classifier rule <1-256>
```

Parameters

`<0-65535>`	Ethernet decimal
`arp`	Address Resolution Protocol
`atalkaarp`	Appletalk AARP
`atalkddp`	Appletalk DDP
`atmmulti`	MultiProtocol Over ATM
`atmtransport`	Frame-based ATM Transport
`dec`	DEC Assigned
`deccustom`	DEC Customer use
`decdiagnostics`	EC Diagnostics
`decdnadumpload`	DEC DNA Dump/Load
`decdnaremoteconsole`	DEC DNA Remote Console
`decdnarouting`	DEC DNA Routing
`declat`	DEC LAT
`decsyscomm`	DEC Systems Comms Arch
`g8bpqx25`	G8BPQ AX.25
`ieeeaddrtrans`	Xerox IEEE802.3 PUP Address Translation
`ieeepup`	Xerox IEEE802.3 PUP
`ip`	IP address
`ipv6`	IPv6 address
`ipx`	IPX address
`pppdiscovery`	PPPoE discovery
`pppsession`	PPPoE session
`rarp`	Reverse Address Resolution
`x25`	CCITT X.25
`xeroxaddrtrans`	Xerox PUP Address Translation
`xeroxpup`	Xerox PUP

`ethv2`	Ethernet v2
`nosnapllc`	Indicates LLC without snap encapsulation
`snapllc`	Indicates LLC snap encapsulation

Default

By default, vlan classifier rule value is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 proto ip
(config)#no vlan classifier rule 2
```


© 2021 IP Infusion Inc. Proprietary

vlan database

Use this command to enter the VLAN configuration mode to add, delete, or modify values associated with a single VLAN.

Command Syntax

```
vlan database
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, note the change to VLAN configuration mode from Configure mode:

```
#configure terminal
(config)#vlan database
(config-vlan)#
```

vlan dtag

Use this command to enable or disable double tagging packets with an outer-VLAN identifier and an inner-VLAN identifier.

An example of when to use this command is in a GPON application, where an S-tag uniquely identifies an OLT channel partition and a C-tag uniquely identifies a subscriber/service on that channel partition.

Use the `no` form of this command to not double tag packets.

Command Syntax

```
vlan dtag DTAG-VLAN-IDs bridge <1-32> state (enable|disable) subscriber
no vlan dtag DTAG-VLAN-IDs bridge <1-32>
```

Parameters

`DTAG-VLAN-IDs`	Outer-VLAN identifier and inner-VLAN identifier in the format 100.200, where 100 is the outer tag and 200 is the inner tag
`<1-32>`	Bridge number
`enable`	Enable double tagging
`disable`	Suspend double tagging

Default

No default value is specified

Command Mode

VLAN database mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#vlan database
(config-vlan)#vlan dtag 2000.3001 bridge 1 state enable subscriber
```


© 2021 IP Infusion Inc. Proprietary

vlan state

This command enables or disables the state of a particular VLAN on the bridge.

Command Syntax

```
vlan <2-4094> bridge <1-32> (state (enable|disable)|)
```

Parameters

`<1-32>`	Specify bridge group ID
`state`	Indicates the operational state of the VLAN
`enable`	Sets VLAN into a enable state.
`disable`	Sets VLAN into a disable state.
`name`	The VLAN name
`WORD`	The name of the VLAN

Default

By default, vlan bridge state is disabled.

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#vlan database
(config-vlan)#vlan 45 bridge 1 state enable
```

vlan VLAN_RANGE bridge

This command allows you to create a single/range of VLAN’s on the VLAN aware bridges.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE bridge <1-32>
vlan <2-4094> bridge <1-32> (state (enable|disable)|)
vlan VLAN_RANGE bridge <1-32> (name WORD|) state (enable | disable)
no vlan VLAN_RANGE bridge <1-32>
```

Parameters

`VLAN_RANGE`	The vlan-id or range of vlan-id's separated by ','&'-'
`bridge`	Specify the bridge group ID in the range <1-32>.
`state`	Indicates the operational state of the VLAN.
`enable`	Sets VLAN into an enable state.
`disable`	Sets VLAN into a disable state.

Default

By default, vlan bridge state is disabled

Command Mode

Configuration Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#vlan 3-40,56 bridge 4
(config)#no vlan 2-5 bridge 2
```


© 2021 IP Infusion Inc. Proprietary

vlan VLAN_RANGE type customer

This command allows you to create a single/range of VLAN’s on the VLAN customer aware.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE (type (customer)|) bridge <1-32> (name WORD|) (state
  (disable|enable)|)
no vlan VLAN_RANGE type (customer) bridge <1-32>
no vlan VLAN_RANGE bridge <1-32>
```

Parameters

VLAN_RANGE	The vlan-id or range of vlan-id's separated by ','&'-'
bridge	Specify the bridge group ID in the range <1-32>.
state	Indicates the operational state of the VLAN.
enable	Sets VLAN into an enable state.
disable	Sets VLAN into a disable state.
customer	

Default

By default, vlan customer state is disabled

Command Mode

Configuration Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#vlan type
(config)#no vlan type
```

vlan VLAN_RANGE type service

This command allows you to create a single/range of VLAN’s on the VLAN service.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE type service (point-point|multipoint-multipoint|rooted-multipoint)
  bridge <1-32> (state (disable|enable)|)
vlan VLAN_RANGE type service (point-point|multipoint-multipoint|rooted-multipoint)
  bridge <1-32> name WORD (state (disable|enable)|)
no vlan VLAN_RANGE type service bridge <1-32>
```

Parameters

VLAN_RANGE	The vlan-id or range of vlan-id's separated by ','&'-'
bridge	Specify the bridge group ID in the range <1-32>.
state	Indicates the operational state of the VLAN.
enable	Sets VLAN into an enable state.
disable	Sets VLAN into a disable state
service	

Default

By default, with the name WORD this can only be given in “vlan database” mode.

Command Mode

Configuration Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#vlan type
(config)#no vlan type
```


© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 8 802.1x Commands

This chapter provides a description, syntax, and examples of the 802.1X commands. It includes the following commands:

- auth-mac auth-fail-action
- auth-mac disable
- auth-mac dynamic-vlan-creation
- auth-mac enable
- auth-mac mac-aging
- auth-mac system-auth-ctrl
- debug dot1x
- dot1x initialize
- dot1x keytxenabled
- dot1x port-control
- dot1x protocol-version
- dot1x quiet-period
- dot1x reauthMax
- dot1x reauthentication
- dot1x system-auth-ctrl
- dot1x timeout re-authperiod
- dot1x timeout server-timeout
- dot1x timeout supp-timeout
- dot1x timeout tx-period
- ip radius source-interface
- radius-server dot1x deadtime
- radius-server dot1x host
- radius-server dot1x key
- radius-server dot1x retransmit
- radius-server dot1x timeout
- show debugging dot1x
- show dot1x
- snmp restart auth

© 2021 IP Infusion Inc. Proprietary

auth-mac auth-fail-action

Use this command to specify the required action after authentication fails for any source MAC (Media Access Control). If `drop-traffic` is specified, data destined to that MAC is dropped. The MAC will be added to the forwarding database in Discarded mode.

If `restrict-vlan` is specified, the unauthorized MAC is added to a restricted VLAN. The MAC will be added to the forwarding database in Forwarding mode.

Command Syntax

```
auth-mac auth-fail-action (restrict-vlan <2-4094>|drop-traffic)
```

Parameters

`drop-traffic`	Drops traffic destined to unauthorized source.
`restrict-vlan`	Adds unauthorized MAC address to restricted VLAN.
`<2-4094>`	Identity of the VLAN in the range of <2-4094>.

Default

drop-traffic

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac auth-fail-action restrict-vlan 12
```


© 2021 IP Infusion Inc. Proprietary

auth-mac disable

Use this command to disable MAC authentication on an interface. See the auth-mac enable command to enable MAC authentication on a interface.

Command Syntax

```
auth-mac disable
auth-mac disable mode (filter|shutdown)
```

Parameters

mode	Use this parameter to disable the MAC authentication mode on an interface.
filter	Filter the frames for the MAC when in an unauthorized state.
shutdown	Shut down the interface when the MAC is unauthenticated.

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac disable

#configure terminal
(config)#interface eth0
(config-if)#auth-mac disable mode filter

(config)#interface eth0
(config-if)#auth-mac disable mode shutdown
```

© 2021 IP Infusion Inc. Proprietary

auth-mac dynamic-vlan-creation

Use this command to enable or disable dynamic VLAN creation after successful MAC authentication.

Command Syntax

```
auth-mac dynamic-vlan-creation (enable|disable)
```

Parameters

`disable`	Disables dynamic VLAN creation: after a successful authentication, the MAC will be added to the forwarding database with the default VLAN
`enable`	Enables dynamic VLAN creation: after a successful authentication, the MAC under authentication will be added to the VLAN identifier attribute in the radius server configuration file

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac dynamic-vlan-creation disable

#configure terminal
(config)#interface eth0
(config-if)#auth-mac dynamic-vlan-creation enable
```


© 2021 IP Infusion Inc. Proprietary

auth-mac enable

Use this command to enable MAC authentication on an interface. See the auth-mac disable command to disable MAC authentication on an interface.

Command Syntax

```
auth-mac enable
auth-mac enable mode (filter|shutdown)
```

Parameters

mode	Use this parameter to enable the MAC authentication mode on an interface.
filter	Filter the frames for the MAC when in an unauthorized state.
shutdown	Shut down the interface when the MAC is unauthenticated.

Default

By default, MAC authentication is globally disabled on the device.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac enable

#configure terminal
(config)#interface eth0
(config-if)#auth-mac enable mode filter

(config)#interface eth0
(config-if)#auth-mac enable mode shutdown
```

© 2021 IP Infusion Inc. Proprietary

auth-mac mac-aging

Use this command to either enable or disable MAC aging. When enabled, a MAC entry is added to the forwarding database, with aging time equal to the bridge aging time. Otherwise, the MAC entry will not be aged out. If MAC aging is disabled, the MAC entry will not be aged out.

Command Syntax

```
auth-mac mac-aging (enable|disable)
```

Parameters

`disable`	Disables MAC aging.
`enable`	Enables MAC aging.

Default

Disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac mac-aging disable

#configure terminal
(config)#interface eth0
(config-if)#auth-mac mac-aging enable
```


© 2021 IP Infusion Inc. Proprietary

auth-mac system-auth-ctrl

Use this command to enable MAC authentication globally. If MAC authentication is not enabled, other MAC authentication related commands throw an error when issued.

Use the `no` parameter with this command to disable MAC authentication globally.

Command Syntax

```
auth-mac system-auth-ctrl
no auth-mac system-auth-ctrl
```

Parameters

None

Default

Authentication system messages are not displayed.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#auth-mac system-auth-ctrl

(config)#no auth-mac system-auth-ctrl
```

debug dot1x

Use this command to turn on or turn off 802.1x debugging at various levels.

Use the `no` parameter with this command or the `undebug` command to turn off debugging.

Command Syntax

```
debug dot1x (all|)
debug dot1x event
debug dot1x nsm
debug dot1x packet
debug dot1x timer
no debug dot1x (all|)
no debug dot1x event
no debug dot1x nsm
no debug dot1x packet
no debug dot1x timer
undebug dot1x (all|)
undebug dot1x event
undebug dot1x packet
undebug dot1x nsm
undebug dot1x timer
```

Parameters

`all`	Sets debugging for all 802.1x levels.
`event`	Sets debugging for 802.1x events.
`nsm`	Sets debugging for 802.1x NSM information.
`packet`	Sets debugging for 802.1x packets.
`timer`	Sets debugging for 802.1x timer.

Default

No default value is specified.

Command Mode

Exec, Privileged Exec, and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug dot1x all
(config)#debug dot1x event
```


© 2021 IP Infusion Inc. Proprietary

dot1x initialize

Use this command to unauthorize a port, and attempt reauthentication on the specified interface.

Command Syntax

```
dot1x initialize interface IFNAME
```

Parameters

`interface`	Interface name.

Default

No default value is specified.

Command Mode

Privileged Exec

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#dot1x initialize interface eth0
```

dot1x keytxenabled

Use this command to enable or disable key transmission over an Extensible Authentication Protocol (EAP) packet between the authenticator and supplicant.

Command Syntax

```
dot1x keytxenabled (enable|disable)
```

Parameters

`disable`	Disables the key transmission.
`enable`	Enables the key transmission.

Default

The dot1x keytxenabled default is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if) #dot1x keytxenabled disable

#configure terminal
(config)#interface eth0
(config-if) #dot1x keytxenabled enable
```


© 2021 IP Infusion Inc. Proprietary

dot1x port-control

Use this command to force a port state.

Use the `no` parameter with this command to remove a port from the 802.1x management.

Command Syntax

```
dot1x port-control dir (in|both)
dot1x port-control (force-unauthorized|force-authorized|auto)
no dot1x port-control
```

Parameters

`auto`	Specify to enable authentication on port.
`dir`	Specify the packet control direction.
`both`	Discard receive and transmit packets from the supplicant
`in`	Discard receive packets from the supplicant
`force-authorized`	Specify to force a port to always be in an authorized state.
`force-unauthorized`	Specify to force a port to always be in an unauthorized state.

Default

The dot1x port-control default is active.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x port-control auto

(config)#interface eth0
(config-if)#no dot1x port-control
```

dot1x protocol-version

Use this command to set the protocol version of dot1x to 1 or 2. The protocol version must be synchronized with the Xsupplicant being used in that interface.

Use the `no` parameter with this command to set the protocol version to the default value (2).

Command Syntax

```
dot1x protocol-version <1-2>
no dot1x protocol-version
```

Parameters

`<1-2>`	Indicates the EAP Over LAN (EAPOL) version.

Default

The default dot1x protocol version is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x protocol-version 2

(config)#interface eth0
(config-if)#no dot1x protocol-version
```


© 2021 IP Infusion Inc. Proprietary

dot1x quiet-period

Use this command to set the quiet-period time interval.

When a switch cannot authenticate a client, the switch remains idle for a quiet-period interval of time, then tries again. By administratively changing the quiet-period interval, by entering a lower number than the default, a faster response time can be provided.

Use the `no` parameter with this command to set the configured quiet period to the default (60 seconds).

Command Syntax

```
dot1x quiet-period <1-65535>
no dot1x quiet-period
```

Parameter

`<1-65535>`	Seconds between the retrial of authentication.

Default

The default dot1x protocol version is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x quiet-period 200
```

dot1x reauthMax

Use this command to set the maximum reauthentication value, which sets the maximum number of reauthentication attempts after which the port will be unauthorized.

Use the `no` parameter with this command to set the reauthentication maximum to the default value (2).

Command Syntax

```
dot1x reauthMax <1-10>
no dot1x reauthMax
```

Parameter

`<1-10>`	Indicates the maximum number of reauthentication attempts after which the port will be unauthorized.

Default

The default is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following sets the maximum reauthentication value to 5.

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x reauthMax 5
```

The following sets the reauthentication maximum to the default value.

```
#configure terminal
(config)#interface eth0
(config-if)#no dot1x reauthMax
```


© 2021 IP Infusion Inc. Proprietary

dot1x reauthentication

Use this command to enable reauthentication on a port.

Use the `no` parameter to disable reauthentication on a port.

Command Syntax

```
dot1x reauthentication
no dot1x reauthentication
```

Parameters

None

Default

The dot1x reauthentication default is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x reauthentication
```

dot1x system-auth-ctrl

Use this command to enable globally authentication.

Use the `no` parameter to disable globally authentication.

Command Syntax

```
dot1x system-auth-ctrl
no dot1x system-auth-ctrl
```

Parameters

None

Default

Authentication is off by default.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#dot1x system-auth-ctrl
```


© 2021 IP Infusion Inc. Proprietary

dot1x timeout re-authperiod

Use this command to set the interval between reauthorization attempts.

Use the `no` parameter to disable the interval between reauthorization attempts.

Command Syntax

```
dot1x timeout re-authperiod <1-4294967295>
no dot1x timeout re-authperiod
```

Parameter

`<1-4294967295>` Specify the seconds between reauthorization attempts.

Default

Default time is 3600 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout re-authperiod 25
```

dot1x timeout server-timeout

Use this command to set the authentication sever response timeout.

Use the `no` parameter to disable the authentication sever response timeout.

Command Syntax

```
dot1x timeout server-timeout <1-65535>
no dot1x timeout server-timeout
```

Parameter

`<1-65535>`	Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout server-timeout 555

(config)#interface eth0
(config-if)#no dot1x timeout server-timeout
```


© 2021 IP Infusion Inc. Proprietary

dot1x timeout supp-timeout

Use this command to set the interval for a supplicant to respond.

Use the `no` parameter to disable the authentication sever response timeout.

Command Syntax

```
dot1x timeout supp-timeout <1-65535>
no dot1x timeout supp-timeout
```

Parameter

`<1-65535>`	Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout supp-timeout 40

(config)#interface eth0
(config-if)#no dot1x timeout supp-timeout
```

dot1x timeout tx-period

Use this command to set the interval between successive attempts to request an ID.

Use the `no` parameter to disable the interval between successive attempts to request an ID.

Command Syntax

```
dot1x timeout tx-period <1-65535>
no dot1x timeout tx-period
```

Parameter

`<1-65535>`	Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout tx-period 34

(config)#interface eth0
(config-if)#no dot1x timeout tx-period
```


© 2021 IP Infusion Inc. Proprietary

ip radius source-interface

Use this command to set the local address sent in packets to the radius server.

Use the `no` parameter to clear the local address.

Command Syntax

```
ip radius source-interface HOSTNAME PORT
no ip radius source-interface
```

Parameters

`HOSTNAME`	Specify the radius client in the dotted IP address, or in the hostname format.
`PORT`	Specify the radius client port number. The default port number is 1812.

Default

The default port number is 1812.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip radius source-interface myhost 1812

(config)#no ip radius source-interface
```

radius-server dot1x deadtime

Use this command to specify the number of minutes a radius server, which is not responding to authentication requests, is passed over by requests for radius authentication. To improve radius response times when some servers might be unavailable, use this command to cause the unavailable servers to be skipped immediately.

Use the `no` form of this command to set deadtime to the default value of 0.

Command Syntax

```
radius-server dot1x deadtime MIN
no radius-server dot1x deadtime
```

Parameter

`dot1x`	IEEE 802.1X Port-Based Access Control.
`MIN`	Length of time (in minutes) that a radius server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours). Enter a value in the range 1 to 1440.

Default

Deadtime is set to 0

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server dot1x deadtime 10

(config)#no radius-server dot1x deadtime
```


© 2021 IP Infusion Inc. Proprietary

radius-server dot1x host

Use this command to specify the IP address or host name of the remote radius server host and assign authentication and accounting destination port numbers. Multiple radius-server host commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified. If no host-specific timeout, retransmit, or key values are specified, the global values apply to that host.

If the auth-port parameter is not specified, it will take the default value of the auth-port. If you do not specify the auth-port to unconfigure, and the default value of the auth-port does not match the port you are trying to unconfigure, the specified radius-server host will not be unconfigured.

Use the `no` form of the command to unconfigure a specified radius-server.

Command Syntax

```
radius-server dot1x host (A.B.C.D|HOSTNAME|X:X::X:X)(|(key ((0 WORD) | (7 WORD) |
  (WORD))(|(auth-port <0-65535> (|(timeout <1-60> (|(retransmit <1-100>)))))))
no radius-server dot1x host (A.B.C.D|HOSTNAME|X:X::X:X)(|(key ((0 WORD) | (7 WORD)
  | (WORD))(|(auth-port <0-65535> (|(timeout (|(retransmit <1-100>)))))))
```

Parameters

`dot1x`	IEEE 802.1X Port-Based Access Control.
`A.B.C.D`	IPv4 address of the RADIUS server.
`HOSTNAME`	Host name or DNS name of the RADIUS server.
`X:X::X:X`	IPv6 address of the RADIUS server.
`auth-port`	RADIUS server's port for authentication.
`key`	Specify the global shared key.
`retransmit`	Global RADIUS server retransmit count.
`timeout`	Specify the RADIUS server timeout(default: 5 seconds).
`0`	To specify shared key in clear-text form.
`7`	To specify shared key in encrypted form.
`WORD`	RADIUS shared secret(clear text) (Max Size 63).
`<0-65535>`	Port number.
`<0-100>`	Global RADIUS server retransmit count.
`<1-60>`	RADIUS server timeout period in seconds.

Default

The default value of auth-port is 1645.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server dot1x host hostname auth-port 1233 timeout 1 retransmit
2

(config)#no radius-server dot1x host hostname auth-port 1233
```


© 2021 IP Infusion Inc. Proprietary

radius-server dot1x key

Use this command to set the shared secret key between a Radius server and a client.

Use the `no` form of the command to undo this configuration.

Command Syntax

```
radius-server dot1x key ((0 WORD) | (7 WORD) | (WORD))
no radius-server dot1x key ((0 WORD) | (7 WORD) | (WORD))
```

Parameter

`dot1x`	IEEE 802.1X Port-Based Access Control.
`0`	To specify shared key in clear-text form.
`7`	To specify shared key in encrypted form.
`WORD`	Shared secret among radius server and 802.1X client (Max Size 63).

Default

No default value is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server dot1x key 0 abcd

#configure terminal
(config)#no radius-server dot1x 0 abcd
```

radius-server dot1x retransmit

Use this command to specify the number of times the router transmits each radius request to the server before giving up.

Use the `no` form of this command to disable retransmission.

Command Syntax

```
radius-server dot1x retransmit RETRIES
no radius-server dot1x retransmit
```

Parameter

`dot1x`	IEEE 802.1X Port-Based Access Control.
`RETRIES`	Specify the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.

Default

The default value is 3.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server dot1x retransmit 12

(config)#no radius-server dot1x retransmit
```


© 2021 IP Infusion Inc. Proprietary

radius-server dot1x timeout

Use this command to specify the number of seconds a router waits for a reply to a radius request before retransmitting the request.

Use the `no` parameter to use the default value.

Command Syntax

```
radius-server dot1x timeout <1-60>
no radius-server dot1x timeout
```

Parameter

`dot1x`	IEEE 802.1X Port-Based Access Control.
`<1-60>`	RADIUS server timeout period in seconds.

Default

The default value is 5 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server dot1x timeout 20

#configure terminal
(config)#no radius-server dot1x timeout
```

show debugging dot1x

Use this command to display the status of the debugging of the 802.1x system.

Command Syntax

```
show debugging dot1x
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging dot1x
802.1X debugging status:
```


© 2021 IP Infusion Inc. Proprietary

show dot1x

Use this command to display IEEE 802.1x port-based access control information.

Command Syntax

```
show dot1x
show dot1x all
show dot1x diagnostics interface IFNAME
show dot1x interface IFNAME
show dot1x sessionstatistics interface IFNAME
show dot1x statistics interface IFNAME
```

Parameters

`all`	Display all IEEE 802.1x port-based access control information.
`diagnostics`	Display diagnostics information.
`IFNAME`	Interface name.
`sessionstatistics`	Display the statistics for a session.
`statistics`	Display the statistics.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is an output of this command displaying the state of the system.

```
#show dot1x
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.mySite.com.12103
% Next radius message id: 0
```

The following is an output of this command displaying detailed information for all ports.

```
#show dot1x all
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.mySite.com.12103
% Next radius message id: 0
% Dot1x info for interface eth1 - 3
%  portEnabled: true - portControl: auto
%  portStatus: unauthorized - currentId: 11
%  reAuthenticate: disabled
%  abort:F fail:F start:F timeout:F success:F
%  PAE: state: connecting - portMode: auto
%  PAE: reAuthCount: 2 - rxRespId: 0
```

```
%  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
%  BE: state: idle - reqCount: 0 - idFromServer: 0
%  BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2
%  CD: adminControlledDirections: in - operControlledDirections: in
%  CD: bridgeDetected: false
%  KR: rxKey: false
%  KT: keyAvailable: false - keyTxEnabled: false
```

The following tables describes the output of the `show dot1x` command.

Table 8-107: Port variables

Entry	Description
portEnabled	Interface operational status (Up-true/down-false)
portControl	Current control status of the port for 802.1x control
portStatus	802.1x status of the port (authorized/unauthorized)
reAuthenticate	Reauthentication enabled/disabled status on port
reAuthPeriod	Reauthentication period

Table 8-108: Supplicant PAE related global variables

Entry	Description
abort	Abort authentication when true
fail	Failed authentication attempt when false
start	Start authentication when true
timeout	Authentication attempt timed out when true
success	Authentication successful when true

Table 8-109: 802.1x Operational state of interface

Entry	Description
mode	Configured 802.1x mode
reAuthCount	Reauthentication count
quietperiod	Time between reauthentication attempts
reAuthMax	Maximum reauthentication attempts

© 2021 IP Infusion Inc. Proprietary

Table 8-110: Backend authentication state machine variables and constants

Entry	Description
state	State of the port.
reqCount	Number of requests sent to server
suppTimeout	Number of seconds the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request.
serverTimeout	Number of seconds the port waits for a reply when relaying a response from the supplicant to the authentication server before timing out.
maxReq	Maximum number of times a request packet is retransmitted to the supplicant before the authentication session times out.

Table 8-111: Controlled directions state machine

Entry	Description
adminControlledDirections	Administrative value (Both/In)
operControlledDirections	Operational Value (Both/In)

Table 8-112: KR -- Key receive state machine

Entry	Description
rxKey	True when EAPOL-Key message is received by supplicant or authenticator. false when key is transmitted

Table 8-113: Key Transmit state machine

Entry	Description
keyAvailable	False when key has been transmitted by authenticator, true when new key is available for key exchange
keyTxEnabled	Key transmission enabled/disabled status

snmp restart auth

Use this command to restart SNMP in Authentication

Command Syntax

```
snmp restart auth
```

Parameters

None

Default

No default value is specified.

Default

The default port is UDP 162.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart auth
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 9 Link Layer Discovery Protocol Commands

This chapter describes the Link Layer Discovery Protocol (LLDP) commands.

- lldp debug
- lldp ip
- lldp run
- lldp tlv
- lldp tlv-select
- set lldp chassis-id-tlv
- set lldp disable
- set lldp enable
- set lldp locally-assigned
- set lldp management-address-tlv
- set lldp msg-tx-hold
- set lldp system-description
- set lldp system-name
- set lldp timer
- set lldp too-many-neighbors
- show lldp
- snmp restart lldp

© 2021 IP Infusion Inc. Proprietary

lldp debug

Use this command to turn on debugging functions for LLDP.

Use the `no` form of this command to turn off LLDP debugging functions

Command Syntax

```
lldp debug (event|rx|tx|message)
no lldp debug (event|rx|tx|message)
```

Parameters

`event`	Event debugging
`message`	NSM message debugging
`rx`	RX debugging
`tx`	TX debugging

Command Mode

Exec mode and Privileged Exec mode

Examples

```
#lldp debug event
#lldp debug messages
```


© 2021 IP Infusion Inc. Proprietary

lldp ip

Use this command to set the Link Layer Discovery Protocol with an IP address to be used as a chassis and management ID.

Use the `no` form of this command to remove this value.

Command Syntax

```
lldp ip address A.B.C.D
no lldp ip address
```

Parameters

`A.B.C.D`	Enter the IP address value

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#lldp ip address 1.1.1.1
(config)#no lldp ip address
```

lldp run

Use this command to start the Link Layer Discovery Protocol (LLDP).

Use the `no` form of this command to stop LLDP.

Command Syntax

```
lldp run
```

```
no lldp run
```

Parameters

None

Command Mode

Configure mode

Example

```
#configure terminal
(config)#lldp run

(config)#no lldp run
```


© 2021 IP Infusion Inc. Proprietary

lldp tlv

Use this command to set the TLVs enabled for transmission on a port. Make sure that the complete set of Type Length Values (TLVs) is specified when giving this command, because TLVs not specified are disabled.

Command Syntax

```
lldp tlv {chassis-id|port-id|ttl|port-description|system-name|system-
  description|system-capabilities|management-address|ieee-8021-org-specific|ieee-
  8023-org-specific}
```

Parameters

`chassis-id`	Chassis ID type length values (TLV)
`port-id`	Port ID TLV
`ttl`	Time to live TLV
`port-description`	Port description TLV
`system-name`	System name TLV
`system-description`	System Description
`system-capabilities`	System capabilities TLV
`management-address`	Management address TLV
`ieee-8021-org-specific`	IEEE 802.1 organizationally-specific TLV
`ieee-8023-org-specific`	IEEE 802.3 organizationally-specific TLV

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#lldp tlv chassis-id ieee-8021-org-specific ieee-8023-org-specific
management-address port-description port-id system-capabilities system-
description system-name ttl
```

lldp tlv-select

Use this command to configure interface LLDP parameters.

This command can be executed globally for all ports (configure mode) or locally for a specific port (interface mode).

When you give this command globally on all ports:

- The `show running-config` command only displays the options in global mode.
- A global configuration overrides an interface-level configuration. For example, if you disable an option on an interface, it is enabled after enabling the same option globally. If the option was enabled previously, the show output is suppressed and only global mode is displayed (to avoid duplicating the same configuration).
- After enabling a global configuration, when a new LLDP agent is configured on a port, it inherits the global TLV configuration. However, show output does not appear per interface/agent.
- After enabling globally, if you disable an option on an interface, the "no" form for this command is shown for that interface.
- Enabling an already enabled option causes an error.

If you disable globally on all ports:

- The option is removed globally, as well as overrides configurations for all interfaces.
- If the option was not enabled globally, it causes an error.

When enabled locally on a port:

- If the same option was enabled globally, it causes an error.
- If not already enabled, the option is enabled for the given interface alone.

When disabled locally on a port:

- If the option was not present locally or globally, it causes an error.
- If the option was enabled globally, the option is removed from this interface alone. No command will be displayed in show output.

Use the *no* form of this command to remove interface LLDP parameter configurations.

Command Syntax

```
lldp tlv-select (port-description|system-name| system-description|system-
  capabilities|management-address| ieee-8021-org-specific | ieee-8023-org-specific)
no lldp tlv-select (port-description|system-name|system-description|system-
  capabilities|management-address|ieee-8021-org-specific | ieee-8023-org-specific)
```

Parameters

`port-description`
: Port description TLV

`system-name`
: System name TLV

`system-description`
: System Description

`system-capabilities`
: System capabilities TLV

`management-address`

© 2021 IP Infusion Inc. Proprietary

Management address TLV

`ieee-8021-org-specific`

IEEE 802.1 organizationally-specific TLV

`ieee-8023-org-specific`

IEEE 802.3 organizationally-specific TLV

Command Mode

Configure mode and interface mode

Example

```
#configure terminal
(config)#lldp tlv-select system-capabilities

#configure terminal
(config)#interface eth2
(config-if)#lldp-agent
(config-if-lldp-agent)#lldp tlv-select system-capabilities
```

set lldp chassis-id-tlv

Use this command to set the chassis ID subtype for the LLDP agent on a port.

Command Syntax

```
set lldp chassis-id-tlv (mac-address | ip-address)
```

Parameters

`mac-address`	Use the MAC address as the chassis ID
`ip-address`	Use the management IP address as the chassis ID

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp chassis-id-tlv ip-address
```


© 2021 IP Infusion Inc. Proprietary

set lldp disable

Use this command to disable the LLDP agent on a port.

Command Syntax

```
set lldp disable
```

Parameters

None

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp disable
```

set lldp enable

Use this command to enable an LLDP agent on a port and specify its type.

Command Syntax

```
set lldp enable (txonly|txrx|rxonly)
```

Parameters

`rxonly`	Receive-only
`txonly`	Transmit-only
`txrx`	Transmit and receive

Default

By default, no LLDP agent is enabled for a port.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp enable txrx
```


© 2021 IP Infusion Inc. Proprietary

set lldp locally-assigned

Use this command to locally set the LLDP port identifier.

Command Syntax

```
set lldp locally-assigned NAME
```

Parameters

NAME	Name of the port.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp locally-assigned port1
```

set lldp management-address-tlv

Use this command to set the management address subtype for the LLDP agent on a port.

Command Syntax

```
set lldp management-address-tlv (mac-address | ip-address)
```

Parameters

`mac-address`	Use the MAC address as the chassis ID
`ip-address`	Use the management IP address as the chassis ID

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp management-address-tlv ip-address
```


© 2021 IP Infusion Inc. Proprietary

set lldp msg-tx-hold

Use this command to set the Time To Live (TTL) value for LLDPDUs to be transmitted by the port. The value set with this command is multiplied by the `msg-tx-interval` value (see set lldp timer), which determines the final TTL value.

Command Syntax

```
set lldp msg-tx-hold VALUE
```

Parameters

`VALUE`	Time in seconds

Default

The default value of the TTL is 4 seconds.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config)#set lldp msg-tx-hold 3
```

set lldp system-description

Use this command to set the string that identifies the LLDP system.

Command Syntax

```
set lldp system-description LINE
```

Parameters

LINE	Description of the LLDP system.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#set lldp system-description LLDP agent on B1
```


© 2021 IP Infusion Inc. Proprietary

set lldp system-name

Use this command to set the name of the LLDP system.

Command Syntax

```
set lldp system-name NAME
```

Parameters

NAME	Name of the LLDP system.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#set lldp system-name LLDP1
```

set lldp timer

Use this command to set the interval at which LLDP frames are transmitted.

Command Syntax

```
set lldp timer msg-tx-interval <5-32768>
set lldp timer reinitDelay VALUE
set lldp timer tx-delay <1-8192>
```

Parameters

`<5-32768>`	Message transmit interval value
`VALUE`	Reinit delay value
`<1-8192>`	Transmit delay value in range of: (1 <= `tx-delay` <= ((0.25)* `msg-tx-interval`)

Default Values

The default value for `msg-tx-interval` is 30 seconds.

The default value for `reinitDelay` is 2 seconds.

The default value of the `tx-delay` is 2 seconds.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp timer msg-tx-interval 40

#configure terminal
(config)#interface eth0
(config-if)#set lldp timer reinitDelay 3

#configure terminal
(config)#interface eth0
(config-if)#set lldp timer tx-delay 3
```


© 2021 IP Infusion Inc. Proprietary

set lldp too-many-neighbors

Use this command to set the action to take when the remote table is full.

Command Syntax

```
set lldp too-many-neighbors limit <1-65535> discard received-info timer <1-65535>
set lldp too-many-neighbors limit <1-65535> discard existing-info MAC
  timer <1-65535>
```

Parameters

`limit`	The limit on the number of LLDP neighbors.
`<1-65535>`	The limit on the number of LLDP neighbors.
`received-info`	The information received for this neighbor.
`timer`	The period after which received information is discarded.
`<1-65535>`	The period in seconds after which received information is discarded.
`existing-info`	The information for this neighbor.
`MAC`	Identifies the remote LLDP Agent for which information is discarded.
`timer`	The period in seconds after which existing information is discarded.
`<1-65535>`	The period in seconds after which existing information is discarded.

Default Value

No upper limit is enforced for the number of remote LLDP agents.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#set lldp too-many-neighbors limit 20 disc existing-info 1.1.1.1.1
timer 1

(config)#interface eth1
(config-if)#set lldp too-many-neighbors limit 1 discard received-info timer 1
```

show lldp

Use this command to display LLDP port information.

Command Syntax

```
show lldp port IFNAME
show lldp port IFNAME statistics
```

Parameters

IFNAME	Name of the interface
statistics	LLDP port statistics

Command Mode

Exec mode and Privileged Exec mode

Example

The following sample output from this command displays detailed information about an LLDP-enabled port.

```
#show lldp port eth0
Remote LLDP
MAC Address: 01:06:29:CF:79:A1
TTL: 60
Network Address: 192.168.1.0
Interface Name: eth1
Interface Locally Assigned String: Port-a
Interface Description: bridge
Interface Number: 2
Port Vlan ID: 1
Protocol ID: 274242030202
AutoNego Support: Supported
AutoNego Capability: 1
Operational MAU Type: 3
Link Aggregation Status: Capable
Link Aggregation Port ID: 0
Max Frame Size: 128
System name:
System Description: bridge
System Capabilities: 4
System Capabilities Enabled: 4
```

The following sample output from this command displays all LLDP statistics for a selected port.

```
#show lldp port eth0 statistics
LLDP Port statistics for eth0
Frames transmitted: 22
Frames Aged out: 0
Frames Discarded: 0
Frames with Error: 0
Frames Received: 5
TLVs discarded: 0
TLVs unrecognized 0
```


© 2021 IP Infusion Inc. Proprietary

snmp restart lldp

Use this command to restart SNMP in Link Layer Discovery Protocol (LLDP)

Command Syntax

```
snmp restart lldp
```

Parameters

None

Command Mode

Configure mode

Examples

```
#snmp restart lldp
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 10 Port Security Commands

This chapter describes the port security commands.

- port-security
- show port-security
- switchport port-security
- switchport port-security logging
- switchport port-security mac-address
- switchport port-security maximum

port-security

Use this command to enable or disable port security globally.

Command Syntax

```
port-security (enable | disable)
```

Parameters

`enable`	Enable port security globally
`disable`	Disable port security globally

Default

By default, port security is enabled globally.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
(config)#port-security enable
(config)#
```


© 2021 IP Infusion Inc. Proprietary

show port-security

Use this command to display the port security configuration for all interfaces or for a particular interface.

Command Syntax

```
show port-security (interface IFNAME |)
```

Parameters

IFNAME	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#show port-security
Port port-security mode MAC limit CVLAN SVLAN static secure MAC
-----------------------------------------------------------------
ge1  dynamic            3         2           0000.0000.1112
                                   10          0000.0000.3333

#show port-security interface ge1
Port Security Mode : Dynamic
Secure MAC limit : 3
Static Secure MAC list :
CVLAN SVLAN MAC Address
---------------------------
2           0000.0000.1112
10          0000.0000.3333
```

switchport port-security

Use this command to enable port security on an interface.

Use the `no` form of this command to disable port security on an interface. This command removes configured secured MAC, if any, on this interface.

Note: This command is supported for physical, LAG, and MLAG (active) interfaces only. Enabling port security on an interface removes learned MAC addresses of interfaces (whether learned by static or dynamic means), and then relearns the secure MAC addresses. Multicast MAC addresses are not considered as part of the MAC learning limit.

Note: This command is ignored when port security is already enabled on an interface.

Command Syntax

```
switchport port-security (static |)
no switchport port-security
```

Parameters

`static`	Static mode

Default

By default this feature is disabled; the default mode of port security is to dynamically learn. In dynamic mode, devices learn MAC addresses dynamically. You can program static MACs, however, dynamic MAC learning will not be allowed in static mode for port security.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode hybrid
(config-if)#switchport hybrid allowed vlan all
(config-if)#switchport port-security
```


© 2021 IP Infusion Inc. Proprietary

switchport port-security logging

Use this command to enable violated MAC logging on a port security enabled interface.

Use the `disable` parameter with this command to disable violated mac logging on a port security enabled interface.

Command Syntax

```
switchport port-security logging (enable | disable)
```

Parameters

`enable`	Enable violated MAC logging
`disable`	Disable violated MAC logging

Default

By default logging is disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security logging enable
```

switchport port-security mac-address

Use this command to add static secure MAC addresses.

Use the `no` form of this command to remove static secure MAC addresses.

Command Syntax

```
switchport port-security mac-address XXXX.XXXX.XXXX
no switchport port-security mac-address XXXX.XXXX.XXXX
switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094>
no switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094>
switchport port-security mac-address XXXX.XXXX.XXXX svlanId <2-4094>
no switchport port-security mac-address XXXX.XXXX.XXXX svlanId <2-4094>
switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094> svlanId <2-
  4094>
no switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094> svlanId <2-
  4094>
```

Parameters

`XXXX.XXXX.XXXX`	Static secure MAC address
`vlanId`	VLAN identifier
`<2-4094>`	VLAN identifier
`svlanId`	SVLAN identifier
`<2-4094>`	SVLAN identifier

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security mac-address 0000.0000.1112 vlan 2
(config-if)# no switchport port-security mac-address 0000.0000.1112 vlan 2
(config)#interface ge2
(config-if)#switchport port-security mac-address 0000.1111.2222
(config-if)#no switchport port-security mac-address 0000.1111.2222
(config)#interface ge3
(config-if)#switchport port-security mac-address 0000.2222.3333 svlan 9
(config-if)#no switchport port-security mac-address 0000.2222.3333 svlan 9
(config)#interface ge4
```


© 2021 IP Infusion Inc. Proprietary

```
(config-if)#switchport port-security mac-address 0000.2222.3333 vlan 23 svlan
31
(config-if)#no switchport port-security mac-address 0000.2222.3333 vlan 23
svlan 31
```

switchport port-security maximum

Use this command to set the MAC address learning limit for an interface.

Note: This command is supported for physical, LAG, and MLAG (active) interfaces only. When a newly configured maximum learn limit is less than the previous value, you must remove/flush-out the unwanted MACs to stop traffic forwarding from the unwanted source MAC addresses. MAC addresses can be removed using the clear mac address-table command.

Use `no` form cli to set the maximum limit back to default value 1.

Command Syntax

```
switchport port-security maximum <1-1000>
no switchport port-security maximum
```

Parameters

`<1-1000>`	Maximum MAC address learning limit

Default

The default MAC address learning limit is 1.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security maximum 3

#configure terminal
(config)#interface po1
(config-if)#switchport port-security maximum 3

#configure terminal
(config)#interface mlag1
(config-if)#switchport port-security maximum 3
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 11 VLAN Cross-Connect Commands

This chapter contains VLAN cross-connect commands.

- cross-connect
- disable
- outer-vlan VLAN_RANGE2 (inner-vlan VLAN_RANGE2 |)
- show cross-connect

cross-connect

Use this command to enter VLAN cross-connect mode to configure cross-connect parameters.

Use the `no` form of this command to delete a cross-connect.

Command Syntax

```
cross-connect WORD
no cross-connect WORD
```

Parameters

`WORD`	Cross-connect name, length <1-255>

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#cross-connect VC1
(config-XC)#

#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#no cross-connect VC1
(config)#
```


© 2021 IP Infusion Inc. Proprietary

disable

Use this command to make a cross-connect administratively disabled or enabled.

Command Syntax

```
disable
no disable
```

Parameters

None

Command Mode

Cross-connect mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
OcNOS#sh cross-connect
Cross-connect name : VC1
EP1:ce24/1     EP2:ce31/1     Admin Status:UP          Oper Status:UP
+=============================================================================================
============================+
| EP      | OVID    | IVID    | Rx packets    | Rx bytes     | Tx packets    |Tx bytes
|Interface Status|
+=============================================================================================
============================+
| EP1     |100      |     -    |0             |0             |0             |0
|UP              |
| EP2     |100      |     -    |0             |0             |0             |0
|UP              |
+=============================================================================================
============================+


cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
OcNOS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#cross-connect VC1
OcNOS(config-XC)#disable
2021 Mar 22 07:35:30.083 : OcNOS : NSM : CRITI : [VXC_DOWN_2]: Cross_Connect VC1 changed
state to down
OcNOS(config-XC)#end
OcNOS#sh cross-connect
ross-connect name : VC1
EP1:ce24/1     EP2:ce31/1     Admin Status:DOWN        Oper Status:DOWN
```

```
+=============================================================================================
============================+
| EP      | OVID    | IVID    | Rx packets    | Rx bytes     | Tx packets    |Tx bytes
|Interface Status|
+=============================================================================================
============================+
| EP1     |    -    |    -    |0              |0             |0              |0
|UP             |
| EP2     |    -    |    -    |0              |0             |0              |0
|UP             |
+=============================================================================================
============================+

cross-connect summary
Total XC    : 1
Admin Up    : 0
Admin Down  : 1
Total Rules : 0

OcNOS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#cross-connect VC1
OcNOS(config-XC)#no disable
OcNOS(config-XC)#2021 Mar 22 07:35:46.814 : OcNOS : NSM : CRITI : [VXC_UP_2]:
Cross_Connect VC1 changed state to up
OcNOS#sh cross-connect
Cross-connect name : VC1
EP1:ce24/1     EP2:ce31/1     Admin Status:UP         Oper Status:UP
+=============================================================================================
============================+
| EP      | OVID    | IVID    | Rx packets    | Rx bytes     | Tx packets    |Tx bytes
|Interface Status|
+=============================================================================================
============================+
| EP1*    |    -    |    -    |47836          |47836000      |0              |0
|UP             |
| EP2*    |    -    |    -    |0              |0             |48149          |48149000
|UP             |
+=============================================================================================
============================+

cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```


© 2021 IP Infusion Inc. Proprietary

outer-vlan VLAN_RANGE2 (inner-vlan VLAN_RANGE2 |)

Use this command to configure parameters for VLAN cross-connect.

Command Syntax

```
outer-vlan VLAN_ID inner-vlan VLAN_ID ep1 IFNAME ep2 IFNAME
```

Parameters

`outer-vlan`	Outer-VLAN associated with the cross-connect
`VLAN ID`	VLAN ID <2 - 4094>
`inner-vlan`	Inner-VLAN associated with the cross-connect
`VLAN ID`	VLAN ID <2 - 4094>
`ep1`	Interface for cross-connect endpoint 1
`IFNAME`	Interface name for endpoint 1
`ep2`	Interface for cross-connect endpoint 2
`IFNAME`	Interface name for endpoint 2

Command Mode

Cross-connect mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#conf t
Enter configuration commands, one per line.End with CNTL/Z. (config)#cross-connect VC1
(config-XC)#vlan ep1 ce25/1 ep2 ce16/1
(config-VXC)#outer-vlan 10 inner-vlan 20
(config-VXC)#
```

show cross-connect

Use this command to display the VLAN cross-connect configuration.

Command Syntax

```
show cross-connect
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
OcNOS#sh cross-connect
Cross-connect name : VC1
EP1:ce25/1     EP2:ce16/1     Admin Status:UP         Oper Status:UP
+=============================================================================
============================+
| EP      | OVID    | IVID    | Rx packets    | Rx bytes     | Tx packets    |Tx bytes
|Interface Status|
+=============================================================================
============================+
| EP1     |100      |     -    |0             |0             |0             |0
|UP              |
| EP2     |100      |     -    |0             |0             |0             |0
|UP              |
+=============================================================================
============================+


cross-connect summary
Total XC    : 1
Admin Up    : 1
Admin Down  : 0
Total Rules : 1
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 12 Unidirectional Link Detection Commands

This section describes the Unidirectional Link Detection (UDLD) commands.

- udld
- udld message-time
- udld mode
- udld state
- show udld
- show udld interface

udld

Use this command to enable or disable the UDLD feature globally.

Command Syntax

```
udld  (enable | disable)
```

Parameters

None

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
(config)#udld enable
```


© 2021 IP Infusion Inc. Proprietary

udld message-time

Use this command to set the UDLD message interval.

Command Syntax

```
udld message-time <7-90>
```

Parameters

<7-90>	Interval time in seconds

Default

15 seconds

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
config)#udld message-time 50
```

udld mode

Use this command to configure UDLD mode as aggressive or normal.

Command Syntax

```
udld mode (aggressive | normal)
```

Parameters

`aggressive`	Aggressive mode
`normal`	Normal mode

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
(config-if)#udld mode aggressive
```


© 2021 IP Infusion Inc. Proprietary

udld state

Use this command to enable or disable the UDLD feature for an interface.

Command Syntax

```
udld state (enable | disable)
```

Parameters

None

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
(config)#int xe7
(config-if)#udld state enable
```

show udld

Use this command to display UDLD statistic for all interface.

Command Syntax

```
show udld
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#show udld
UDLD                    : Enable
Message Interval(sec)   : 15
Port    UDLD Status     Mode            Link-Status
------------------------------------------------
xe7     Enable          Normal          Bi-Directional
```

Table 12-114 explains the output fields.

Table 12-114: show udld output fields

Field	Description
UDLD	Whether UDLD is enabled or disabled
Message Interval	Message interval in seconds
Port	Interface name
UDLD Status	Whether UDLD is enabled or disabled on the interface
Mode	Whether the mode is aggressive or normal
Link-Status	State of the link: Unknown Loop-Back Neighbor Mismatch Unidirectional Undetermined Bi-Directional

© 2021 IP Infusion Inc. Proprietary

show udld interface

Use this command to display UDLD settings for particular interface.

Command Syntax

```
show udld interface IFNAME
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 5.0.

Examples

```
#show udld interface xe14
UDLD Status           : Enable
UDLD Mode             : Aggressive
Link-State            : Bi-Directional
#
```

Table 12-115 explains the output fields.

Table 12-115: show udld interface output fields

Field	Description
UDLD Status	Whether UDLD is enabled or disabled
UDLD Mode	Whether the mode is aggressive or normal
Link-State	State of the link: Unknown Loop-Back Neighbor Mismatch Unidirectional Undetermined Bi-Directional

© 2021 IP Infusion Inc. Proprietary

SECTION 6 # Layer 3

Layer 3 Unicast Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *Static Routes*
- Chapter 2, *RIP*
- Chapter 3, *RIPng*
- Chapter 4, *OSPFv2*
- Chapter 5, *OSPFv3*
- Chapter 6, *IS-IS IPv4*
- Chapter 7, *IS-IS IPv6 Configuration*
- Chapter 8, *IS-IS Graceful Restart Configuration*
- Chapter 9, *BGP*
- Chapter 10, *BGP Labeled Unicast*
- Chapter 11, *BGP Graceful Restart Configuration*
- Chapter 12, *Static Route Discard Configuration*
- Chapter 13, *Route-map Continue Configuration*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Static Routes

This chapter contains basic static routing configuration examples.

This example shows the complete configuration to enable static routing in a simple network topology. A static route is composed of a network prefix (host address) and a nexthop (gateway). Static routes are useful in small networks. They are simple solutions for making a few destinations reachable. Large networks use dynamic routing protocols.

Topology

Router R1 is configured with these static routes:

- The remote network 10.10.12.0/24
- The loopback address (host addresses) of router R2
- The loopback address of router R3

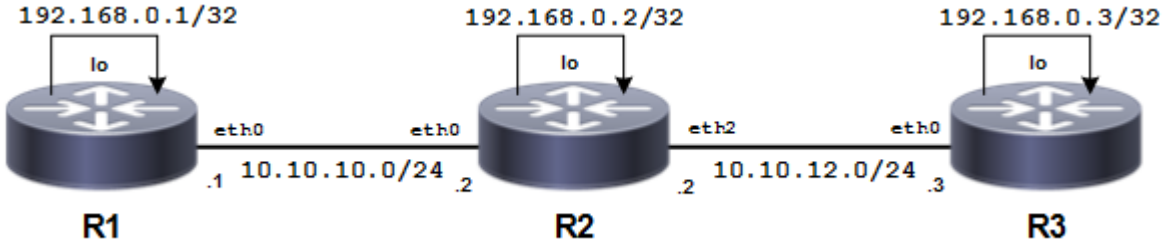


Figure 1-79: Basic Static Route

In all three routes, interface `eth0` of router R2 is the gateway. Router R3 is configured with a default static route that is equivalent to configuring separate static routes with the same gateway or nexthop address. Router R2 has two routes, one for each of the remote routers' loopback address.

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 192.168.0.1/32`	Configure the IP address on this interface, and specify a 32-bit mask, making it a host address.
`(config-if)#exit`	Exit interface mode.

`(config)#ip route 10.10.12.0/24 10.10.10.2`
`(config)#ip route 192.168.0.2/32 10.10.10.2`
`(config)#ip route 192.168.0.3/32 10.10.10.2`
	Specify the destination prefix and mask for the network and a gateway.
	Because R2 is the only next hop available, you can configure a default route instead of configuring the same static route for individual addresses. See the configuration of R3.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 192.168.0.2/32`	Configure the IP address on this interface, and specify a 32-bit mask, making it a host address.
`(config-if)#exit`	Exit interface mode.
`(config)#ip route 192.168.0.1/32 10.10.10.1` `(config)#ip route 192.168.0.3/32 10.10.12.3`	Specify the destination and mask for the network and a gateway.

R3

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 192.168.0.3/32`	Configure the IP address on this interface, and specify a 32-bit mask, making it a host address.
`(config-if)#exit`	Exit interface mode.
`(config)#ip route 0.0.0.0/0 10.10.12.2`	Specify 10.10.12.2 as a default gateway to reach any network. Because 10.10.12.2 is the only available route, you can specify it as the default gateway instead of specifying it as the gateway for an individual network or host address.

Validation

show ip route, show ip route summary, show ip route database

R1

```
#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth1
S       10.10.12.0/24 [1/0] via 10.10.10.2, eth1
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.1/32 is directly connected, lo
S       192.168.0.2/32 [1/0] via 10.10.10.2, eth1
S       192.168.0.3/32 [1/0] via 10.10.10.2, eth1

#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
```


© 2021 IP Infusion Inc. Proprietary

```
IP routing table maximum-paths   : 8
Total number of IPv4 routes      : 8
Total number of IPv4 paths       : 8
Route Source    Networks
kernel          1
connected       4
static          3
Total           8
FIB             0

ECMP statistics (active in ASIC):
---------------------------------
 Total number of IPv4 ECMP routes   : 0
 Total number of IPv4 ECMP paths    : 0

---------------------------------

#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
K    *> 0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C    *> 10.10.10.0/24 is directly connected, eth1
S    *> 10.10.12.0/24 [1/0] via 10.10.10.2, eth1
C    *> 10.12.4.0/24 is directly connected, eth0
C    *> 127.0.0.0/8 is directly connected, lo
C    *> 192.168.0.1/32 is directly connected, lo
S    *> 192.168.0.2/32 [1/0] via 10.10.10.2, eth1
S    *> 192.168.0.3/32 [1/0] via 10.10.10.2, eth1

Gateway of last resort is not set
```

R2

```
#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth1
C       10.10.12.0/24 is directly connected, eth2
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
S       192.168.0.1/32 [1/0] via 10.10.10.1, eth1
```

```
C       192.168.0.2/32 is directly connected, lo
S       192.168.0.3/32 [1/0] via 10.10.12.3, eth2

#sh ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths   : 8
Total number of IPv4 routes      : 9
Total number of IPv4 paths       : 9
Route Source    Networks
kernel          1
connected       5
static          3
Total           9
FIB             0

ECMP statistics (active in ASIC):
---------------------------------
 Total number of IPv4 ECMP routes   : 0
 Total number of IPv4 ECMP paths    : 0

---------------------------------

#sh ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
K    *> 0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C    *> 10.10.10.0/24 is directly connected, eth1
C    *> 10.10.12.0/24 is directly connected, eth2
C    *> 10.12.4.0/24 is directly connected, eth0
C    *> 127.0.0.0/8 is directly connected, lo
S    *> 192.168.0.1/32 [1/0] via 10.10.10.1, eth1
C    *> 192.168.0.2/32 is directly connected, lo
S    *> 192.168.0.3/32 [1/0] via 10.10.12.3, eth2

Gateway of last resort is not set
```

R3

```
#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
```


© 2021 IP Infusion Inc. Proprietary

```
C       10.10.12.0/24 is directly connected, eth2
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.3/32 is directly connected, lo

#sh ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths   : 8
Total number of IPv4 routes      : 6
Total number of IPv4 paths       : 6
Route Source    Networks
kernel          2
connected       4
Total           6
FIB             0

ECMP statistics (active in ASIC):
---------------------------------
 Total number of IPv4 ECMP routes   : 0
 Total number of IPv4 ECMP paths    : 0
---------------------------------


#sh ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
K    *> 0.0.0.0/0 [0/0] via 10.12.4.1, eth0
S       0.0.0.0/0 [1/0] via 10.10.12.2 inactive
C    *> 10.10.12.0/24 is directly connected, eth2
C    *> 10.12.4.0/24 is directly connected, eth0
C    *> 127.0.0.0/8 is directly connected, lo
C    *> 192.168.0.3/32 is directly connected, lo

Gateway of last resort is not set
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 RIP

This chapter contains basic Router Information Protocol (RIP) configuration examples.

Enable RIP

This example shows the minimum configuration required to enable RIP on an interface. R1 and R2 are two routers connecting to network 10.10.11.0/24. R1 and R2 are also connected to networks 10.10.10.0/24 and 10.10.12.0/24, respectively. To enable RIP, first define the RIP routing process, then associate a network with the routing process.

Topology

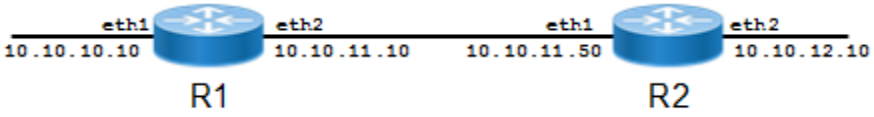


Figure 2-80: Enable RIP Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24` `(config-router)#network 10.10.11.0/24`	Associate networks with the RIP process.

R2

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.11.0/24` `(config-router)#network 10.10.12.0/24`	Associate networks with the RIP process.

Validation

show ip rip, show running-config, show ip protocols rip, show ip rip interface, show ip route

R1

```
#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth1
Rc 10.10.11.0/24                           1                  eth2
```

```
#show running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.2/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.108/24
!
interface eth1
 ip address 10.10.10.10/24
!
interface eth2
 ip address 10.10.11.10/24
!
router rip
 network 10.10.10.0/24
 network 10.10.11.0/24
!
line con 0
 login
line vty 0 39
 login
!
end

#show ip protocols rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 14 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
```


© 2021 IP Infusion Inc. Proprietary

```
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             2     2
    eth2             2     2
  Routing for Networks:
    10.10.10.0/24
    10.10.11.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 2
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.10/24
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.10/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth1
C       10.10.11.0/24 is directly connected, eth2
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.2/32 is directly connected, lo
```

R2

```
#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.11.0/24                           1                  eth1
Rc 10.10.12.0/24                           1                  eth2

2#show running-config
!
no service password-encryption
!
hostname rtr2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.3/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.183/24
!
interface eth1
 ip address 10.10.11.50/24
!
interface eth2
 ip address 10.10.12.10/24
!
router rip
 network 10.10.11.0/24
 network 10.10.12.0/24
!
line con 0
 login
line vty 0 39
```


© 2021 IP Infusion Inc. Proprietary

```
 login
!
end

#show ip protocols rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 5 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             2     2
    eth2             2     2
  Routing for Networks:
    10.10.11.0/24
    10.10.12.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 2
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.12.10/24
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.50/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default
```

```
IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.11.0/24 is directly connected, eth1
C       10.10.12.0/24 is directly connected, eth2
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.3/32 is directly connected, lo
```

Specify RIP Version

Configure a router to receive and send specific versions of packets on an interface. In this example, router R2 is configured to receive and send RIP version 1 and version 2 information on both eth1 and eth2 interfaces.

Topology

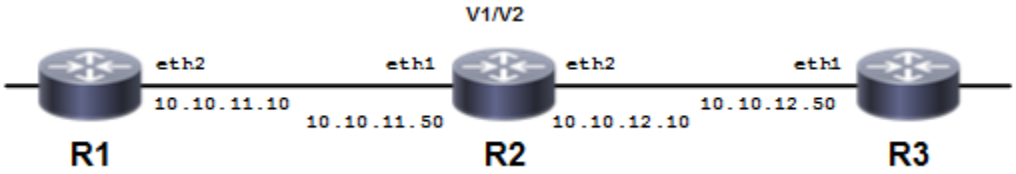


Figure 2-81: RIP Version Topology

R2

`#configure terminal`	Enter configure mode
`(config)#router rip`	Enable the RIP routing process
`(config-router)#exit`	Exit router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip rip send version 1 2`	Send RIP version 1 and version 2 packets out this interface
`(config-if)#ip rip receive version 1 2`	Receive RIP version 1 and version 2 packets from this interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip rip send version 1 2`	Send RIP version 1 and version 2 packets out this interface
`(config-if)#ip rip receive version 1 2`	Receive RIP version 1 and version 2 packets from this interface

Validation

R2

```
#sh ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default
```


© 2021 IP Infusion Inc. Proprietary

```
   Network            Next Hop         Metric From            If     Time
Rc 10.10.11.0/24                           1                  eth1
Rc 10.10.12.0/24                           1                  eth2

#sh running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.2/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.108/24
!
interface eth1
 ip address 10.10.11.50/24
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth2
 ip address 10.10.12.10/24
 ip rip send version 1 2
 ip rip receive version 1 2
!
router rip
 network 10.10.11.0/24
 network 10.10.12.0/24
!
line con 0
 login
line vty 0 39
 login
!
end

#show ip protocols rip
```

```
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 29 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             1 2   1 2
    eth2             1 2   1 2
  Routing for Networks:
    10.10.11.0/24
    10.10.12.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.10.11.10           120  00:00:31               0           0
    10.10.12.50           120  00:00:08               0           0
  Number of routes (including connected): 2
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.12.10/24
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.50/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0
```


© 2021 IP Infusion Inc. Proprietary

```
K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.11.0/24 is directly connected, eth1
C       10.10.12.0/24 is directly connected, eth2
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.2/32 is directly connected, lo
```

Authentication with a Single Key

OcNOS RIP provides a choice of configuring authentication with a single key or with multiple keys. This example shows authenticating routing information exchange using a single key.

Topology

Routers R1 and R2 are running RIP and exchanging routing updates. To configure single-key authentication on R1, specify an interface, then define a key or password for that interface. Next, specify an authentication mode. Any receiving RIP packet on this specified interface should have the same string as the password. For an exchange of updates between R1 and R2, define the same password and authentication mode on R2.

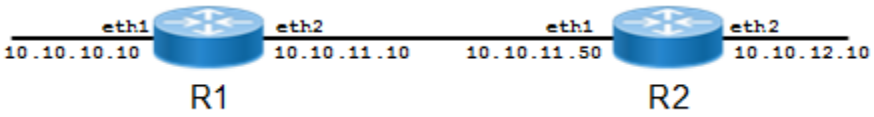


Figure 2-82: Single-key Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Specify the interface (`eth1`) for authentication.
`(config-if)#ip rip authentication string ABC`	Specify the authentication string (`ABC`) for this interface.
`(config-if)#ip rip authentication mode md5`	Specify the authentication mode to be MD5.

R2

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Exit router mode.

`(config)#interface eth2`	Specify the interface (`eth2`) for authentication.
`(config-if)#ip rip authentication string ABC`	Specify the authentication string (`ABC`) on this interface.
`(config-if)#ip rip authentication mode md5`	Specify the authentication mode to be MD5.

Validation

show running-config, show ip rip, show ip protocol rip, show ip rip interface, show ip route

R1

```
#show running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.1/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.92/24
!
interface eth1
 ip address 10.10.10.10/24
 ip rip authentication mode md5
 ip rip authentication string 0x5c5b790e25d29287
!
interface eth2
 ip address 10.10.11.10/24
!
router rip
 network 10.10.10.0/24
 redistribute connected
!
```


© 2021 IP Infusion Inc. Proprietary

```
line con 0
 login
line vty 0 39
 login
!
end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth1
C  10.10.11.0/24                           1                  eth2
R  10.10.12.0/24      10.10.10.50          2 10.10.10.50      eth1   02:33
C  10.12.4.0/24                            1                  eth0
C  192.168.0.1/32                          1                  lo
R  192.168.0.2/32     10.10.10.50          2 10.10.10.50      eth1   02:33

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 26 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             2     2
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.10.10.50           120  00:00:31               0           0
  Number of routes (including connected): 6
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  RIP is not enabled on this interface
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.10/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
```

```
  RIP is not enabled on this interface

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth1
C       10.10.11.0/24 is directly connected, eth2
R       10.10.12.0/24 [120/2] via 10.10.10.50, eth1, 00:04:05
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.1/32 is directly connected, lo
R       192.168.0.2/32 [120/2] via 10.10.10.50, eth1, 00:04:05
```

R2

```
#sh running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.2/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.108/24
!
interface eth1
 ip address 10.10.12.50/24
!
```

 © 2021 IP Infusion Inc. Proprietary

```
interface eth2
 ip address 10.10.10.50/24
 ip rip authentication mode md5
 ip rip authentication string 0x5c5b790e25d29287
!
router rip
 network 10.10.10.0/24
 redistribute connected
!
line con 0
 login
line vty 0 39
 login
!
end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth2
R  10.10.11.0/24      10.10.10.10          2 10.10.10.10      eth2   02:58
C  10.10.12.0/24                           1                  eth1
C  10.12.4.0/24                            1                  eth0
R  192.168.0.1/32     10.10.10.10          2 10.10.10.10      eth2   02:58
C  192.168.0.2/32                          1                  lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 5 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth2             2     2
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.10.10.10           120  00:00:01               0           0
  Number of routes (including connected): 6
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
```

```
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.50/24
eth1 is up, line protocol is up
  RIP is not enabled on this interface
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth2
R       10.10.11.0/24 [120/2] via 10.10.10.10, eth2, 00:07:36
C       10.10.12.0/24 is directly connected, eth1
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
R       192.168.0.1/32 [120/2] via 10.10.10.10, eth2, 00:07:36
C       192.168.0.2/32 is directly connected, lo
```

Text Authentication with Multiple Keys

This example illustrates text authentication of the routing information exchange process for RIP using multiple keys. Routers R1 and R2 are running RIP, and exchanging routing updates. To configure authentication on R1, define a key chain, specify keys in the key chain, then define the authentication string or passwords to use by the keys. Set the time period during which it is valid to receive or send the authentication key by specifying the accept and send lifetimes. After defining the key string, specify the key chain (or set of keys) that will be used for authentication on each interface, and the authentication mode to use.

R1 receives all packets that contain any key string that matches one of the key strings included in the specified key chain (within the accept lifetime) on that interface. The key ID is not considered for matching. For additional security, the accept lifetime and send lifetime are configured such that every fifth day, the key ID and key string changes. To maintain continuity, the accept lifetimes should be configured to overlap. This will accommodate different time setup on machines. However, the send lifetime is not required to overlap, and IP Infusion Inc. recommends configuring no overlapping for the send lifetime.

© 2021 IP Infusion Inc. Proprietary

Topology

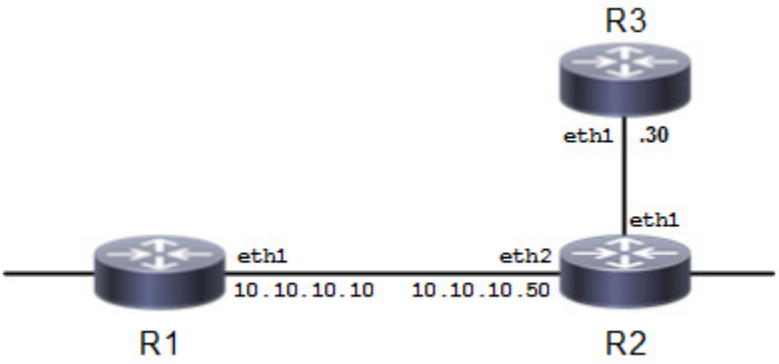


Figure 2-83: Multiple-key Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Exit router mode.
`(config)#key chain SUN`	Enter Keychain management mode to add keys to the key chain `SUN`.
`(config-keychain)#key 10`	Add authentication key ID (`10`) to the key chain `SUN`.
`(config-keychain-key)#key-string ABC`	Specify a password (`ABC`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be received. In this case, key string `ABC` can be received from noon of March 2 to 2 pm March 7, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `ABC` can be sent from noon of March 2 to noon of March 7, 2003.
`(config-keychain-key)#exit`	Exit Keychain-Key mode, and return to Keychain mode.
`(config-keychain)#key 20`	Add another authentication key (`20`) to the key chain `SUN`.
`(config-keychain-key)#key-string Earth`	Specify a password (`Earth`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003`	Specify the time period during which authentication key string `Earth` can be received. In this case, key string `Earth` can be received from noon of March 7 to 2 pm March 12, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `Earth` can be sent from noon of March 7 to noon of March 12, 2003.
`(config-keychain-key)#end`	Enter Privileged Exec mode.

© 2021 IP Infusion Inc. Proprietary

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify interface `eth1` as the interface you want to configure.
`(config-if)#ip rip authentication key chain SUN`	Enable RIPv2 authentication on `eth1` interface and specify the key chain `SUN` to use for authentication.
`(config-if)#ip rip authentication mode text`	Specify text authentication mode to use for RIP packets. This step is optional, because text is the default mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Exit router mode.
`(config)#key chain MOON`	Enter Keychain management mode to add keys to the key chain `MOON`.
`(config-keychain)#key 30`	Add authentication key ID (`30`) to the key chain `MOON`.
`(config-keychain-key)#key-string ABC`	Specify a password (`ABC`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be received. In this case, key string `ABC` can be received from noon of March 2 to 2 pm March 7, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `ABC` can be sent from noon of March 2 to noon of March 7, 2003.
`(config-keychain)#key 40`	Add another authentication key (`40`) to the key chain `MOON`.
`(config-keychain-key)#key-string Earth`	Specify a password (`Earth`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003`	Specify the time period during which authentication key string `Earth` can be received. In this case, key string `Earth` can be received from noon of March 7 to 2 pm March 12, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `Earth` can be sent from noon of March 7 to noon of March 12, 2003.
`(config-keychain-key)#end`	Enter Privileged Exec mode.
`#configure terminal`	Enter configure mode.
`(config)#interface eth2`	Specify interface `eth2` as the interface you want to configure.
`(config-if)#ip rip authentication key chain MOON`	Enable RIPv2 authentication on the `eth1` interface, and specify the key chain `MOON` to use for authentication.
`(config-if)#ip rip authentication mode text`	Specify the authentication mode to use for RIP packets. This step is optional, because text is the default mode.

© 2021 IP Infusion Inc. Proprietary

Validation

show running-config, show ip rip, show ip protocol rip, show ip rip interface, show ip route

R1

```
#sh running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
!
key chain SUN
 key 10
  key-string 0x5c5b790e25d29287
  accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003
  send-lifetime 12:00:00 Mar 02 2003 12:00:00 Mar 07 2003
 key 20
  key-string 0x51b2c401dd313187
  accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003
  send-lifetime 12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.1/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.92/24
!
interface eth1
 ip address 10.10.10.10/24
 ip rip authentication mode text
 ip rip authentication key-chain chain SUN
!
interface eth2
!
router rip
 network 10.10.10.0/24
```

```
 redistribute connected
!
line con 0
 login
line vty 0 39
 login
!
end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                         1                    eth1
C  10.12.4.0/24                          1                    eth0
C  192.168.0.1/32                       1                    lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 16 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             2     2      chain SUN
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 3
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is down, line protocol is down
  RIP is not enabled on this interface
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.10/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface
```


© 2021 IP Infusion Inc. Proprietary

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth1
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.1/32 is directly connected, lo
```

R2

```
#sh running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
key chain MOON
 key 30
  key-string 0x5c5b790e25d29287
  accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003
  send-lifetime 12:00:00 Mar 02 2003 12:00:00 Mar 07 2003
 key 40
  key-string 0x51b2c401dd313187
  accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003
  send-lifetime 12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.2/32 secondary
 ipv6 address ::1/128
!
interface eth0
```

```
 ip address 10.12.4.108/24
!
interface eth1
!
interface eth2
 ip address 10.10.10.50/24
 ip rip authentication mode text
 ip rip authentication key-chain chain MOON
!
router rip
 network 10.10.10.0/24
 redistribute connected
!
line con 0
 login
line vty 0 39
 login
!
end

#sh ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth2
C  10.12.4.0/24                            1                  eth0
C  192.168.0.2/32                          1                  lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 5 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth2             2     2      chain MOON
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 3
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
```


© 2021 IP Infusion Inc. Proprietary

```
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.50/24
eth1 is down, line protocol is down
  RIP is not enabled on this interface
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth2
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.2/32 is directly connected, lo
```

MD5 Authentication with Multiple Keys

This example illustrates the MD5 authentication of the routing information exchange process for RIP using multiple keys. Routers R1 and R2 are running RIP, and exchanging routing updates. To configure authentication on R1, define a key chain, specify keys in the key chain, then define the authentication string or passwords to use by the keys. Then, set the time period during which it is valid to receive or send the authentication key by specifying the accept and send lifetimes. After defining the key string, specify the key chain (or the set of keys) that will be used for authentication on the interface, and the authentication mode to use. Configure R2 and R3 to have the same key ID and key string as R1 for the time that updates are to be exchanged.

In MD5 authentication, both the key ID and key string are matched for authentication. R1 will receive only packets that match both the key ID and the key string in the specified key chain (within the accept lifetime) on that interface. In the following example, R2 has the same key ID and key string as R1. For additional security, the accept lifetime and send lifetime are configured such that every fifth day, the key ID and key string changes. To maintain continuity, the accept lifetimes should be configured to overlap; however, the send lifetime should not overlap.

Topology

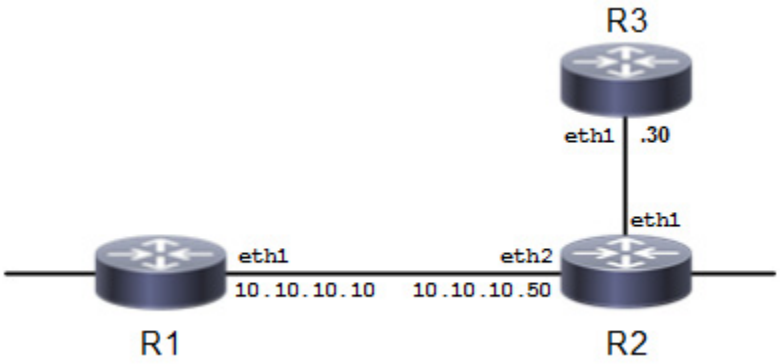


Figure 2-84: MD5 Multiple-key Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Exit router mode.
`(config)#key chain SUN`	Enter Keychain management mode to add keys to the key chain `SUN`.
`(config-keychain)#key 1`	Add authentication key ID (`1`) to the key chain `SUN`.
`(config-keychain-key)#key-string ABC`	Specify a password (`ABC`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be received. In this case, key string `ABC` can be received from noon of March 2 to 2 pm March 7, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `ABC` can be sent from noon of March 2 to noon of March 7, 2003.
`(config-keychain-key)#exit`	Exit Keychain-Key mode, and return to Keychain mode.
`(config-keychain)#key 2`	Add another authentication key (`2`) to the key chain `SUN`.
`(config-keychain-key)#key-string Earth`	Specify a password (`Earth`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003`	Specify the time period during which authentication key string `Earth` can be received. In this case, key string `Earth` can be received from noon of March 7 to 2 pm March 12, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `Earth` can be sent from noon of March 7 to noon of March 12, 2003.
`(config-keychain-key)#end`	Enter Privileged Exec mode.
`#configure terminal`	Enter configure mode.

© 2021 IP Infusion Inc. Proprietary

(config)#interface eth1	Specify interface eth1 as the interface you want to configure.
(config-if)#ip rip authentication key chain SUN	Enable RIPv2 authentication on the eth1 interface, and specify the key chain SUN to use for authentication.
(config-if)#ip rip authentication mode md5	Specify MD5 authentication mode to use for RIP packets.

R2

#configure terminal	Enter configure mode.
(config)#router rip	Define a RIP routing process, and enter Router mode.
(config-router)#network 10.10.10.0/24	Associate network 10.10.10.0/24 with the RIP process.
(config-router)#redistribute connected	Enable redistributing from connected routes.
(config-router)#exit	Exit router mode.
(config)#key chain MOON	Enter Keychain management mode to add keys to the key chain MOON.
(config-keychain)#key 1	Add authentication key ID (1) to the key chain MOON.
(config-keychain-key)#key-string ABC	Specify a password (ABC) to use by the specified key.
(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003	Specify the time period during which the authentication key can be received. In this case, key string ABC can be received from noon of March 2 to 2 pm March 7, 2003.
(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003	Specify the time period during which the authentication key can be sent. In this case, key string ABC can be sent from noon of March 2 to noon of March 7, 2003.
(config-keychain)#key 2	Add another authentication key (2) to the key chain MOON.
(config-keychain-key)#key-string Earth	Specify a password (Earth) to use by the specified key.
(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003	Specify the time period during which the authentication key can be received. In this case, key string Earth can be received from noon of March 7 to 2 pm March 12, 2003.
(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003	Specify the time period during which the authentication key can be sent. In this case, key string Earth can be sent from noon of March 7 to noon of March 12, 2003.
(config-keychain-key)#end	Enter Privileged Exec mode.
#configure terminal	Enter configure mode.
(config)#interface eth2	Specify interface eth2 as the interface you want to configure.
(config-if)#ip rip authentication key chain MOON	Enable RIPv2 authentication on the eth1 interface, and specify the key chain MOON to use for authentication.
(config-if)#ip rip authentication mode md5	Specify the authentication mode to use for RIP packets.

Validation

show running-config, show ip rip, show ip protocol rip, show ip rip interface

R1

```
#sh running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
!
key chain SUN
 key 1
  key-string 0x5c5b790e25d29287
  accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003
  send-lifetime 12:00:00 Mar 02 2003 12:00:00 Mar 07 2003
 key 2
  key-string 0x51b2c401dd313187
  accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003
  send-lifetime 12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.1/32 secondary
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.4.92/24
!
interface eth1
 ip address 10.10.10.10/24
 ip rip authentication mode md5
 ip rip authentication key-chain chain SUN
!
interface eth2
!
router rip
 network 10.10.10.0/24
```


© 2021 IP Infusion Inc. Proprietary

```
 redistribute connected
!
line con 0
 login
line vty 0 39
 login
!
end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth1
C  10.12.4.0/24                            1                  eth0
C  192.168.0.1/32                          1                  lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 19 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth1             2     2      chain SUN
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 3
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is down, line protocol is down
  RIP is not enabled on this interface
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.10/24
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface
```

R2

```
#sh running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
key chain MOON
 key 1
  key-string 0x5c5b790e25d29287
  accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003
  send-lifetime 12:00:00 Mar 02 2003 12:00:00 Mar 07 2003
 key 2
  key-string 0x51b2c401dd313187
  accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003
  send-lifetime 12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
!
ip domain-lookup
spanning-tree mode provider-rstp

feature telnet
feature ssh
no feature tacacs+
snmp-server view all .1 included
ntp enable
sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ip address 192.168.0.2/32 secondary
 ipv6 address ::1/128
!
interface eth0
ip address 10.12.4.108/24
!
interface eth1
!
interface eth2
 ip address 10.10.10.50/24
 ip rip authentication mode md5
 ip rip authentication key-chain chain MOON
!
router rip
 network 10.10.10.0/24
 redistribute connected
!
line con 0
 login
line vty 0 39
 login
```


© 2021 IP Infusion Inc. Proprietary

```
!
end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
       X - Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth2
C  10.12.4.0/24                            1                  eth0
R  192.168.0.1/32     10.10.10.10         16 10.10.10.10     eth2   01:29
C  192.168.0.2/32                          1                  lo


#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 9 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    eth2             2     2      chain MOON
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 4
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down
  RIP is not enabled on this interface
eth2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.50/24
eth1 is down, line protocol is down
  RIP is not enabled on this interface
eth0 is up, line protocol is up
  RIP is not enabled on this interface
lo is up, line protocol is up
  RIP is not enabled on this interface
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 RIPng

This chapter contains a basic RIPng configuration example.

Topology

The diagram shows the minimum configuration required to enable RIPng on an interface. R1 and R2 are two routers connected to network 3ffe:11::/64. To enable RIPng, first define the RIPng routing process, then enable RIPng on each interface.

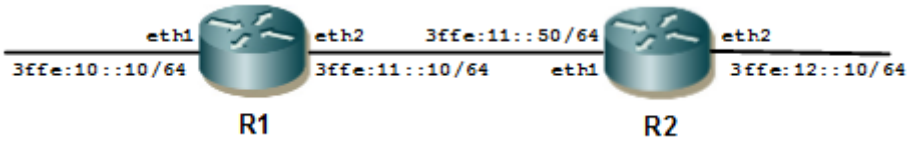


Figure 3-85: RIPng Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router rip`	Enable RIPng routing on interface `eth1`.
`(config-if)#exit`	Exit interface mode, and enter Configure mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router rip`	Enable RIPng routing on interface `eth2`.
`(config-if)#exit`	Exit interface mode, and enter Configure mode.
`(config)#router ipv6 rip`	Define a RIPng routing process, and enter Router mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router rip`	Enable RIPng routing on interface `eth1`.
`(config-if)#exit`	Exit interface mode, and enter Configure mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router rip`	Enable RIPng routing on interface `eth2`.
`(config-if)#exit`	Exit interface mode, and enter Configure mode.
`(config)#router ipv6 rip`	Define a RIPng routing process, and enter Router mode.

Validation

show ipv6 rip

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 OSPFv2

This chapter contains basic OSPFv2 (Open Shortest Path First) configuration examples.

Enable OSPF on an Interface

The diagram shows the minimum configuration required to enable OSPF on an interface. R1 and R2 are two routers in Area 0 connecting to network 10.10.10.0/24.

Note: Configure one interface so that it belongs to only one area. It is possible, however, to configure different interfaces on a router to belong to different areas.

Topology

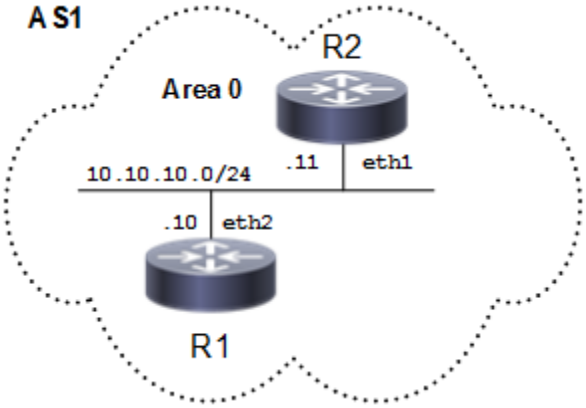


Figure 4-86: Basic OSPF Topology

R1

`#configure terminal`	Enter configure mode
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).

R2

`#configure terminal`	Enter configure mode
`(config)#router ospf 200`	Configure the routing process, and specify the Process ID `(200)`. The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface `(10.10.10.0/24)` on which OSPF runs, and associate the area ID `(0)` with the interface.

Validation

R1

```
#show ip ospf
 Routing Process "ospf 100" with ID 10.12.26.88
 Process uptime is 1 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 4
 Number of LSA received 4
 Number of areas attached to this router: 1
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:00:08.102 ago
        SPF algorithm executed 3 times
        Number of LSA 7. Checksum 0x0312b5
 Dste Staus: Disabled

#show ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.10.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:11
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 13 sent 19, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 3 sent 5
  LS-Ack received 3 sent 3, Discarded 0
No authentication
```


© 2021 IP Infusion Inc. Proprietary

```
#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.89       1   Full/Backup     00:00:39    10.10.10.11     eth2
0


#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.10.0/24 [1] is directly connected, eth2, Area 0.0.0.0
```

R2

```
#show  ip ospf
 Routing Process "ospf 200" with ID 10.12.26.89
 Process uptime is 1 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 3
 Number of LSA received 5
 Number of areas attached to this router: 1
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:00:45.638 ago
        SPF algorithm executed 4 times
        Number of LSA 7. Checksum 0x0312b5
 Dste Staus: Disabled

#show ip ospf interface
eth1 is up, line protocol is up
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
```

```
  Process ID 200, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 30 sent 31, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 3
  LS-Ack received 2 sent 3, Discarded 0
No authentication


#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 200 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address         Interface
Instance ID
10.12.26.88      1   Full/DR        00:00:33   10.10.10.10    eth1
0

#show ip ospf route

OSPF process 200:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.10.0/24 [1] is directly connected, eth1, Area 0.0.0.0
```


© 2021 IP Infusion Inc. Proprietary

Set Priority

This example shows how to set the priority for an interface. Set a high priority for a router to make it the Designated Router (DR). Router R3 is configured to have a priority of 10, which is higher than the default priority (1) of R1 and R2; making it the DR.

Topology

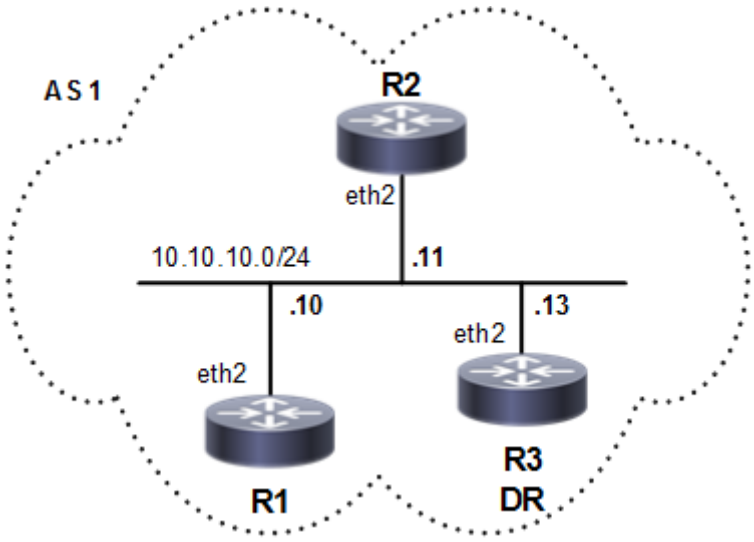


Figure 4-87: Set OSPF Priority

R3

`#configure terminal`	Enter configure mode
`(config)#``interface eth2`	Enter interface mode.
`(config-if)#``ip ospf priority 10`	Specify the router priority to a higher priority (10) to make R3 the Designated Router (DR).
`(config-if)#``exit`	Exit interface mode.
`(config)#``router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#``network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface.

R1

`#configure terminal`	Enter configure mode
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).

© 2021 IP Infusion Inc. Proprietary

R2

`#configure terminal`	Enter configure mode
`(config)#router ospf 200`	Configure the routing process, and specify the Process ID (`200`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface.

Validation

R1

```
#sh ip ospf neighbor

Total number of full neighbors: 2
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.89       1   Full/DROther    00:00:39    10.10.10.11     eth2
0
10.12.26.90      10   Full/DR         00:00:32    10.10.10.13     eth2
0

#sh ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.10.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.10.13
  Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:10
  Neighbor Count is 2, Adjacent neighbor count is 2
  Suppress hello for 0 neighbor(s)
  Hello received 30 sent 19, DD received 6 sent 8
  LS-Req received 2 sent 2, LS-Upd received 16 sent 6
  LS-Ack received 8 sent 7, Discarded 0
  No authentication

#sh running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
```


© 2021 IP Infusion Inc. Proprietary

```
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.88/24
!
interface eth1
!
interface eth2
 ip address 10.10.10.10/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
interface eth7
!
router ospf 100
 network 10.10.10.0/24 area 0.0.0.0
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end
```

R2

```
#sh running-config
!
no service password-encryption
!
hostname R2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.89/24
```

```
!
interface eth1
!
interface eth2
 ip address 10.10.10.11/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
router ospf 200
 network 10.10.10.0/24 area 0.0.0.0
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end

#sh ip ospf neighbor

Total number of full neighbors: 2
OSPF process 200 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/Backup     00:00:30    10.10.10.10     eth2
0
10.12.26.90      10   Full/DR         00:00:31    10.10.10.13     eth2
0
R2#

R2#sh ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
  Process ID 200, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DROther, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.10.13
  Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 2, Adjacent neighbor count is 2
  Suppress hello for 0 neighbor(s)
  Hello received 71 sent 36, DD received 7 sent 7
  LS-Req received 2 sent 2, LS-Upd received 9 sent 4
  LS-Ack received 3 sent 4, Discarded 1
  No authentication
```

R3

```
#sh running-config
!
```


© 2021 IP Infusion Inc. Proprietary

```
no service password-encryption
!
hostname R3
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
spanning-tree mode provider-rstp

ethernet cfm enable
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.90/24
!
interface eth1
!
interface eth2
 ip address 10.10.10.13/24
 ip ospf priority 10
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
router ospf 100
 network 10.10.10.0/24 area 0.0.0.0
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end

#sh ip ospf neighbor

Total number of full neighbors: 2
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/Backup     00:00:33    10.10.10.10     eth2
0
10.12.26.89       1   Full/DROther    00:00:30    10.10.10.11     eth2
0
```

```
#sh ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.10.13/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.90, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 10, TE Metric 1
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.10.13
  Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 2, Adjacent neighbor count is 2
  Suppress hello for 0 neighbor(s)
  Hello received 99 sent 60, DD received 8 sent 6
  LS-Req received 2 sent 2, LS-Upd received 9 sent 12
  LS-Ack received 9 sent 6, Discarded 1
```

No authentication

Area Border Router

This example shows configuration for an Area Border Router. R2 is an Area Border Router (ABR). On R2, Interface eth0 is in Area 0, and Interface eth1 is in Area 1.

Topology

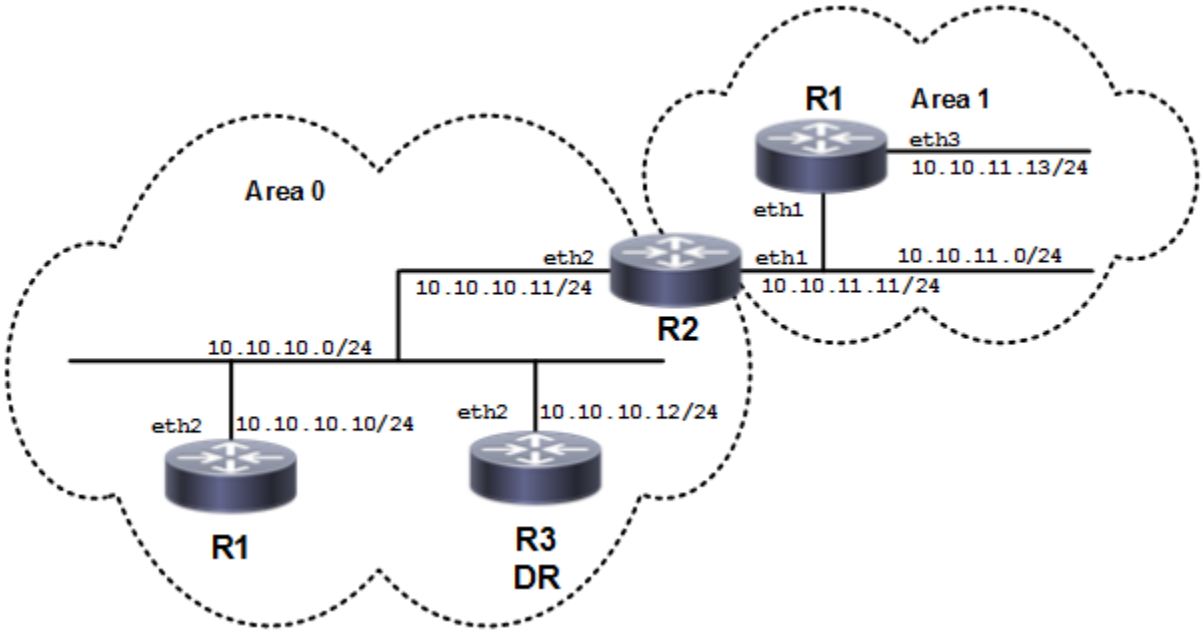


Figure 4-88: OSPF ABR Topology

© 2021 IP Infusion Inc. Proprietary

Configuration

R2

`#configure terminal`	Enter configure mode
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface.
`(config-router)#network 10.10.11.0/24 area 1`	Define the other interface `(10.10.11.0/24)` on which OSPF runs, and associate the area ID `(1)` with the interface.

Validation

R2

```
#show running-config
!
no service password-encryption
!
hostname R2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.89/24
!
interface eth1
 ip address 10.10.11.11/24
!
interface eth2
 ip address 10.10.10.11/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
```

```
router ospf 100
 network 10.10.10.0/24 area 0.0.0.0
 network 10.10.11.0/24 area 0.0.0.1
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end

#sh ip ospf
 Routing Process "ospf 100" with ID 10.12.26.89
 Process uptime is 4 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 9
 Number of LSA received 18
 Number of areas attached to this router: 2
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 2
        Area has no authentication
        SPF algorithm last executed 00:01:54.085 ago
        SPF algorithm executed 7 times
        Number of LSA 11. Checksum 0x0428ac
    Area 0.0.0.1
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Number of fully adjacent virtual neighbors through this area is 0
        Area has no authentication
        SPF algorithm last executed 00:00:41.737 ago
SPF algorithm executed 3 times
        Number of LSA 8. Checksum 0x043ce4
 Dste Staus: Disabled

#show ip ospf interface
eth2 is up, line protocol is up
```


© 2021 IP Infusion Inc. Proprietary

```
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:11
  Neighbor Count is 2, Adjacent neighbor count is 2
  Suppress hello for 0 neighbor(s)
  Hello received 66 sent 38, DD received 11 sent 7
  LS-Req received 2 sent 2, LS-Upd received 15 sent 14
  LS-Ack received 14 sent 10, Discarded 0
  No authentication
eth1 is up, line protocol is up
  Internet Address 10.10.11.11/24, Area 0.0.0.1, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.92, Interface Address 10.10.11.13
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.11.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 22 sent 24, DD received 3 sent 9
  LS-Req received 1 sent 1, LS-Upd received 4 sent 5
  LS-Ack received 4 sent 3, Discarded 0
  No authentication

#show ip ospf neighbor

Total number of full neighbors: 3
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/Backup     00:00:34    10.10.10.10     eth2
0
10.12.26.90       1   Full/DROther    00:00:32    10.10.10.12     eth2
0
10.12.26.92       1   Full/DR         00:00:33    10.10.11.13     eth1
0

#show ip ospf database

            OSPF Router with ID (10.12.26.89) (Process ID 100 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age     Seq#       CkSum  Link count
10.12.26.88     10.12.26.88     365     0x80000005 0x10bc 1
10.12.26.89     10.12.26.89     312     0x80000006 0x0fb8 1
10.12.26.90     10.12.26.90     363     0x80000003 0x10b8 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age     Seq#       CkSum
10.10.10.11     10.12.26.89     364     0x80000002 0xe7fd
```

```
                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#     CkSum     Route
10.10.11.0      10.12.26.89      312     0x80000001 0x95fd 10.10.11.0/24

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#     CkSum  Opaque ID
1.0.0.1         10.12.26.88      363     0x80000003 0xa972 1
1.0.0.1         10.12.26.89      362     0x80000003 0xad6c 1
1.0.0.1         10.12.26.90      363     0x80000001 0xb564 1
1.0.0.10        10.12.26.88      363     0x80000003 0x0a32 10
1.0.0.10        10.12.26.89      362     0x80000002 0x2417 10
1.0.0.10        10.12.26.90      363     0x80000001 0x3efb 10

                Router Link States (Area 0.0.0.1)

Link ID         ADV Router       Age     Seq#      CkSum  Link count
10.12.26.89     10.12.26.89      245     0x80000004 0x3d88 1
10.12.26.92     10.12.26.92      241     0x80000004 0x2698 1

                Net Link States (Area 0.0.0.1)
Link ID         ADV Router       Age     Seq#      CkSum
10.10.11.13     10.12.26.92      246     0x80000001 0x6ffb

                Summary Link States (Area 0.0.0.1)

Link ID         ADV Router       Age     Seq#      CkSum     Route
10.10.10.0      10.12.26.89      312     0x80000001 0xa0f3 10.10.10.0/24

                Area-Local Opaque-LSA (Area 0.0.0.1)

Link ID         ADV Router      Age      Seq#      CkSum  Opaque ID
1.0.0.1         10.12.26.89      243     0x80000001 0xb16a 1
1.0.0.1         10.12.26.92      244     0x80000001 0xbd58 1
1.0.0.8         10.12.26.89      234     0x80000002 0x96a2 8
1.0.0.8         10.12.26.92      244     0x80000001 0xc272 8
```

Redistribute Routes into OSPF

In this example, the configuration causes BGP routes to be imported into the OSPF routing table, and advertised as Type 5 External LSAs into Area 0.

© 2021 IP Infusion Inc. Proprietary

Topology

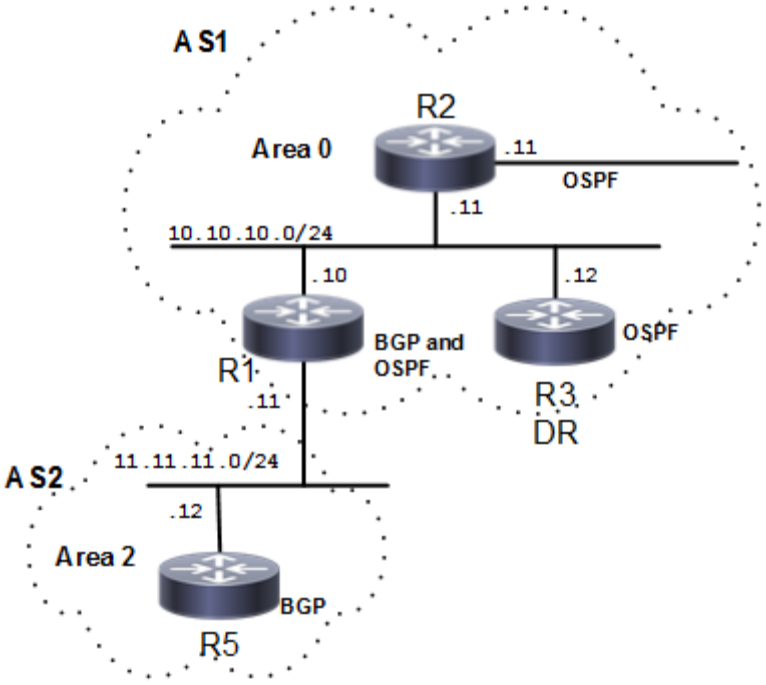


Figure 4-89: Redistribute Routes

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#redistribute bgp`	Specify redistributing routes from other routing protocol (BGP) into OSPF.

Validation

```
#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.9.0/24 [1] is directly connected, eth2, Area 0.0.0.0
C  10.10.10.0/24 [1] is directly connected, eth3, Area 0.0.0.0
O  10.10.11.0/24 [101] via 10.10.10.11, eth3, Area 0.0.0.0
C  10.10.12.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O  10.10.13.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
O  10.10.14.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
```

© 2021 IP Infusion Inc. Proprietary

Cost

A route can be made the preferred route by changing its cost. In this example, cost has been configured to make R2 the next hop for R1.

The default cost for each interface is 1. Interface eth2 on R2 has a cost of 100, and Interface eth2 on R3 has a cost of 150. The total cost to reach 10.10.14.0/24 (R4) through R2 and R3 is computed as follows:

R2: 1+100 = 101

R3: 1+150 = 151

Therefore, R1 chooses R2 as its next hop to destination 10.10.14.0/24 because it has the lower cost.

Topology

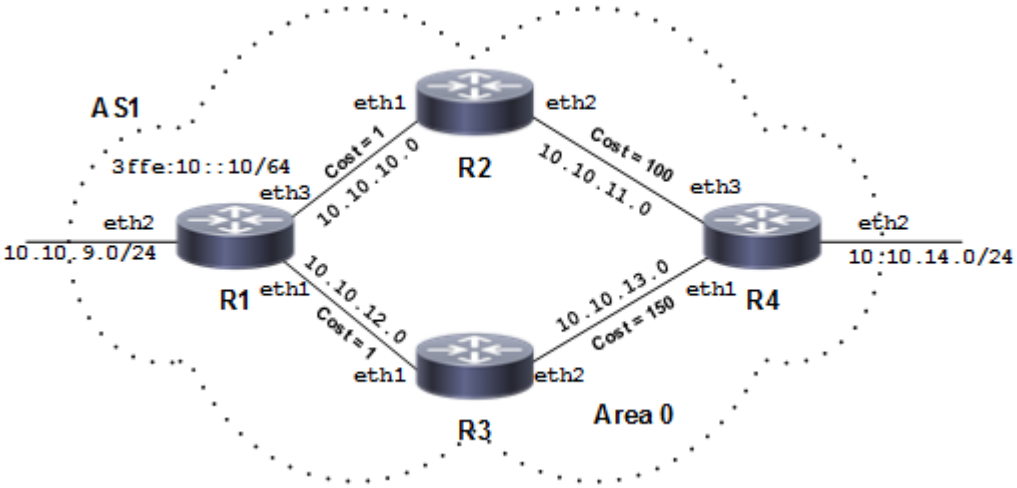


Figure 4-90: Configure Cost Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#network 10.10.9.0/24 area 0`
`(config-router)#network 10.10.10.0/24 area 0`
`(config-router)#network 10.10.12.0/24 area 0`
	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface (area ID `0` specifies the backbone area).

R2

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip ospf cost 100`	Set the OSPF cost of this link to `100`.
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 10.10.11.0/24 area 0`	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface.

R3

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip ospf cost 150`	Set the OSPF cost of this link to `100`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.12.0/24 area 0` `(config-router)#network 10.10.13.0/24 area 0`	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface.

R4

`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#network 10.10.11.0/24 area 0`
`(config-router)#network 10.10.13.0/24 area 0`
`(config-router)#network 10.10.14.0/24 area 0`
	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface.

Validation

R1

```
#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.9.0/24 [1] is directly connected, eth2, Area 0.0.0.0
C  10.10.10.0/24 [1] is directly connected, eth3, Area 0.0.0.0
O  10.10.11.0/24 [101] via 10.10.10.11, eth3, Area 0.0.0.0
C  10.10.12.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O  10.10.13.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
O  10.10.14.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0

#sh ip ospf interface
eth3 is up, line protocol is up
  Internet Address 10.10.10.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
```

```
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 43 sent 69, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 16 sent 18
  LS-Ack received 10 sent 11, Discarded 0
  No authentication
eth2 is up, line protocol is up
  Internet Address 10.10.9.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.9.10
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Hello received 0 sent 68, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
  No authentication
eth1 is up, line protocol is up
  Internet Address 10.10.12.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.12.10
  Backup Designated Router (ID) 10.12.26.90, Interface Address 10.10.12.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
Hello received 29 sent 66, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 10 sent 12
  LS-Ack received 10 sent 9, Discarded 0
  No authentication
```

R2

```
#sh ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  10.10.9.0/24 [2] via 10.10.10.10, eth1, Area 0.0.0.0
C  10.10.10.0/24 [1] is directly connected, eth1, Area 0.0.0.0
C  10.10.11.0/24 [100] is directly connected, eth2, Area 0.0.0.0
O  10.10.12.0/24 [2] via 10.10.10.10, eth1, Area 0.0.0.0
O  10.10.13.0/24 [101] via 10.10.11.11, eth2, Area 0.0.0.0
O  10.10.14.0/24 [101] via 10.10.11.11, eth2, Area 0.0.0.0

#sh ip ospf interface
```


© 2021 IP Infusion Inc. Proprietary

```
eth2 is up, line protocol is up
  Internet Address 10.10.11.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 100
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 100
  Designated Router (ID) 10.12.26.89, Interface Address 10.10.11.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.11.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 56 sent 77, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 11 sent 7
  LS-Ack received 4 sent 8, Discarded 0
  No authentication
eth1 is up, line protocol is up
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 74 sent 75, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 18 sent 16
  LS-Ack received 10 sent 12, Discarded 0
  No authentication
```

R3

```
#sh ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  10.10.9.0/24 [2] via 10.10.12.10, eth1, Area 0.0.0.0
O  10.10.10.0/24 [2] via 10.10.12.10, eth1, Area 0.0.0.0
O  10.10.11.0/24 [102] via 10.10.12.10, eth1, Area 0.0.0.0
C  10.10.12.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O  10.10.13.0/24 [103] via 10.10.12.10, eth1, Area 0.0.0.0
O  10.10.14.0/24 [103] via 10.10.12.10, eth1, Area 0.0.0.0

#sh ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.13.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.90, Network Type
BROADCAST, Cost: 150
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 150
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.13.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.13.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
```

© 2021 IP Infusion Inc. Proprietary

```
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 85 sent 94, DD received 3 sent 4
  LS-Req received 0 sent 0, LS-Upd received 3 sent 4
  LS-Ack received 3 sent 3, Discarded 0
  No authentication
eth1 is up, line protocol is up
  Internet Address 10.10.12.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.90, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.12.10
  Backup Designated Router (ID) 10.12.26.90, Interface Address 10.10.12.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 92 sent 92, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 12 sent 10
  LS-Ack received 8 sent 10, Discarded 0
  No authentication
```

R4

```
#sh ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  10.10.9.0/24 [3] via 10.10.11.10, eth3, Area 0.0.0.0
                    via 10.10.13.10, eth1, Area 0.0.0.0
O  10.10.10.0/24 [2] via 10.10.11.10, eth3, Area 0.0.0.0
C  10.10.11.0/24 [1] is directly connected, eth3, Area 0.0.0.0
O  10.10.12.0/24 [2] via 10.10.13.10, eth1, Area 0.0.0.0
C  10.10.13.0/24 [1] is directly connected, eth1, Area 0.0.0.0
C  10.10.14.0/24 [1] is directly connected, eth2, Area 0.0.0.0

#sh ip ospf interface
eth3 is up, line protocol is up
  Internet Address 10.10.11.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.92, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.89, Interface Address 10.10.11.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.11.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 95 sent 96, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 7 sent 11
  LS-Ack received 7 sent 5, Discarded 0
  No authentication
eth2 is up, line protocol is up
  Internet Address 10.10.14.10/24, Area 0.0.0.0, MTU 1500
```


© 2021 IP Infusion Inc. Proprietary

```
  Process ID 100, VRF (default), Router ID 10.12.26.92, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.92, Interface Address 10.10.14.10
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:10
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Hello received 0 sent 95, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
  No authentication
eth1 is up, line protocol is up
  Internet Address 10.10.13.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.92, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.13.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.13.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
 Hello received 92 sent 93, DD received 4 sent 3
  LS-Req received 0 sent 0, LS-Upd received 4 sent 3
  LS-Ack received 3 sent 3, Discarded 0
  No authentication
```

Virtual Links

Virtual links are used to connect a temporarily-disjointed non-backbone area to the backbone area, or to repair a non-contiguous backbone area. In this example, the ABR R3 has temporarily lost connection to Area 0, in turn, disconnecting Area 2 from the backbone area. The virtual link between ABR R1 and ABR R2 connects Area 2 to Area 0. Area 1 is used as a transit area.

Topology

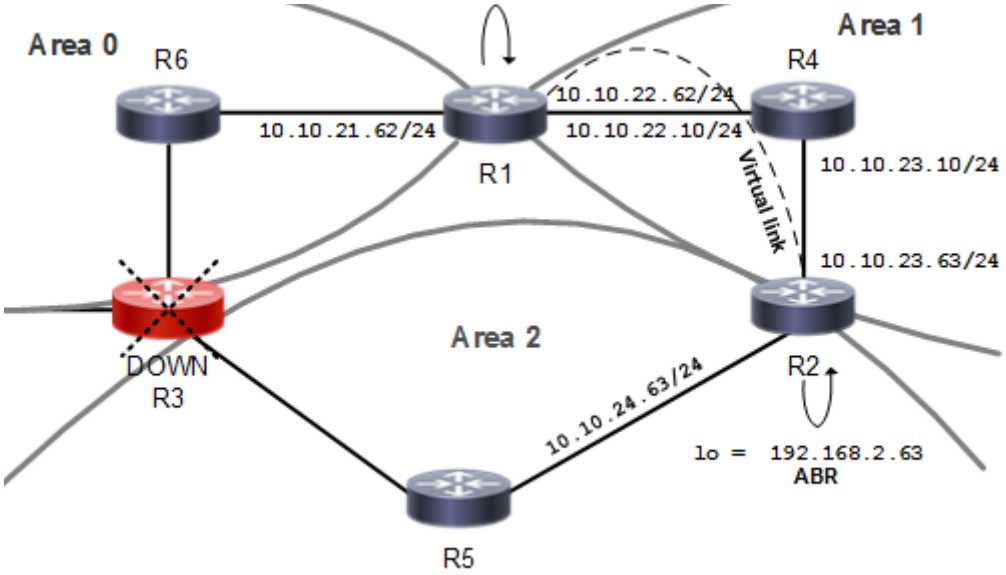


Figure 4-91: Virtual Links Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify loopback as the interface you want to configure.
`(config-if)#ip address 192.168.1.62/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#ospf router-id 192.168.1.62`	Configure the OSPF Router ID (`192.168.1.62`) for this router.
`(config-router)#network 10.10.21.0/24 area 0` `(config-router)#network 10.10.22.0/24 area 1`	Define interfaces on which OSPF runs, and associate the area IDs `(0 and 1)` with the interface.
`(config-router)#area 1 virtual-link 192.168.2.63`	Configure a virtual link between this router R1 and R2 (Router ID `192.168.2.63`) through transit area 1.

R2

`(config)#interface lo`	Specify loopback as the interface you want to configure.
`(config-if)#ip address 192.168.2.63/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#ospf router-id 192.168.2.63`	Configure the OSPF Router ID (`192.168.1.63`) for this router.

© 2021 IP Infusion Inc. Proprietary

`(config-router)#network 10.10.23.0/24 area 1`
`(config-router)#network 10.10.24.0/24 area 2`
`(config-router)#network 192.168.2.63/32 area 2`
	Define interfaces on which OSPF runs, and associate the area IDs `(1 and 2)` with the interface.

`(config-router)#area 1 virtual-link 192.168.1.62`	Configure a virtual link between this router R2 and R1 (Router ID `192.168.2.62`) through transit area `1`.

Validation

```
R1#show ip ospf virtual-links
Virtual Link VLINK0 to router 2.2.2.2 is up
  Transit area 0.0.0.1 via interface eth2
  Hello suppression enabled
  DoNotAge LSA allowed
  Local address 13.13.13.1/32
  Remote address 12.12.12.1/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  No authentication
    Adjacency state Down

R2#show ip ospf virtual-links
Virtual Link VLINK0 to router 1.1.1.1 is up
  Transit area 0.0.0.1 via interface eth1
  Hello suppression enabled
  DoNotAge LSA allowed
  Local address 12.12.12.1/32
  Remote address 13.13.13.1/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  No authentication
    Adjacency state Init

R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
192.168.20.5      1   Full/DR         00:00:34    13.13.13.2      eth2
0


R2#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
192.168.20.5      1   Full/DR         00:00:36    12.12.12.2      eth1
0
1.1.1.1           1   Init/ -           00:00:32    13.13.13.1      VLINK0
R1#show ip ospf route
```

```
OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

IA 2.2.2.2/32 [12] via 13.13.13.2, eth2, Area 0.0.0.1
O  12.12.12.0/24 [2] via 13.13.13.2, eth2, Area 0.0.0.1
C  13.13.13.0/24 [1] is directly connected, eth2, Area 0.0.0.1

R2#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  2.2.2.2/32 [10] is directly connected, lo, Area 0.0.0.2
C  12.12.12.0/24 [1] is directly connected, eth1, Area 0.0.0.1
O  13.13.13.0/24 [2] via 12.12.12.2, eth1, Area 0.0.0.1

R1#show ip ospf
 Routing Process "ospf 100" with ID 1.1.1.1
 Process uptime is 39 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 6
 Number of LSA received 15
 Number of areas attached to this router: 2
MemPool - struct ospf lsa             : (0-16) | Total (16/100000)
blk_size:160
MemPool - struct rxmt                 : | Total (0/0) blk_size:8
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 0
        Area has no authentication
        SPF algorithm last executed 00:10:05.434 ago
        SPF algorithm executed 1 times
        Number of LSA 3. Checksum 0x01bf9c
    Area 0.0.0.1
```


© 2021 IP Infusion Inc. Proprietary

```
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Number of fully adjacent virtual neighbors through this area is 0
        Area has no authentication
        SPF algorithm last executed 00:09:57.432 ago
        SPF algorithm executed 7 times
        Number of LSA 13. Checksum 0x076e78
 Dste Staus: Disabled

R2#show ip ospf
 Routing Process "ospf 100" with ID 2.2.2.2
 Process uptime is 16 hours 48 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 11
 Number of LSA received 12
 Number of areas attached to this router: 3
MemPool - struct ospf lsa             : (0-20) | Total (20/100000)
blk_size:160
MemPool - struct rxmt                 : | Total (0/0) blk_size:8
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 0
        Area has no authentication
        SPF algorithm last executed 00:11:05.618 ago
        SPF algorithm executed 1 times
        Number of LSA 4. Checksum 0x018ce2
    Area 0.0.0.1
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Number of fully adjacent virtual neighbors through this area is 0
        Area has no authentication
        SPF algorithm last executed 00:11:03.619 ago
        SPF algorithm executed 6 times
        Number of LSA 13. Checksum 0x076e78
    Area 0.0.0.2
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 0
        Number of fully adjacent virtual neighbors through this area is 0
```

```
        Area has no authentication
        SPF algorithm last executed 00:11:05.618 ago
        SPF algorithm executed 3 times
        Number of LSA 3. Checksum 0x0139cf
Dste Staus: Disabled
```

OSPF Authentication

There are three types of OSPF authentications--Null (Type 0), Simple Text (Type 1), and MD5 (Type 2). With Null authentication, routing exchanges over the network are not authenticated. In Simple Text authentication, the authentication type is the same for all routers that communicate using OSPF in a network. For MD5 authentication, configure a key and a key ID on each router. The router generates a message digest on the basis of the key, key ID, and OSPF packet, and adds it to the OSPF packet.

The authentication type can be configured on a per-interface basis or a per-area basis. Additionally, Interface and Area authentication can be used together. Area authentication is used for an area, and interface authentication is used for a specific interface in the area. If the Interface authentication type is different from the Area authentication type, the Interface authentication type overrides the Area authentication type. If the Authentication type is not specified for an interface, the Authentication type for the area is used. The authentication command descriptions contain details of each type of authentication.

In the example below, R1 and R2 are configured for both the interface and area authentications. The authentication type of interface eth1 on R1 and interface eth0 on R2 is MD5 mode, and is defined by the area authentication command; however, the authentication type of interface eth2 on R1 and interface eth1 on R2 is plain text mode, and is defined by the `ip ospf authentication` command. This interface command overrides the `area authentication` command.

Topology

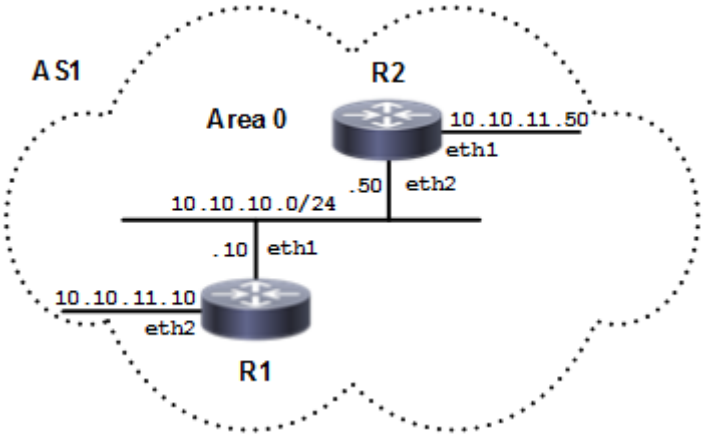


Figure 4-92: OSPF Authentication Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.

© 2021 IP Infusion Inc. Proprietary

(config-router)#network 10.10.10.0/24 area 0 (config-router)#network 10.10.11.0/24 area 0	Define interfaces on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#area 0 authentication message-digest	Enable MD5 authentication on area 0.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip ospf message-digest-key 1 md5 test	Register the MD5 key test for OSPF authentication. The key ID is 1.
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode.
(config-if)#ip ospf authentication	Enable the OSPF packet to use text authentication on the current interface (eth2).
(config-if)#ip ospf authentication-key test	Specify an OSPF authentication password (test) for the neighboring routers.

R2

#configure terminal	Enter configure mode.
(config)#router ospf 100	Configure the routing process, and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 10.10.10.0/24 area 0 (config-router)#network 10.10.11.0/24 area 0	Define interfaces on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#area 0 authentication message-digest	Enable MD5 authentication on area 0.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip ospf message-digest-key 1 md5 test	Register MD5 key test for OSPF authentication. The key ID is 1.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip ospf authentication	Enable the OSPF packet to use text authentication on the current interface (eth1).
(config-if)#ip ospf authentication-key test	Specify an OSPF authentication password test for the neighboring routers.

Validation

R1

```
R1#sh running-config
!
no service password-encryption
!
hostname R1
!
logging monitor 7
```

```
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.88/24
!
interface eth1
 ip address 10.10.10.10/24
 ip ospf message-digest-key 1 md5 0x293da85becc67703
!
interface eth2
 ip address 10.10.11.10/24
 ip ospf authentication
 ip ospf authentication-key 0x293da85becc67703
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
interface eth7
!
router ospf 100
 area 0.0.0.0 authentication message-digest
 network 10.10.9.0/24 area 0.0.0.0
 network 10.10.10.0/24 area 0.0.0.0
 network 10.10.11.0/24 area 0.0.0.0
 network 10.10.12.0/24 area 0.0.0.0
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end


R1#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address         Interface
Instance ID
```


© 2021 IP Infusion Inc. Proprietary

```
10.12.26.89     1   Full/DR        00:00:38   10.10.10.50    eth1
0
```

R2

```
R2#sh running-config
!
no service password-encryption
!
hostname R2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.89/24
!
interface eth1
 ip address 10.10.11.50/24
 ip ospf authentication
 ip ospf authentication-key 0x293da85becc67703
!
interface eth2
 ip address 10.10.10.50/24
 ip ospf message-digest-key 1 md5 0x293da85becc67703
 ip ospf cost 100
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
router ospf 100
 area 0.0.0.0 authentication message-digest
 network 10.10.10.0/24 area 0.0.0.0
 network 10.10.11.0/24 area 0.0.0.0
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end
```

© 2021 IP Infusion Inc. Proprietary

```
R2#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/Backup     00:00:33    10.10.10.10     eth2
0
```

Multiple OSPF Instances

By using multiple OSPF instances, OSPF routes can be segregated, based on their instance number. Routes of one instance are stored differently from routes of another instance running in the same router.

To configure multiple OSPF instances, perform the following procedures referring to the topology diagram below:

1. Enable OSPF on an interface.
2. Enable multiple instances.
3. Configure redistribution among multiple instances.

   Note: Optionally, redistribution can be configured with the metric, type or route-map options.

Topology

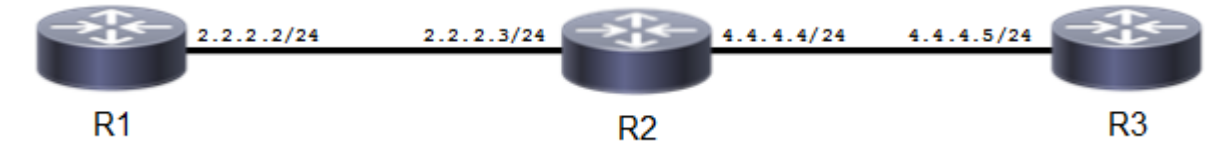


Figure 4-93: Multiple OSPF Instances

© 2021 IP Infusion Inc. Proprietary

Enable Multiple OSPF Instances on a Router

In this example, routers R1, R2, and R3 are in Area 0, and all run OSPF.

R1

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ip address 2.2.2.2/24`	Specify the IP address of the interface.
`(config-if)#no shutdown`	Activate the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 10`	Configure an OSPF instance with an instance ID of `10`.
`(config-router)#router-id 5.5.5.5`	Configure the router ID to use on this instance.
`(config-router)#network 2.2.2.0/24 area 0`	Advertise the network with the area ID.

R2

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ip address 2.2.2.3/24`	Specify the IP address of the interface.
`(config-if)#no shutdown`	Activate the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 10`	Configure an OSPF instance with an instance ID of `10`.
`(config-router)#router-id 6.6.6.6`	Configure the router ID to use on this instance.
`(config-router)#network 2.2.2.0/24 area 0`	Advertise the network with the area ID.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth2`	Enter interface mode for `eth2`.
`(config-if)#ip address 4.4.4.4/24`	Configure the IP address.
`(config-if)#no shutdown`	Activate the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 15`	Configure an OSPF instance with an instance ID of `15`.
`(config-router)#router-id 8.8.8.8`	Configure the router ID to use on this instance.
`(config-router)#network 4.4.4.0/24 area 0`	Advertise the network with the area ID.

R3

`(config)#``interface eth1`	Enter interface mode for `eth1`.
`(config-if)#``ip address 4.4.4.5/24`	Configure the IP address.
`(config-if)#``no shutdown`	Activate the interface.
`(config-if)#``exit`	Exit interface mode.
`(config)#``router ospf 15`	Configure an OSPF instance with an instance ID of `15`.
`(config-router)#``router-id 7.7.7.7`	Configure the router ID to use on this instance.
`(config-router)#``network 4.4.4.0/24 area 0`	Advertise the network with the area ID.

© 2021 IP Infusion Inc. Proprietary

Validation

R1

```
R1#sh running-config
!
no service password-encryption
!
hostname R1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.88/24
!
interface eth1
 ip address 2.2.2.2/24
!
interface eth2
 ip address 10.10.11.10/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
interface eth7
!
router ospf 10
 ospf router-id 5.5.5.5
 network 2.2.2.0/24 area 0.0.0.0
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end

R1#sh ip ospf neighbor
```


© 2021 IP Infusion Inc. Proprietary

```
Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
6.6.6.6           1   Full/Backup     00:00:39    2.2.2.3         eth1
0

R1#sh ip ospf route

OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0
```

R2

```
R2#sh running-config
!
no service password-encryption
!
hostname R2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.89/24
!
interface eth1
 ip address 2.2.2.3/24
!
interface eth2
 ip address 4.4.4.4/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
router ospf 10
 ospf router-id 6.6.6.6
 network 2.2.2.0/24 area 0.0.0.0
cspf disable-better-protection
```

```
!
router ospf 15
 ospf router-id 8.8.8.8
 network 4.4.4.0/24 area 0.0.0.0
 no capability cspf
!
line con 0
 login
line vty 0 39
 login
!
end

R2#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
5.5.5.5           1   Full/DR         00:00:33    2.2.2.2         eth1
0

Total number of full neighbors: 1
OSPF process 15 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
7.7.7.7           1   Full/Backup     00:00:31    4.4.4.5         eth2
0

R2#sh ip ospf route

OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0

OSPF process 15:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  4.4.4.0/24 [1] is directly connected, eth2, Area 0.0.0.0
```

R3

```
R3#sh running-config
!
no service password-encryption
!
hostname R3
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
```


© 2021 IP Infusion Inc. Proprietary

```
!
ip pim register-rp-reachability
!
interface lo
 mtu 65536
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface eth0
 ip address 10.12.26.90/24
!
interface eth1
 ip address 4.4.4.5/24
!
interface eth2
 ip address 10.10.13.10/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
router ospf 15
 ospf router-id 7.7.7.7
 network 4.4.4.0/24 area 0.0.0.0
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end

R3#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 15 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
8.8.8.8           1   Full/DR         00:00:30    4.4.4.4         eth1
0
```

Redistribute among Multiple Instances

In this example, routes of one instance are redistributed to another instance to enable ping from R1 to R3 or vice versa; and R2 redistributes routes from one instance to another.

R2

`(config)#router ospf 15`	Configure an OSPF instance with instance ID `15`.
`(config-router)#router-id 8.8.8.8`	Configure the router ID.

(config-router)#redistribute ospf 10	Redistribute instance 10 routes.
(config-router)#redistribute connected	Redistribute connected routes to instance 15.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 10	Configure an OSPF instance with instance ID 10.
(config-router)#router-id 6.6.6.6	Configure the router ID.
(config-router)#redistribute ospf 15	Redistribute instance 15 routes.
(config-router)#redistribute connected	Redistribute connected routes to instance 10.

Redistribute with the Metric Option

In this example, on R3, R1 and R2 have each other's routes with a metric of 100.

R2

(config)#router ospf 15	Configure an OSPF instance with instance ID 15.
(config-router)#router-id 8.8.8.8	Configure the router ID.
(config-router)#redistribute ospf 10 metric 100	Redistribute instance 10 routes with metric 100.
(config-router)#redistribute connected	Redistribute connected routes to instance 15.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 10	Configure an OSPF instance with instance ID 10.
(config-router)#router-id 6.6.6.6	Configure the router ID.
(config-router)#redistribute ospf 15 metric 100	Redistribute instance 15 routes with metric 100.
(config-router)#redistribute connected	Redistribute connected routes to instance 10.

Redistribute with the Type Option

In this example, on R3, R1 has R3 routes as type 2, and R2 has R1 routes as type 1.

R2

(config)#router ospf 15	Configure an OSPF instance with instance ID 15.
(config-router)#router-id 8.8.8.8	Configure the router ID.
(config-router)#redistribute ospf 10 metric-type 1	Redistribute instance 10 routes with metric-type 1.
(config-router)#redistribute connected	Redistribute connected routes to instance 15.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 10	Configure an OSPF instance with instance ID 10.
(config-router)#router-id 6.6.6.6	Configure the router ID.
(config-router)#redistribute ospf 15 metric-type 2	Redistribute instance 15 routes with type 2.
(config-router)#redistribute connected	Redistribute connected routes to instance 10.

© 2021 IP Infusion Inc. Proprietary

Redistribute with the Route-Map Option

R2

`(config)#route-map 1 permit 10`	Enter route-map mode, specifying route-map ID.
`(config-route-map)#set metric 100`	Set metric value.
`(config-route-map)#set metric-type type-2`	Set metric-type.
`(config-route-map)#exit`	Exit route-map mode.
`(config)#route-map 2 permit 10`	Enter route-map mode, specifying route-map ID.
`(config-route-map)#set metric 200`	Set metric value.
`(config-route-map)#set metric-type type-1`	Set metric-type.
`(config-route-map)#exit`	Exit route-map mode.
`(config)#router ospf 15`	Configure an OSPF instance with instance ID `15`.
`(config-router)#router-id 8.8.8.8`	Configure the router ID.
`(config-router)#redistribute ospf 10 route-map 1`	Redistribute instance `10` routes with route map `1`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 10`	Configure an OSPF instance with instance ID `10`.
`(config-router)#router-id 6.6.6.6`	Configure the router ID.
`(config-router)#redistribute ospf 15 route-map 2`	Redistribute instance `15` routes with route map `2`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `10`.

Validation

```
R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
6.6.6.6           1   Full/DR         00:00:39    2.2.2.3         eth1
0

R2#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 10 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
5.5.5.5           1   Full/Backup     00:00:35    2.2.2.2         eth1
0

Total number of full neighbors: 1
OSPF process 15 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
```

```
7.7.7.7         1   Full/Backup     00:00:36    4.4.4.5       eth2
0
R3#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 15 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
8.8.8.8         1   Full/DR         00:00:40    4.4.4.4       eth2
0
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     2.2.2.0/24 is directly connected, eth1, 00:08:40
O E1  4.4.4.0/24 [110/201] via 2.2.2.3, eth1, 00:01:18
C     5.5.5.5/32 is directly connected, lo, 00:08:41
O E2  6.6.6.6/32 [110/20] via 2.2.2.3, eth1, 00:01:10
O E2  8.8.8.8/32 [110/20] via 2.2.2.3, eth1, 00:01:10
C     127.0.0.0/8 is directly connected, lo, 00:08:44
C     192.168.20.0/24 is directly connected, eth0, 00:08:40

Gateway of last resort is not set

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     2.2.2.0/24 is directly connected, eth1, 5d00h02m
C     4.4.4.0/24 is directly connected, eth2, 5d00h02m
C     6.6.6.6/32 is directly connected, lo, 4d23h59m
C     8.8.8.8/32 is directly connected, lo, 4d23h59m
C     127.0.0.0/8 is directly connected, lo, 5d00h09m
C     192.168.20.0/24 is directly connected, eth0, 5d00h08m

Gateway of last resort is not set

R3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
```


© 2021 IP Infusion Inc. Proprietary

```
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
O E2  2.2.2.0/24 [110/20] via 4.4.4.4, eth2, 00:02:45
C     4.4.4.0/24 is directly connected, eth2, 00:07:12
C     5.5.5.5/32 is directly connected, lo, 00:16:35
O E2  6.6.6.6/32 [110/20] via 4.4.4.4, eth2, 00:02:45
O E2  8.8.8.8/32 [110/20] via 4.4.4.4, eth2, 00:02:45
C     127.0.0.0/8 is directly connected, lo, 00:16:39
C     192.168.20.0/24 is directly connected, eth0, 00:15:36

Gateway of last resort is not set

#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.9.0/24 [1] is directly connected, eth2, Area 0.0.0.0
C  10.10.10.0/24 [1] is directly connected, eth3, Area 0.0.0.0
O  10.10.11.0/24 [101] via 10.10.10.11, eth3, Area 0.0.0.0
C  10.10.12.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O  10.10.13.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
O  10.10.14.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0

R2#show route-map

route-map 1, permit, sequence 10
  Match clauses:
  Set clauses:
    metric 100
    metric-type type-2
route-map 2, permit, sequence 10
  Match clauses:
  Set clauses:
    metric 200
    metric-type type-1

R1#show ip ospf route

OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0
E1 4.4.4.0/24 [201] via 2.2.2.3, eth1
E2 6.6.6.6/32 [1/20] via 2.2.2.3, eth1
E2 8.8.8.8/32 [1/20] via 2.2.2.3, eth1
E2 192.168.20.0/24 [1/20] via 2.2.2.3, eth1

R2#show ip ospf route
```

```
OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0

OSPF process 15:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  4.4.4.0/24 [1] is directly connected, eth2, Area 0.0.0.0

R3#show ip ospf route

OSPF process 15:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

E2 2.2.2.0/24 [1/20] via 4.4.4.4, eth2
C  4.4.4.0/24 [1] is directly connected, eth2, Area 0.0.0.0
E2 6.6.6.6/32 [1/20] via 4.4.4.4, eth2
E2 8.8.8.8/32 [1/20] via 4.4.4.4, eth2
E2 192.168.20.0/24 [1/20] via 4.4.4.4, eth2
```

Multiple OSPF Instances on Same Subnet

Multiple OSPF instances can be configured on the same subnet. The OSPF instance ID supports separate OSPFv2 protocol instances. With this feature, an adjacency is formed only if the received packet's instance ID is the same as the instance ID configured for that interface.

Topology

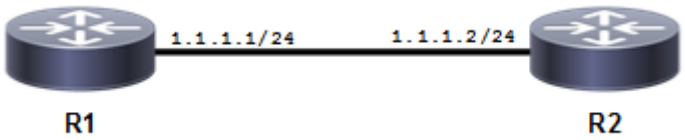


Figure 4-94: Multiple Instances on the Same Subnet

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#enable ext-ospf-multi-inst`	Enable multiple-instance capability.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of `1`.

© 2021 IP Infusion Inc. Proprietary

(config-router)#network 1.1.1.0/24 area 0 instance-id 1	Advertise the network in Area 0 with an instance ID of 1.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 2	Configure an OSPF instance with an instance ID of 2.
(config-router)#network 1.1.1.0/24 area 0 instance-id 2	Advertise the network in Area 0 with an instance ID of 2.
(config-router)#exit	Exit Router mode, and return to Configure mode.

R2

#configure terminal	Enter configure mode.
(config)#enable ext-ospf-multi-inst	Enable multiple-instance capability.
(config)#router ospf 1	Configure an OSPF instance with an instance ID of 1.
(config-router)#network 1.1.1.0/24 area 0 instance-id 1	Advertise the network in Area 0 with an instance ID of 1.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 2	Configure an OSPF instance with an instance ID of 2.
(config-router)#network 1.1.1.0/24 area 0 instance-id 2	Advertise the network in Area 0 with an instance ID of 2.
(config-router)#exit	Exit Router mode, and return to Configure mode.

Validation

R1

```
R1#show ip ospf interface
eth1 is up, line protocol is up
  Internet Address 1.1.1.1/24, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.12.26.88, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 1.1.1.1
  Backup Designated Router (ID) 10.12.26.89, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:10
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 7 sent 16, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 3 sent 5
  LS-Ack received 3 sent 3, Discarded 0
  No authentication
  Internet Address 1.1.1.1/24, Area 0.0.0.0, MTU 1500
  Process ID 2, VRF (default), Router ID 10.12.26.88, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 1.1.1.1
  Backup Designated Router (ID) 10.12.26.89, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
```

```
  Hello received 4 sent 12, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 3 sent 5
  LS-Ack received 3 sent 3, Discarded 0
  No authentication

R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address        Interface
Instance ID
10.12.26.89      1   Full/Backup    00:00:35   1.1.1.2       eth1
1

Total number of full neighbors: 1
OSPF process 2 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address        Interface
Instance ID
10.12.26.89      1   Full/Backup    00:00:33   1.1.1.2       eth1
2
```

R2

```
R2#sh ip ospf interface
eth1 is up, line protocol is up
  Internet Address 1.1.1.2/24, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.12.26.89, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 1.1.1.1
  Backup Designated Router (ID) 10.12.26.89, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 17 sent 17, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 3
  LS-Ack received 2 sent 3, Discarded 0
  No authentication
  Internet Address 1.1.1.2/24, Area 0.0.0.0, MTU 1500
  Process ID 2, VRF (default), Router ID 10.12.26.89, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 1.1.1.1
  Backup Designated Router (ID) 10.12.26.89, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 13 sent 14, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 3
  LS-Ack received 2 sent 3, Discarded 0
  No authentication

R2#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
```


© 2021 IP Infusion Inc. Proprietary

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/DR         00:00:32    1.1.1.1         eth1
1

Total number of full neighbors: 1
OSPF process 2 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/DR         00:00:37    1.1.1.1         eth1
2
```

Multi-Area Adjacency Configuration

Multiple OSPF areas for a same subnet can be configured between two routers. In the diagram below, OSPF is enabled between R2 and R3 under area 0 and area 1, though there is only one link available between these two routers. Multi-area adjacency allows establishing adjacency on multiple areas between the Area Border Routers (ABRs). The specified interface of the ABR is associated with multiple areas.

Each multi-area-adjacency internally implements point-to-point functionality, once the adjacency reaches the FULL state. This point-to-point link provides a topological path for that area. Like a virtual link, there is no restriction for multi-area adjacency that the packets always go through the backbone.

Topology

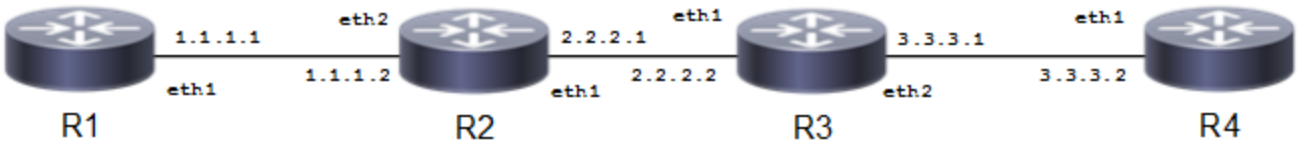


Figure 4-95: One Subnet with Multiple OSPF Areas

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of `1`.
`(config-router)#network 1.1.1.0/24 area 1`	Configure OSPF between R1 and R2 under area `1`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of `1`.
`(config-router)#network 1.1.1.0/24 area 1`	Configure OSPF between R1 and R2 under area `1`.
`(config-router)#network 2.2.2.0/24 area 0`	Configure OSPF between R2 and R3 under area `0`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 2.2.2.1/24`	Configure IP address on the interface.
`(config-if)#ip ospf 1 multi-area 0.0.0.1 neighbor 2.2.2.2`	Configure multi area adjacency.
`(config-if)#exit`	Exit interface mode.

R3

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of `1`.
`(config-router)#network 2.2.2.0/24 area 0`	Configure OSPF between R2 and R3 under area `0`.
`(config-router)#network 3.3.3.0/24 area 1`	Configure OSPF between R3 and R4 under area `1`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 2.2.2.2/24`	Configure IP address on the interface.
`(config-if)#ip ospf 1 multi-area 0.0.0.1 neighbor 2.2.2.1`	Configure multi area adjacency.
`(config-if)#exit`	Exit interface mode.

R4

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of `1`.
`(config-router)#network 3.3.3.0/24 area 1`	Configure OSPF between R3 and R4 under area `1`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.

Validation

show ip ospf multi-area-adjacencies, show ip ospf neighbor, show ip ospf route, show ip route

R2

```
R2#show ip ospf multi-area-adjacencies
  Multi-area-adjacency link on interface eth1 to neighbor 2.2.2.2
  Internet Address 2.2.2.1/24, Area 0.0.0.1, MTU 1500
  Process ID 1, Router ID 10.12.26.89, Network Type POINTTOPOINT, Cost: 1
  Transmit Delay is 1 sec, State Point-To-Point, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 16 sent 53, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 10 sent 5
  LS-Ack received 3 sent 9, Discarded 0

R2#show ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
```


© 2021 IP Infusion Inc. Proprietary

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/DR         00:00:35    1.1.1.1         eth2
0
10.12.26.90       1   Full/Backup     00:00:33    2.2.2.2         eth1
0
10.12.26.90         1   Full/ -           00:00:35    2.2.2.2         eth1

R2#show ip ospf route

OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  1.1.1.0/24 [1] is directly connected, eth2, Area 0.0.0.1
C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O  3.3.3.0/24 [2] via 2.2.2.2, eth1, Area 0.0.0.1


R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
C       1.1.1.0/24 is directly connected, eth2
C       2.2.2.0/24 is directly connected, eth1
O       3.3.3.0/24 [110/2] via 2.2.2.2, eth1, 00:05:44
C       10.12.26.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set
```

R3

```
R3#show ip ospf multi-area-adjacencies
  Multi-area-adjacency link on interface eth1 to neighbor 2.2.2.1
  Internet Address 2.2.2.2/24, Area 0.0.0.1, MTU 1500
  Process ID 1, Router ID 10.12.26.90, Network Type POINTTOPOINT, Cost: 1
  Transmit Delay is 1 sec, State Point-To-Point, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 41 sent 41, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 10
  LS-Ack received 8 sent 3, Discarded 0

R3#sh ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
```

```
10.12.26.89      1   Full/DR         00:00:39    2.2.2.1       eth1
0
10.12.26.92      1   Full/Backup     00:00:36    3.3.3.2       eth2
0
10.12.26.89       1    Full/ -          00:00:30    2.2.2.1         eth1
R3#sh ip ospf route

OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  1.1.1.0/24 [2] via 2.2.2.1, eth1, Area 0.0.0.1
C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0
C  3.3.3.0/24 [1] is directly connected, eth2, Area 0.0.0.1

R3#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

IP Route Table for VRF "default"
O       1.1.1.0/24 [110/2] via 2.2.2.1, eth1, 00:07:31
C       2.2.2.0/24 is directly connected, eth1
C       3.3.3.0/24 is directly connected, eth2
C       10.12.26.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set
```

LSA Throttling

This section contains basic OSPF LSA throttling configuration examples.

The OSPF Link-State Advertisement (LSA) throttling feature provides a mechanism to dynamically slow down link-state advertisement (LSA) updates in OSPF during times of network instability. It also allows faster OSPF convergence by providing LSA rate limiting in milliseconds, when the network is stable.

How OSPF LSA Throttling Works

The `timers throttle lsa all` command controls the generation (sending) of LSAs. The first LSA is always generated immediately upon an OSPF topology change, and the next LSA generated is controlled by the minimum start interval. The subsequent LSAs generated for the same LSA are rate-limited until the maximum interval is reached. The “same LSA” is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID.

The `timers lsa arrival` command controls the minimum interval for accepting the same LSA. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped. It is recommended that the arrival interval be less than or equal to the hold-time interval of the `timers throttle lsa all` command.

© 2021 IP Infusion Inc. Proprietary

Topology

The diagram shows the minimum configuration required to enable OSPF LSA Throttling Timers feature. R1 and R2 are two routers in Area 0 connecting to network 10.10.10.0/24.

Note: Configure one interface so that it belongs to only one area. It is possible, however, to configure different interfaces on a router to belong to different areas.

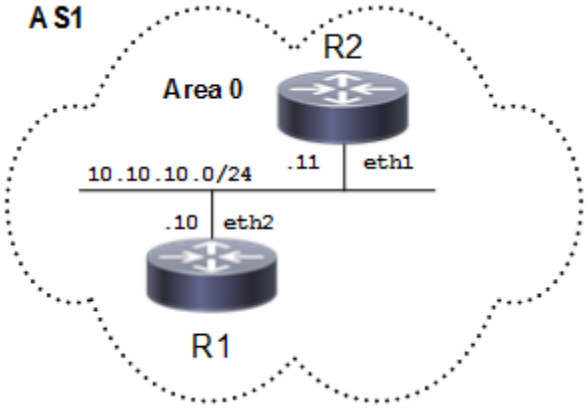


Figure 4-96: Basic OSPF Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface loopback to configure.
`(config-if)#ip address 1.1.1.1/32`	Configure the ip address (1.1.1.1) to interface loopback.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (`1`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#network 1.1.1.1/32 area 0`	Define the interface (`1.1.1.1/32`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#timers throttle lsa all 10000 20000 45000`	Configure LSA Throttling timers (Starting interval: <0-600000>, Min Hold Interval: <1-600000> and Max Wait Interval:< 1-600000>) in milliseconds. The Default value for corresponding timers are: Starting interval: 0, Min Hold Interval: 5 sec and Max Wait Interval: 5 sec.
`(config-router)#logging monitor 7`	Enable logging monitor globally.
`(config-router)#logging level ospf 7`	Enable logging level ospf globally.
`(config-router)#end`	Exit router mode

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID `(1)`. The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface `(10.10.10.0/24)` on which OSPF runs, and associate the area ID `(0)` with the interface.

Validation

R1

Check the output of `show ip ospf` and verify the initial throttle delay, minimum hold time for LSA throttle and maximum wait time for LSA throttle.

```
#show ip ospf 1
 Routing Process "ospf 1" with ID 1.1.1.1
 Process uptime is 11 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 10 secs 0 msecs
 Minimum hold time for LSA throttle 20 secs 0 msecs
 Maximum wait time for LSA throttle 45 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 4
 Number of LSA received 4
 Number of areas attached to this router: 1
MemPool - struct ospf lsa             : (0-8) | Total (8/100000) blk_size:160
MemPool - struct rxmt                 : | Total (0/0) blk_size:8
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 2(2)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:10:12.807 ago
        SPF algorithm executed 5 times
        Number of LSA 7. Checksum 0x02c480
 Dste Staus: Disabled


#show ip ospf neighbor
```


© 2021 IP Infusion Inc. Proprietary

```
Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID  Pri State       Dead Time  Address     Interface Instance ID
3.1.1.1      1   Full/Backup 00:00:34   10.10.10.11   eth1       0


#debug ospf database-timer rate-limit

#show debugging ospf
OSPF debugging status:
  OSPF rate limit timer events debugging is on
```

Here, we administratively shutdown and then bring up the loopback interface to generate Rate Limit Timer events for OSPF debugging to capture.

```
(config)#int lo
(config-if)#shutdown
2019 Mar 29 16:32:36.838 : OcNOS : OSPF : NOTIF : [OSPF_OPR_LINK_DOWN_4]:
Received Link down for interface: lo
2019 Mar 29 16:32:36.838 : OcNOS : OSPF : INFO : Starting Rate Limit Timer for
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: with 10000 msec delay
2019 Mar 29 16:32:36.838 : OcNOS : OSPF : NOTIF : [OSPF_OPR_STATE_4]:
[lo:1.1.1.1]: Status change Loopback -> Down

(config-if)#no shutdown
2019 Mar 29 16:32:42.705 : OcNOS : OSPF : NOTIF : [OSPF_OPR_LINK_UP_4]:
Received Link up for  interface: lo
2019 Mar 29 16:32:42.705 : OcNOS : OSPF : NOTIF : [OSPF_OPR_STATE_4]:
[lo:1.1.1.1]: Status change Down -> Loopback
2019 Mar 29 16:32:46.853 : OcNOS : OSPF : INFO : Rate Limit Timer for
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: expired
2019 Mar 29 16:32:46.853 : OcNOS : OSPF : INFO : For Next Instance of
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: generation wait 20000 msec


(config-if)#shutdown
2019 Mar 29 16:32:54.353 : OcNOS : OSPF : NOTIF : [OSPF_OPR_LINK_DOWN_4]:
Received Link down for interface: lo
2019 Mar 29 16:32:54.353 : OcNOS : OSPF : INFO : Starting Rate Limit Timer for
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: with 12499 msec delay
2019 Mar 29 16:32:54.353 : OcNOS : OSPF : NOTIF : [OSPF_OPR_STATE_4]:
[lo:1.1.1.1]: Status change Loopback -> Down

(config-if)#no shutdown
2019 Mar 29 16:32:59.252 : OcNOS : OSPF : NOTIF : [OSPF_OPR_LINK_UP_4]:
Received Link up for  interface: lo
2019 Mar 29 16:32:59.252 : OcNOS : OSPF : NOTIF : [OSPF_OPR_STATE_4]:
[lo:1.1.1.1]: Status change Down -> Loopback
2019 Mar 29 16:33:06.870 : OcNOS : OSPF : INFO : Rate Limit Timer for
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: expired
2019 Mar 29 16:33:06.870 : OcNOS : OSPF : INFO : For Next Instance of
LSA[0.0.0.0:Type1:1.1.1.1:(self)]: generation wait 40000 msec
```

R2

Check the output of "`show ip ospf neighbor`" and verify that OSPF adjacency is up.

```
#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
```

```
Neighbor ID  Pri  State     Dead Time   Address    Interface  Instance ID
1.1.1.1      1    Full/DR   00:00:33    10.10.10.10   eth1       0
```

Check the output of `show ip ospf database` and verify that LSA (router LSA in this example) is updated according to the configured LSA throttling timers configured on its neighbor.

```
#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum  Link count
3.1.1.1         3.1.1.1          373     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           71     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum
10.10.10.10     1.1.1.1          375     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#      CkSum  Opaque ID
1.0.0.1         3.1.1.1          372     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          373     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          372     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          373     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum  Link count
3.1.1.1         3.1.1.1          378     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           76     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum
10.10.10.10     1.1.1.1          380     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router       Age      Seq#     CkSum Opaque ID
1.0.0.1         3.1.1.1          377     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          378     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          377     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          378     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)
```


© 2021 IP Infusion Inc. Proprietary

```
                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum  Link count
3.1.1.1         3.1.1.1          380     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           78     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum
10.10.10.10     1.1.1.1          382     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#      CkSum  Opaque ID
1.0.0.1         3.1.1.1          379     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          380     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          379     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          380     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum  Link count
3.1.1.1         3.1.1.1          381     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           79     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum
10.10.10.10     1.1.1.1          383     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#      CkSum  Opaque ID
1.0.0.1         3.1.1.1          380     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          381     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          380     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          381     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum  Link count
3.1.1.1         3.1.1.1          382     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           80     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)
```

```
Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1          384     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1          381     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          382     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          381     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          382     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1          383     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1           81     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1          385     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1          382     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1          383     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1          382     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1          383     0x80000001 0x566c 8
```

Configure OSPF LSA Arrival Timers

The diagram shows the minimum configuration required to enable OSPF Minimum LSA Arrival Timers feature. R1 and R2 are two routers in Area 0 connecting to network 10.10.10.0/24.

Note: Configure one interface so that it belongs to only one area. It is possible, however, to configure different interfaces on a router to belong to different areas.

© 2021 IP Infusion Inc. Proprietary

Topology

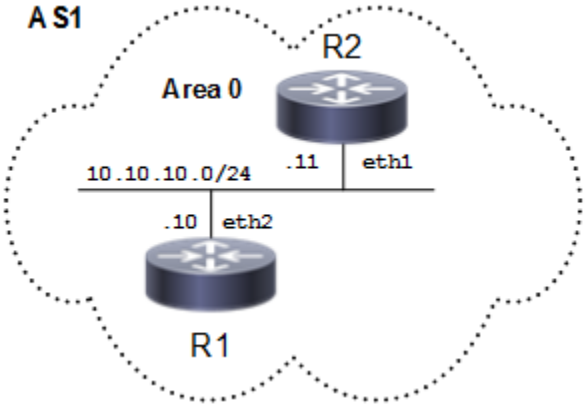


Figure 4-97: Basic OSPF Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface loopback to configure.
`(config-if)#ip address 1.1.1.1/32`	Configure the ip address (1.1.1.1) to interface loopback.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (`1`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#network 1.1.1.1/32 area 0`	Define the interface (`1.1.1.1/32`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#end`	Exit router mode

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID `(1)`. The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#network 10.10.10.0/24 area 0`	Define the interface `(10.10.10.0/24)` on which OSPF runs, and associate the area ID `(0)` with the interface.
`(config-router)#timers lsa arrival 100000`	Configure Minimum LSA Arrival timers (Minimum LSA arrival Interval:< 0-600000>) in milliseconds. The Default value for Minimum LSA Arrival timer is: 1 sec.

Validation

R1

Check the output of `show ip ospf` and verify that the minimum LSA arrival timer by default is set to 1 sec.

```
#show ip ospf
 Routing Process "ospf 1" with ID 1.1.1.1
 Process uptime is 11 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 10 secs 0 msecs
 Minimum hold time for LSA throttle 20 secs 0 msecs
 Maximum wait time for LSA throttle 45 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 4
 Number of LSA received 4
 Number of areas attached to this router: 1
MemPool - struct ospf lsa             : (0-8) | Total (8/100000) blk_size:160
MemPool - struct rxmt                 : | Total (0/0) blk_size:8
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 2(2)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:10:12.807 ago
        SPF algorithm executed 5 times
        Number of LSA 7. Checksum 0x02c480
 Dste Staus: Disabled

#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address         Interface
Instance ID
3.1.1.1          1   Full/Backup      00:00:34    10.10.10.11     eth1
```


© 2021 IP Infusion Inc. Proprietary

R2

Check the output of `show ip ospf` and verify that the minimum LSA arrival timer is set to 100 sec.

```
#show ip ospf
 Routing Process "ospf 1" with ID 3.1.1.1
 Process uptime is 23 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 100 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 3
 Number of LSA received 10
 Number of areas attached to this router: 1
MemPool - struct ospf lsa             : (0-9) | Total (9/100000) blk_size:160
MemPool - struct rxmt                 : | Total (0/0) blk_size:8
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:22:12.911 ago
        SPF algorithm executed 4 times
        Number of LSA 7. Checksum 0x02c281
 Dste Staus: Disabled
```

Check the output of show ip ospf neighbor and verify that OSPF adjacency is up.

```
#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/DR         00:00:35    10.10.10.10     eth1
0
```

Check the output of “show ip ospf database” and verify that LSA is accepted only after a time difference of 100 sec between two consecutive LSAs.

```
#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)
```

```
Link ID         ADV Router       Age     Seq#      CkSum  Link count
3.1.1.1         3.1.1.1         1131     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          829     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum
10.10.10.10     1.1.1.1         1133     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#      CkSum  Opaque ID
1.0.0.1         3.1.1.1         1130     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1131     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1130     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1131     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum  Link count
3.1.1.1         3.1.1.1         1132     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          831     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum
10.10.10.10     1.1.1.1         1134     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#      CkSum  Opaque ID
1.0.0.1         3.1.1.1         1131     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1132     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1131     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1132     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum  Link count
3.1.1.1         3.1.1.1         1133     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          831     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum
10.10.10.10     1.1.1.1         1135     0x80000001 0x18e5
```


© 2021 IP Infusion Inc. Proprietary

```
                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1         1132     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1133     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1132     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1133     0x80000001 0x566c 8


#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1         1134     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          832     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1         1136     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1         1133     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1134     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1133     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1134     0x80000001 0x566c 8
#
#show ip ospf database

            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum  Link count
3.1.1.1         3.1.1.1         1135     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          834     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#       CkSum
10.10.10.10     1.1.1.1         1137     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
1.0.0.1         3.1.1.1         1134     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1135     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1134     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1135     0x80000001 0x566c 8


#show ip ospf database
```

```
            OSPF Router with ID (3.1.1.1) (Process ID 1 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum  Link count
3.1.1.1         3.1.1.1         1136     0x80000004 0xc60c 1
1.1.1.1         1.1.1.1          834     0x80000008 0xb9f2 2

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router       Age     Seq#      CkSum
10.10.10.10     1.1.1.1         1138     0x80000001 0x18e5

                Area-Local Opaque-LSA (Area 0.0.0.0)

Link ID         ADV Router      Age      Seq#      CkSum  Opaque ID
1.0.0.1         3.1.1.1         1135     0x80000001 0x2cf6 1
1.0.0.1         1.1.1.1         1136     0x80000001 0x2af6 1
1.0.0.8         3.1.1.1         1135     0x80000001 0x7d45 8
1.0.0.8         1.1.1.1         1136     0x80000001 0x566c 8
```

Loop-Free Alternate Fast Reroute

This section contains basic OSPF Loop-Free Alternate Fast Reroute (LFA-FRR) configuration examples.

Overview

The goal of (LFA-FRR) is to reduce failure reaction time to 10s of milliseconds by using a pre-computed alternate next-hop in the event that the currently selected primary next-hop fails, so that the alternate can be rapidly used when the failure is detected. A network with this feature experiences less traffic loss and less micro-looping of packets than a network without LFA-FRR.

After enabling LFA-FRR on routers, routers calculate a backup path for each primary path to reach the destination.The backup path is calculated based on the attributes such as node protecting, link protecting, broadcast-link protecting and secondary path.

OSPF LFA and ISIS LFA along with MPLS is not supported. Do not configure OSPF LFA or ISIS LFA, if MPLS is configured or vice-versa.

Topol ogy

The diagram shows the configuration required to enable the OSPF LFA feature.

© 2021 IP Infusion Inc. Proprietary

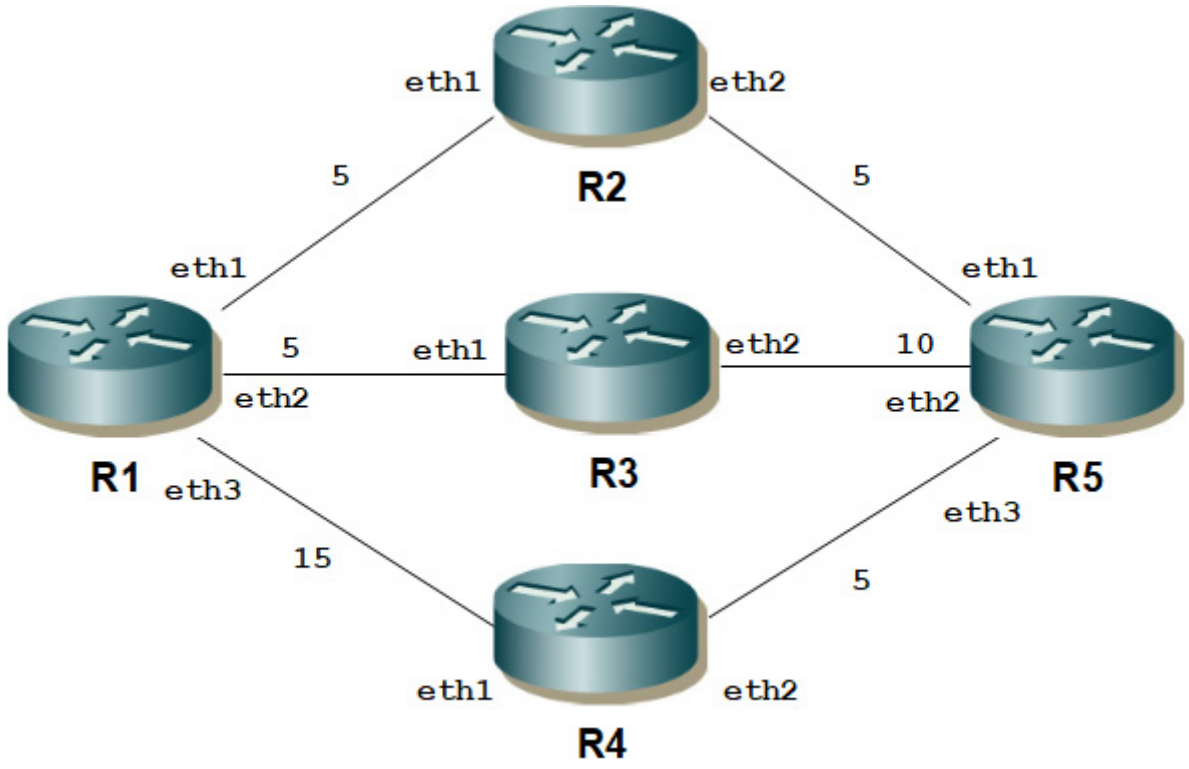


Figure 4-98: Figure 4-13: Basic OSPF-LFA Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#int eth1`	Enter interface mode.
`(config-if)#ip address 10.1.1.1/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth2`	Enter interface mode.
`(config-if)#ip address 20.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#int eth3`	Enter interface mode.
`(config-if)#ip address 30.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process and specify the Process ID (1).
`(config-router)#network 10.1.1.0/24 area 0`	Define the interface (10.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 20.1.1.0/24 area 0`	Define the interface (20.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).

© 2021 IP Infusion Inc. Proprietary

(config-router)#network 30.1.1.0/24 area 0	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#fast-reroute keep-all- paths	Configure LFA-FRR to calculate the available backup path.
(config-router)#end	Exit router mode.

R2

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Configure the IP address of the interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 40.1.1.1/24	Configure the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 10.1.1.0/24 area 0	Define the interface (20.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 40.1.1.0/24 area 0	Define the interface (40.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#end	Exit router mode.

R3

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Configure the IP address of the interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 50.1.1.1/24	Configure the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 20.1.1.0/24 area 0	Define the interface (20.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 50.1.1.0/24 area 0	Define the interface (50.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#end	Exit router mode.

© 2021 IP Infusion Inc. Proprietary

R4

`#configure terminal`	Enter configure mode.
`(config)#int eth1`	Enter interface mode.
`(config-if)#ip address 30.1.1.2/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth2`	Enter interface mode.
`(config-if)#ip address 60.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 30.1.1.0/24 area 0`	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 60.1.1.0/24 area 0`	Define the interface (60.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#end`	Exit router mode.

© 2021 IP Infusion Inc. Proprietary

R5

`#configure terminal`	Enter configure mode.
`(config)#int eth1`	Enter interface mode.
`(config-if)#ip address 40.1.1.2/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth2`	Enter interface mode.
`(config-if)#ip address 50.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#int eth3`	Enter interface mode.
`(config-if)#ip address 60.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 40.1.1.0/24 area 0`	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 50.1.1.0/24 area 0`	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 60.1.1.0/24 area 0`	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#end`	Exit router mode.

Validation

R1

Check OSPF neighborship.

```
#show ip ospf neighbor
OSPF Process 100 VRF (default)
Neighbor ID     Pri   State           Dead Time   Address  Interface Intance ID
2.2.2.2           1   Full/DR         00:00:33    10.1.1.2     eth1  0
3.3.3.3           1   Full/DR         00:00:33    20.1.1.2     eth2  0
4.4.4.4           1   Full/DR         00:00:39    30.1.1.2     eth2  0
#
```

Check the OSPF route installation and LFA-FRR backup path for the primary path.

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter
area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type
1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
```


© 2021 IP Infusion Inc. Proprietary

```
area
* - candidate default

IP Route Table for VRF "default"
C     10.1.1.0/24 is directly connected, eth1
C     20.1.1.0/24 is directly connected, eth2
C 30.1.1.0/24 is directly connected, eth3
O     40.1.1.0/24 [110/10] via 10.1.1.2, eth1, 00:16:43
O     50.1.1.0/24 [110/15] via 20.1.1.2, eth2, 00:16:43
O IA  60.1.1.0/24 [110/15] via 10.1.1.2, eth1, 00:16:43
O E2  70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 00:16:43
O E2 80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 00:16:43
C 127.0.0.0/8 is directly connected, lo
C 192.168.100.0/24 is directly connected, eth0
Gateway of last resort is not set
```

Not mandatory that for all primary path, there exists an LFA backup path only if inequality equation satisfies according to attributes configured on routers, backup path will be calculated.

```
#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area ,p -
stale info
       * - candidate default

IP Route Table for VRF "default"
O       50.1.1.0/24 [110/15] via 20.1.1.2, eth2, 00:00:34
                    [FRR-NH] via 10.1.1.2, eth1

O       60.1.1.0/24 [110/15] via 10.1.1.2, eth1, 00:00:34
                    [FRR-NH] via 20.1.1.2, eth2

O       70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 00:02:27
                    [FRR-NH] via 10.1.1.2, eth1

O       80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 00:02:27
                    [FRR-NH] via 20.1.1.2, eth2
```

Not mandatory that for all primary path, there exists an LFA backup path only if inequality equation satisfies according to attributes configured on routers, backup path will be calculated.

To prohibit an interface from being used as a repair path, disable fast reroute calculation on the interface.

```
(config)#int eth3
(config-if)#ip ospf fast-reroute per-prefix candidate disable
(config-if)#end
```

Verify that the eth3 interface is not used for backup path calculation.

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
O       10.1.1.0/24 [110/10] via 20.1.1.1, eth1, 00:34:04
C       20.1.1.0/24 is directly connected, eth1
O       30.1.1.0/24 [110/20] via 20.1.1.1, eth1, 00:34:04
O       40.1.1.0/24 [110/15] via 20.1.1.1, eth1, 00:34:04
                    [110/15] via 50.1.1.2, eth2, 00:34:04
C       50.1.1.0/24 is directly connected, eth2
O IA    60.1.1.0/24 [110/15] via 50.1.1.2, eth2, 01:08:29
O E2    70.1.1.0/24 [110/20] via 20.1.1.1, eth1, 00:34:03
O E2    80.1.1.0/24 [110/20] via 50.1.1.2, eth2, 01:11:17
C       127.0.0.0/8 is directly connected, lo
C       192.168.100.0/24 is directly connected, eth0
#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area ,p -
stale info
       * - candidate default

IP Route Table for VRF "default"
O       10.1.1.0/24 [110/10] via 20.1.1.1, eth1, 00:00:34
                    [FRR-NH] via 50.1.1.2, eth2

O       30.1.1.0/24 [110/20] via 20.1.1.1, eth1, 00:00:34
                    [FRR-NH] via 50.1.1.2, eth2

O       60.1.1.0/24 [110/15] via 50.1.1.2, eth2, 00:02:27
                    [FRR-NH] via 20.1.1.1, eth1

O       70.1.1.0/24 [110/20] via 20.1.1.1, eth1, 00:02:27
                    [FRR-NH] via 50.1.1.2, eth2

O       80.1.1.0/24 [110/20] via 50.1.1.2, eth2, 00:02:27
```

Note: Now the LFA backup paths have been changed, eth3 is not used.

© 2021 IP Infusion Inc. Proprietary

LFA Tie-Breaker

Based on the index values configured, if inequalities are satisfied, protections will be provided:

- Lower the index will have the highest priority, the path which provides protection with highest priority will be selected. If there are multiple paths providing the highest priority protection, then we will check which path provides the protection which has 2nd highest priority and so on.
- If all the paths provide same priority, then the LFA route is chosen on the basis of path cost.
- If none of the paths provides the protection with highest priority, then we will see which path provides the 2nd highest priority and so on.

```
config)#router ospf 100
(config-router)#fast-reroute tie-break ?
broadcast-interface-disjoint  Prefer broadcast link protecting backup path

                              *Default value is 70

downstream-path               Prefer backup path from downstream

                              *Default value is 90

interface-disjoint            Prefer link protecting backup path

                              *Default value is 60

node-protecting               Prefer node protecting backup path

                              *Default value is 30

primary-path                  Prefer backup path from ECMP set

                              *Default value is 20

secondary-path                Prefer non-ECMP backup path

                              *Default value is 255
(config-router)#fast-reroute tie-break broadcast-interface-disjoint index 1
(config-router)#fast-reroute tie-break node-protecting index 2
```

Verify show ip route and show ip route fast-reroute for backup path calculated according to attributes configured above.

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter
area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type
1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default

IP Route Table for VRF "default"
C     10.1.1.0/24 is directly connected, eth1
C     20.1.1.0/24 is directly connected, eth2
```

```
C 30.1.1.0/24 is directly connected, eth3
O     40.1.1.0/24 [110/10] via 10.1.1.2, eth1, 01:07:26
O     50.1.1.0/24 [110/15] via 20.1.1.2, eth2, 01:07:26
O IA  60.1.1.0/24 [110/15] via 10.1.1.2, eth1, 01:07:26
O E2  70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 01:07:26
O E2 80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 01:07:26
C 127.0.0.0/8 is directly connected, lo
C 192.168.100.0/24 is directly connected, eth0

Gateway of last resort is not set
#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area ,p -
stale info
       * - candidate default

IP Route Table for VRF "default"

O       50.1.1.0/24 [110/15] via 20.1.1.2, eth2, 00:00:34
                    [FRR-NH] via 10.1.1.2, eth1

O       60.1.1.0/24 [110/15] via 10.1.1.2, eth1, 00:02:27
                    [FRR-NH] via 20.1.1.2, eth2

O       70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 00:02:27
                    [FRR-NH] via 10.1.1.2, eth1

O       80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 00:02:27
                    [FRR-NH] via 20.1.1.2, eth2

#show ip ospf route fast-reroute

OSPF process 0:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       OSPF LFA attributes:
       P - Primary, SP - Secondary-Path, ID - Interface Disjoint,
       NP - Node Protecting, BID - Broadcast Interface Disjoint

O  50.1.1.0/24 [15] via 20.1.1.1, eth2, Area 0.0.0.0
                       Backup path:
                        via 10.1.1.2, eth1, Area 0.0.0.0
                       Attributes: Metric: [20] ,LP ,NP, BP
O  60.1.1.0/24 [15] via 10.1.1.2, eth1, Area 0.0.0.0
                       Backup path:
                        via 20.1.1.2, eth2, Area 0.0.0.0
                       Attributes: Metric: [15] ,LP ,NP,BP
```

 © 2021 IP Infusion Inc. Proprietary

```
O  70.1.1.0/24 [20] via 30.1.1.2, eth3, Area 0.0.0.0
                       Backup path:
                        via 10.1.1.2, eth1, Area 0.0.0.0
                       Attributes: Metric: [20] ,LP ,NP,BP
O  80.1.1.0/24 [20] via 10.1.1.2, eth1, Area 0.0.0.0
                       Backup path:
                        via 20.1.1.2, eth2, Area 0.0.0.0
                       Attributes: Metric: [20] ,LP,NP,BP
```

LFA Termination

A router MUST limit the amount of time an alternate next-hop is used after the primary next-hop has become unavailable. This ensures that the router will start using the new primary next-hops.

LFA termination avoids a micro looping in topology, when particular network goes down, LFA backup path will be installed and if termination interval is configured, LFA backup will be still used till the interval and it is used in order to verify new primary path is loop free.

R1

Configure termination interval on R1 in router mode:

`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#fast-reroute terminate-hold-on interval 100000`	Configure LFA termination interval
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

If you check "show ip ospf" you can see the configured termination-hold on interval value along with ospf output:

```
#show ip ospf
IPFRR per-prefix tiebreakers:
    Name                                Index
    Primary path                        20
    Node Protecting                     30
    Interface disjoint                  60
    Broadcast interface disjoint        70
    Secondary path                      255
 LFA termination hold-on timer : 100 secs 0 msecs

#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area ,p -
stale info
       * - candidate default

IP Route Table for VRF "default"
```

```
O       50.1.1.0/24 [110/15] via 20.1.1.2, eth2, 00:00:34
                    [FRR-NH] via 10.1.1.2, eth1

O       60.1.1.0/24 [110/15 via 10.1.1.2, eth1, 00:00:34
                    [FRR-NH] via 20.1.1.2, eth2

O       70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 00:02:27
                    [FRR-NH] via 10.1.1.2, eth1

O       80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 00:02:27
                    [FRR-NH] via 20.1.1.2, eth2
```

Shut down one of the primary nexthops, here eth2 of rtr1:

`(config)#interface eth2`	Enter interface mode.
`(config-if)#shutdown`	Shutdown the interface
`(config-if)#exit`	Exit interface mode
`(config-if)#exit`	Exit interface mode.

```
#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area ,p -
stale info
       * - candidate default

IP Route Table for VRF "default"
O       50.1.1.0/24 [110/15] via 20.1.1.2, eth1, 00:00:34  <<<eth1 which was back-up
path before got  installed as new primary path
                    [FRR-NH] via 30.1.1.2, eth3

O       60.1.1.0/24 [110/15] via 10.1.1.2, eth1, 00:00:34
                    [FRR-NH] via 30.1.1.2, eth3

O       70.1.1.0/24 [110/20] via 30.1.1.2, eth3, 00:02:27
                    [FRR-NH] via 10.1.1.2, eth1

O       80.1.1.0/24 [110/20] via 10.1.1.2, eth1, 00:02:27
                    [FRR-NH] via 30.1.1.2, eth3
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 OSPFv3

This chapter contains basic OSPFv3 configuration examples.

Enable OSPFv3 on an Interface

This example shows the minimum configuration required for enabling OSPFv3 on an interface. R1 and R2 are two routers in Area 0 connecting to the network 3ffe:10::/64. After enabling OSPFv3 on an interface, create a routing instance, and specify the Router ID.

Note: You must explicitly specify a Router ID for the OSPFv3 process to be activated.

Topology

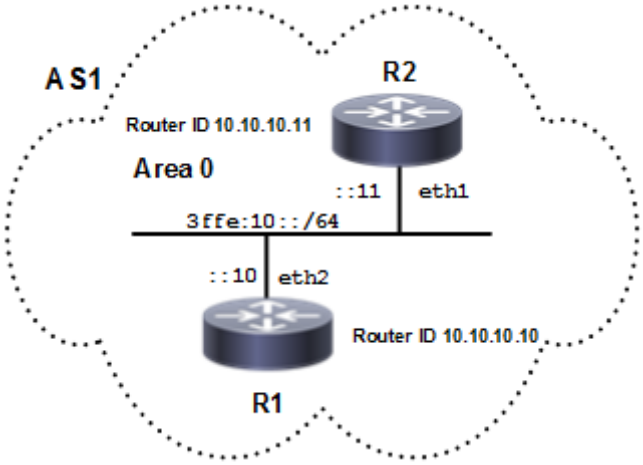


Figure 5-99: Basic OSPFv3 Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.10`	Specify a Router ID for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `0`.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.

`(config-router)#router-id 10.10.10.11`	Specify a Router ID (`10.10.10.11`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.

Validation

R1

```
#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.11       1   Full/Backup     00:00:35    eth2       0

#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.10) (Process *null*)

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10      164       0x80000001 0xf3c6      1
0.0.0.3         10.10.10.11      106       0x80000001 0xd973      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10       94       0x80000003 0xb2f0      1
0.0.0.0         10.10.10.11       95       0x80000003 0x9e05      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10       94       0x80000001 0xf990

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.10       93       0x80000001 0xc35d      1  Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10       94       0x80000002 0x3504
0.0.0.3         10.10.10.11       95       0x80000002 0x6bcc

#show ipv6 ospfv3 topology
```


© 2021 IP Infusion Inc. Proprietary

```
OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10             --
10.10.10.11             1          10.10.10.11          eth2
```

R2

```
#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DR         00:00:31    eth1       0

R2#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.11) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10      341       0x80000001 0xf3c6      1
0.0.0.3         10.10.10.11      281       0x80000001 0xd973      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10      271       0x80000003 0xb2f0      1
0.0.0.0         10.10.10.11      270       0x80000003 0x9e05      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10      271       0x80000001 0xf990

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.10      270       0x80000001 0xc35d      1  Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10      271       0x80000002 0x3504
0.0.0.3         10.10.10.11      270       0x80000002 0x6bcc


R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
```

```
10.10.10.10             1          10.10.10.10          eth1
10.10.10.11             --
```

Set Priority

This example shows how to set priority for an interface. Set a high priority for a router to make it the Designated Router (DR). Router R3 is configured with a priority of 10; this is higher than the default priority (default priority is 1) set for R1 and R2. This makes R3 the DR.

Topology

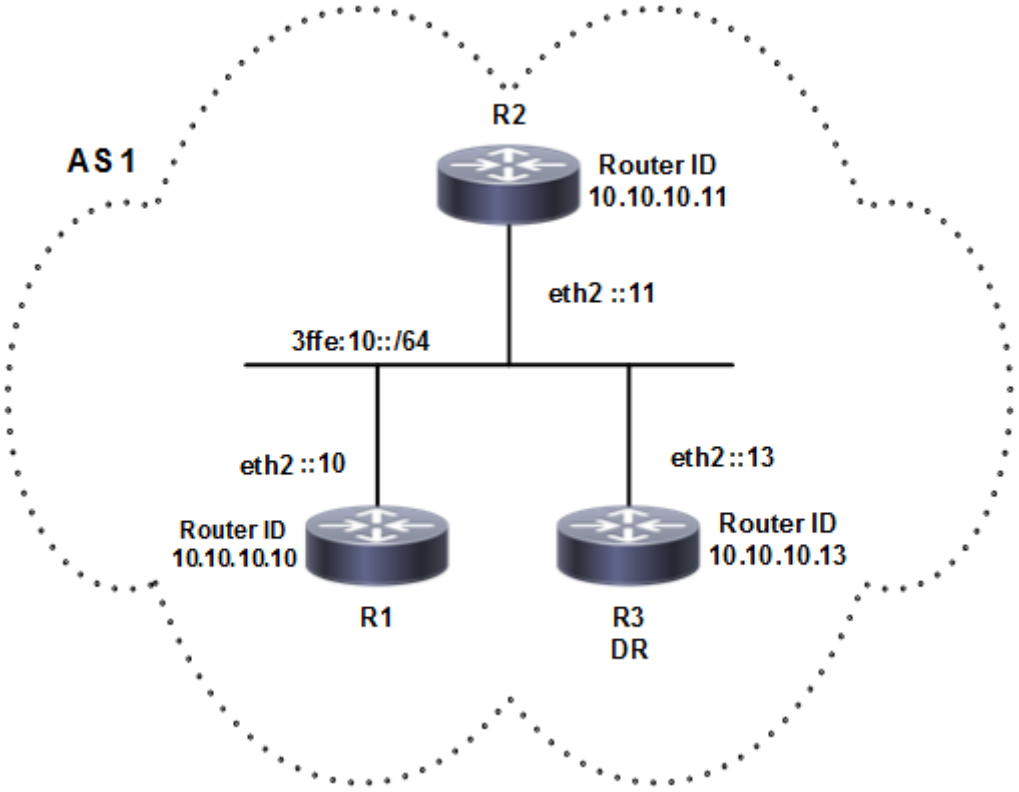


Figure 5-100: OSPFv3 Set Priority

R3

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.13`	Specify a Router ID (`10.10.10.13`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#ipv6 ospf priority 10`	Specify the router priority to a higher priority (10) to make R3 the Designated Router (DR).

© 2021 IP Infusion Inc. Proprietary

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.10`	Specify a Router ID (`10.10.10.10`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.

R2

`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.11`	Specify a Router ID (`10.10.10.11`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.

Validation

R1

```
rtr1#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface Instance ID
10.10.10.11       1   Full/DROther    00:00:37    eth2       0
10.10.10.13      10   Full/DR         00:00:37    eth2       0

rtr1#show ipv6 ospf database
            OSPFv3 Router with ID (10.10.10.10) (Process *null*)

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum Prefix
0.0.0.4         10.10.10.10      398       0x80000001 0xf3c6      1
0.0.0.4         10.10.10.11       71       0x80000001 0x4768      1
0.0.0.4         10.10.10.13      611       0x80000002 0x695b      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10       49       0x80000004 0xf2ac      1
0.0.0.0         10.10.10.11       50       0x80000004 0xecb1      1
0.0.0.0         10.10.10.13       61       0x80000004 0xe0bb      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
```

```
0.0.0.4         10.10.10.13       61        0x80000002 0xa6b0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.13       60       0x80000002 0xd940      1  Network-
LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10       49       0x80000003 0x75bf
0.0.0.4         10.10.10.11       50       0x80000004 0x9f92
0.0.0.4         10.10.10.13       61       0x80000003 0xf935


rtr1#show ipv6 ospfv3 topology
OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits Metric     Next-Hop             Interface
10.10.10.10            --
10.10.10.11            1          10.10.10.11          eth2
10.10.10.13            1          10.10.10.13          eth2
```

R2

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface Instance ID
10.10.10.10       1   Full/Backup     00:00:31    eth2       0
10.10.10.13      10   Full/DR         00:00:39    eth2       0

R2#show ipv6 ospf database
            OSPFv3 Router with ID (10.10.10.11) (Process *null*)

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10       525       0x80000001 0xf3c6      1
0.0.0.4         10.10.10.11       194       0x80000001 0x4768      1
0.0.0.4         10.10.10.13       736       0x80000002 0x695b      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10       175       0x80000004 0xf2ac      1
0.0.0.0         10.10.10.11       174       0x80000004 0xecb1      1
0.0.0.0         10.10.10.13       186       0x80000004 0xe0bb      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.13       186       0x80000002 0xa6b0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)
```


© 2021 IP Infusion Inc. Proprietary

```
Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.13      185       0x80000002 0xd940      1  Network-
LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10      175       0x80000003 0x75bf
0.0.0.4         10.10.10.11      174       0x80000004 0x9f92
0.0.0.4         10.10.10.13      186       0x80000003 0xf935

R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits Metric     Next-Hop             Interface
10.10.10.10            1          10.10.10.10          eth2
10.10.10.11            --
10.10.10.13            1          10.10.10.13          eth2
```

R3

```
R3#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/Backup     00:00:38    eth2       0
10.10.10.11       1   Full/DROther    00:00:29    eth2       0

R3#show ipv6 ospf database
            OSPFv3 Router with ID (10.10.10.13) (Process *null*)

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10      658       0x80000001 0xf3c6      1
0.0.0.4         10.10.10.11      329       0x80000001 0x4768      1
0.0.0.4         10.10.10.13      869       0x80000002 0x695b      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10      309       0x80000004 0xf2ac      1
0.0.0.0         10.10.10.11      309       0x80000004 0xecb1      1
0.0.0.0         10.10.10.13      319       0x80000004 0xe0bb      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.13      319       0x80000002 0xa6b0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.13      318       0x80000002 0xd940      1  Network-
LSA
```

```
                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age         Seq#       CkSum
0.0.0.4         10.10.10.10      309        0x80000003 0x75bf
0.0.0.4         10.10.10.11      309        0x80000004 0x9f92
0.0.0.4         10.10.10.13      319        0x80000003 0xf935

R3#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits Metric     Next-Hop             Interface
10.10.10.10            1          10.10.10.10          eth2
10.10.10.11            1          10.10.10.11          eth2
10.10.10.13            --
```

Area Border Router

This example shows configuration for an Area Border Router. R2 is an Area Border Router (ABR). On R2, interface eth2 is in Area 0, and interface eth1 is in Area 1.

Topology

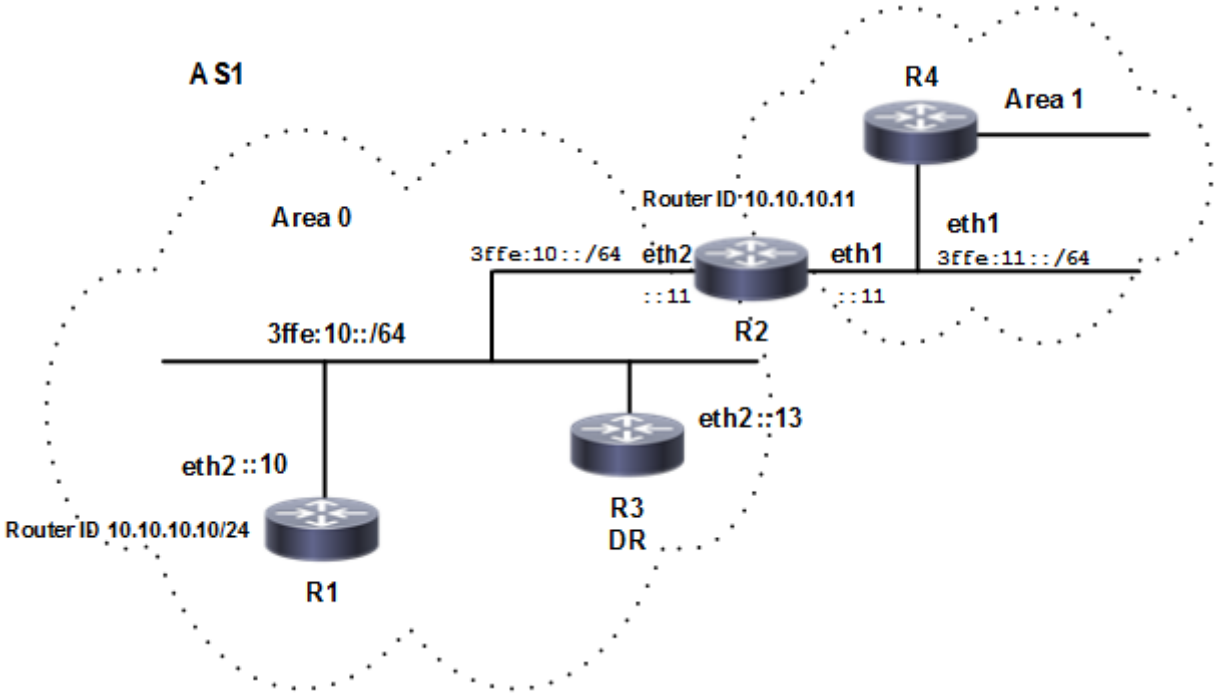


Figure 5-101: OSPFv3 Area Border Router

© 2021 IP Infusion Inc. Proprietary

Configuration

R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.11`	Specify a Router ID (`10.10.10.11`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 1`	Enable OSPFv3 routing on the other interface, and assign the other Area ID `(1)`.

Validation

R2

```
R2S#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DROther    00:00:33    eth1       0
10.10.10.12       1   Full/DR         00:00:31    eth1       0
10.10.10.13       1   Full/DR         00:00:36    eth2       0


R2S#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.11) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.3         10.10.10.10      171       0x80000001 0xaa25      1
0.0.0.3         10.10.10.11      139       0x80000001 0x87eb      1
0.0.0.3         10.10.10.12      132       0x80000001 0x2032      1

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.10.11      139       0x80000001 0xb466      1
0.0.0.4         10.10.10.13      130       0x80000001 0x8c5b      1

                Router-LSA (Area 0.0.0.0)
```

```
Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10       83       0x80000005 0xbae6      1
0.0.0.0         10.10.10.11       82       0x80000005 0xb7e7      1
0.0.0.0         10.10.10.12       87       0x80000003 0xb2ee      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.12       87       0x80000002 0xacad

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.1         10.10.10.11      134       0x80000002 0xfd5e

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.12       86       0x80000001 0xc954      1  Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.10       83       0x80000003 0x57e0
0.0.0.3         10.10.10.11       77       0x80000004 0x81b3
0.0.0.3         10.10.10.12       87       0x80000003 0xaf84

                Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.11       89       0x80000003 0xf1ac      1
0.0.0.0         10.10.10.13       85       0x80000003 0xe2ba      1

                Network-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.13       90       0x80000001 0x067e

                Inter-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.1         10.10.10.11      134       0x80000002 0xccaf

                Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.13       84       0x80000001 0x0eec      1  Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.1)
```


© 2021 IP Infusion Inc. Proprietary

```
Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.11       89       0x80000002 0xb75c
0.0.0.4         10.10.10.13       89       0x80000002 0xdd33


R2S#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10             1          10.10.10.10          eth1
10.10.10.11         B   --
10.10.10.12             1          10.10.10.12          eth1

OSPFv3 paths to Area (0.0.0.1) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.11         B   --
10.10.10.13             1          10.10.10.13          eth2


R2S#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 00:02:52
C      3ffe:10::/64 via ::, eth1, 00:02:51
C      6ffe::/64 via ::, eth2, 00:02:51
C      fe80::/64 via ::, eth2, 00:02:52


R2#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                  Metric
     Next-hop
C  3ffe:10::/64                                    1
     directly connected, eth1, Area 0.0.0.0
C  6ffe::/64                                      1
     directly connected, eth2, Area 0.0.0.1
```

Redistribute Routes into OSPFv3

In this example, the BGP routes are imported into the OSPF routing table, and advertised as Type 5 External LSAs into Area 0.

Topology

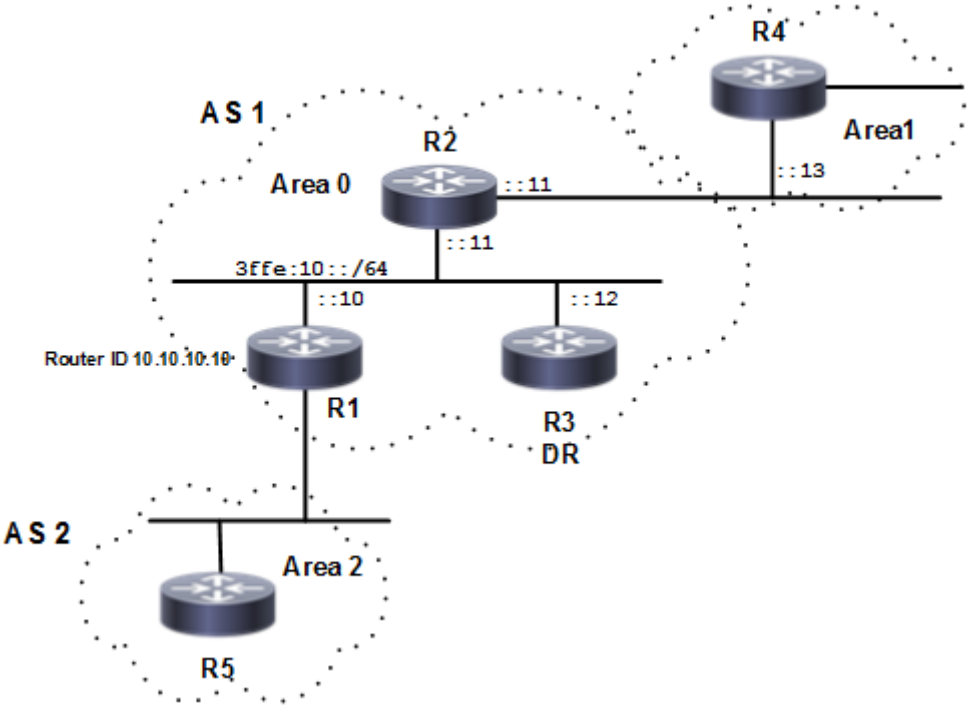


Figure 5-102: OSPFv3 Redistribute Routes

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.10`	Specify a Router ID `(10.10.10.10)` for the OSPFv3 routing process.
`(config-router)#redistribute bgp`	Specify redistributing routes from the other routing protocol (BGP) into OSPFv3.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.

© 2021 IP Infusion Inc. Proprietary

Validation

R2

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State                 Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DR              00:00:40         eth1       0
10.10.10.12       1   Full/DROther    00:00:40          eth1       0
10.10.10.13       1   Full/Backup      00:00:33          eth2       0

R2#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.11) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#               CkSum    Prefix
0.0.0.3           10.10.10.10      364       0x80000002    0x21a3      1
0.0.0.3           10.10.10.11     1046       0x80000001   0xa3f6       1
0.0.0.3           10.10.10.12     1018       0x80000001   0xd00e      1

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#               CkSum     Prefix
0.0.0.4           10.10.10.11     1046      0x80000001   0xc0b0      1
0.0.0.3           10.10.10.13      985       0x80000001   0x61e4      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#               CkSum    Link
0.0.0.0           10.10.10.10     1007       0x80000005   0x9709      1
0.0.0.0           10.10.10.11     1003       0x80000004   0x8d15      1
0.0.0.0           10.10.10.12     1002       0x80000004   0x841e      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#               CkSum
0.0.0.3           10.10.10.10     1007       0x80000002   0xc497

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#               CkSum
0.0.0.1           10.10.10.10      355       0x80000003   0x511b
0.0.0.1           10.10.10.11      1041     0x80000002   0x9cdf

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#               CkSum    Prefix
Reference
0.0.0.2           10.10.10.10     1006       0x80000002 0x56da      1
Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#                  CkSum
0.0.0.3          10.10.10.10      1007      0x80000003      0xc881
```

```
0.0.0.3           10.10.10.11      1003      0x80000003      0xf453
0.0.0.3           10.10.10.12      1002      0x80000003      0x2125

                Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#              CkSum     Link
0.0.0.0           10.10.10.11      973       0x80000004   0xc3db      1
0.0.0.0           10.10.10.13      973       0x80000003   0xa8f7       1

                Network-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#                CkSum
0.0.0.4           10.10.10.11      973       0x80000001     0x1a6c

                Inter-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#                CkSum
0.0.0.1           10.10.10.11     1041      0x80000002     0xeba0
0.0.0.2           10.10.10.11      969       0x80000002     0x4921

                Inter-Area-Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#                CkSum
0.0.0.1           10.10.10.11     1019      0x80000001    0x9c16

                Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#              CkSum    Prefix
Reference
0.0.0.2           10.10.10.11      972       0x80000001  0x9b83      1
Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#                CkSum
0.0.0.4           10.10.10.11      973       0x80000002    0x47ee
0.0.0.3           10.10.10.13      973       0x80000002    0xa989


R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10        EB  1          10.10.10.10          eth1
10.10.10.11         B  --
10.10.10.12         1               10.10.10.12          eth1

OSPFv3 paths to Area (0.0.0.1) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.11         B  --
10.10.10.13         1                 10.10.10.13          eth2


R2#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
```


© 2021 IP Infusion Inc. Proprietary

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe::/64                                         1
     directly connected, eth1, Area 0.0.0.0
C  4ffe::/64                                         1
     directly connected, eth2, Area 0.0.0.1
IA 5ffe::/64                                         2
     via fe80::5054:ff:fe58:fc20, eth1, Area 0.0.0.0


R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 00:44:22
C      3ffe::/64 via ::, eth1, 00:18:00
C      4ffe::/64 via ::, eth2, 00:18:00
O IA   5ffe::/64 [110/2] via fe80::5054:ff:fe58:fc20, eth1, 00:17:32
C      fe80::/64 via ::, eth2, 00:44:22
```

R3

```
R3#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State              Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DR           00:00:37         eth1       0
10.10.10.11       1   Full/Backup     00:00:34          eth1       0


R3#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.12) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age        Seq#               CkSum    Prefix
0.0.0.3           10.10.10.10     459        0x80000002     0x21a3      1
0.0.0.3           10.10.10.11    1142       0x80000001     0xa3f6      1
0.0.0.3           10.10.10.12    1111       0x80000001     0xd00e      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#                CkSum    Link
0.0.0.0           10.10.10.10    1103       0x80000005     0x9709      1
0.0.0.0           10.10.10.11    1099       0x80000004     0x8d15      1
0.0.0.0           10.10.10.12    1096       0x80000004     0x841e      1

                Network-LSA (Area 0.0.0.0)
```

```
Link State ID   ADV Router      Age       Seq#               CkSum
0.0.0.3           10.10.10.10     1103       0x80000002    0xc497

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#                CkSum
0.0.0.1           10.10.10.10      450        0x80000003     0x511b
0.0.0.1           10.10.10.11     1137       0x80000002     0x9cdf

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#               CkSum  Prefix
Reference
0.0.0.2           10.10.10.10     1101       0x80000002   0x56da      1
Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#                 CkSum
0.0.0.3           10.10.10.10     1103       0x80000003    0xc881
0.0.0.3           10.10.10.11     1099       0x80000003    0xf453
0.0.0.3           10.10.10.12     1096       0x80000003    0x2125

R3#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10        EB  1          10.10.10.10            eth1
10.10.10.11         B  1          10.10.10.11             eth1
10.10.10.12            --

R3#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe::/64                                         1
     directly connected, eth1, Area 0.0.0.0
IA 4ffe::/64                                         2
     via fe80::5054:ff:fe5b:1034, eth1, Area 0.0.0.0
IA 5ffe::/64                                         2
     via fe80::5054:ff:fe58:fc20, eth1, Area 0.0.0.0

R3#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 00:45:05
```


© 2021 IP Infusion Inc. Proprietary

```
C       3ffe::/64 via ::, eth1, 00:18:53
O IA    4ffe::/64 [110/2] via fe80::5054:ff:fe5b:1034, eth1, 00:18:39
O IA    5ffe::/64 [110/2] via fe80::5054:ff:fe58:fc20, eth1, 00:18:39
C       fe80::/64 via ::, eth2, 00:45:05
```

Cost

Make a route the preferred route by changing its cost. In this example, cost has been configured to make R2 the next hop for R1.

The default cost for each interface is 10. Interface eth2 on R2 has a cost of 100, and Interface eth2 on R3 has a cost of 150. The total cost to reach 10.10.14.0/24 (R4) through R2 and R3 is computed as follows:

R2: 10+100 = 110

R3: 10+150 = 160

For this reason, R1 chooses R2 as its next hop to destination 10.10.14.0/24, because it has the lower cost.

Topology

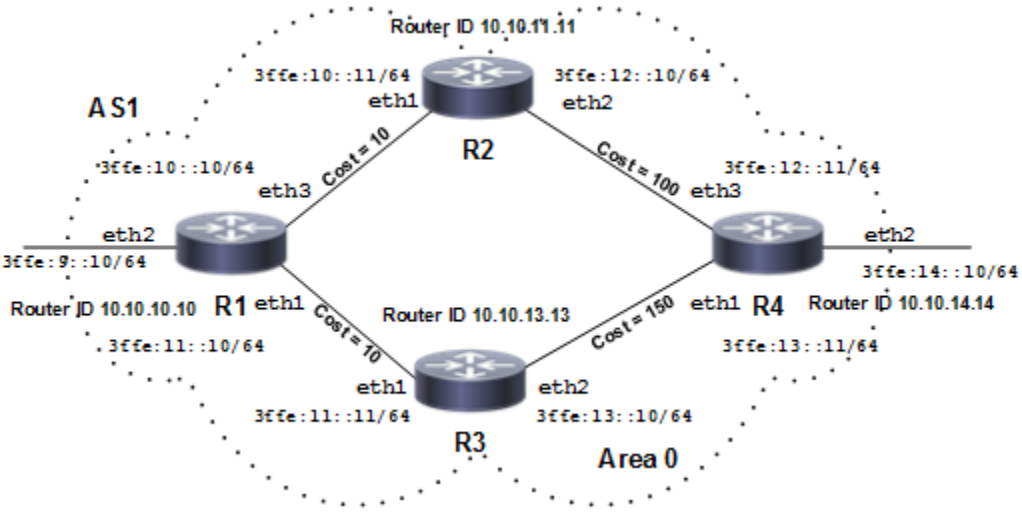


Figure 5-103: Configure Cost OSPFv3

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.10`	Specify a Router ID (`10.10.10.10`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth3`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.

`#configure terminal`	Enter configure mode.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.

R2

`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.11.11`	Specify a Router ID (`10.10.11.11`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#ipv6 ospf cost 100`	Set the cost of the link-state metric (on `eth2`) to `100`.

R3

`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.13.13`	Specify a Router ID (`10.10.13.13`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#ipv6 ospf cost 150`	Set the cost of link-state metric to `150`.

R4

`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.14.14`	Specify a Router ID (`10.10.14.14`) for the OSPFv3 routing process.

© 2021 IP Infusion Inc. Proprietary

(config-router)#exit	Exit OSPF router mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).

Validation

R1

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.13.13       1   Full/Backup     00:00:37    eth1       0
10.10.11.11       1   Full/Backup     00:00:34    eth3       0


R1#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10            --
10.10.11.11            1          10.10.11.11          eth3
10.10.13.13            1          10.10.13.13          eth1
10.10.14.14            101        10.10.11.11          eth3



rtr1#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.10) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.3         10.10.10.10      868       0x80000003 0x4839      1
0.0.0.3         10.10.13.13      747       0x80000003 0x5544      1

                Link-LSA (Interface eth3)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.5         10.10.10.10      898       0x80000003 0xf33e      1
0.0.0.3         10.10.11.11      817       0x80000003 0xce7b      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10       58       0x80000008 0xabaf      2
0.0.0.0         10.10.11.11     1767       0x80000008 0x26cd      2
```

```
0.0.0.0         10.10.13.13     1753       0x80000008 0x9724      2
0.0.0.0         10.10.14.14     1753       0x80000007 0x96b5      2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum
0.0.0.3         10.10.10.10       58       0x80000003 0x4341
0.0.0.5         10.10.10.10      163       0x80000003 0xf88d
0.0.0.4         10.10.11.11     1767       0x80000002 0x5c22
0.0.0.4         10.10.13.13     1753       0x80000002 0x680e

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum  Prefix  Reference
0.0.0.1         10.10.10.10      813       0x80000003 0xd34b      1  Network-
LSA
0.0.0.2         10.10.10.10      743       0x80000003 0xcb53      1  Network-
LSA
0.0.0.2         10.10.11.11      652       0x80000003 0xf91f      1  Network-
LSA
0.0.0.3         10.10.13.13      684       0x80000003 0x22ec      1  Network-
LSA
                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum
0.0.0.3         10.10.10.10      868       0x80000004 0x4fe8
0.0.0.5         10.10.10.10      898       0x80000004 0x39fb
0.0.0.3         10.10.11.11      817       0x80000004 0x72c1
0.0.0.4         10.10.11.11      802       0x80000005 0xe1ea
0.0.0.3         10.10.13.13      747       0x80000004 0x5ad6
0.0.0.4         10.10.13.13      727       0x80000005 0x8f02
0.0.0.3         10.10.14.14      688       0x80000004 0x2df8
0.0.0.5         10.10.14.14      653       0x80000004 0x9c8c


rtr1#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:10::/64                                      1
     directly connected, eth3, Area 0.0.0.0
C  3ffe:11::/64                                      1
     directly connected, eth1, Area 0.0.0.0
O  3ffe:12::/64                                    101
     via fe80::a00:27ff:fef9:2432, eth3, Area 0.0.0.0
O  3ffe:13::/64                                    102
     via fe80::a00:27ff:fef9:2432, eth3, Area 0.0.0.0


rtr1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
```


© 2021 IP Infusion Inc. Proprietary

```
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:22:59
C      3ffe:10::/64 via ::, eth3, 00:51:14
C      3ffe:11::/64 via ::, eth1, 00:50:44
O      3ffe:12::/64 [110/101] via fe80::a00:27ff:fef9:2432, eth3, 00:49:33
O      3ffe:13::/64 [110/102] via fe80::a00:27ff:fef9:2432, eth3, 00:48:21
C      fe80::/64 via ::, eth1, 01:13:13
K      ff00::/8 [0/256] via ::, eth0, 01:22:47
```

R2

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DR         00:00:32    eth1       0
10.10.14.14       1   Full/Backup     00:00:33    eth2       0


R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10            1          10.10.10.10          eth1
10.10.11.11            --
10.10.13.13            2          10.10.10.10          eth1
10.10.14.14            100        10.10.14.14          eth2



R2#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.11.11) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.5         10.10.10.10     1373       0x80000003 0xf33e      1
0.0.0.3         10.10.11.11     1290       0x80000003 0xce7b      1

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.11.11     1275       0x80000003 0x802a      1
0.0.0.5         10.10.14.14     1126       0x80000003 0x4f29      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
```

```
0.0.0.0         10.10.10.10      533        0x80000008 0xabaf      2
0.0.0.0         10.10.11.11      440        0x80000009 0x24ce      2
0.0.0.0         10.10.13.13      427        0x80000009 0x9525      2
0.0.0.0         10.10.14.14      426        0x80000008 0x94b6      2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum
0.0.0.3         10.10.10.10      533        0x80000003 0x4341
0.0.0.5         10.10.10.10      638        0x80000003 0xf88d
0.0.0.4         10.10.11.11      440        0x80000003 0x5a23
0.0.0.4         10.10.13.13      427        0x80000003 0x660f

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum  Prefix  Reference
0.0.0.1         10.10.10.10     1288        0x80000003 0xd34b      1  Network-
LSA
0.0.0.2         10.10.10.10     1218        0x80000003 0xcb53      1  Network-
LSA
0.0.0.2         10.10.11.11     1125        0x80000003 0xf91f      1  Network-
LSA
0.0.0.3         10.10.13.13     1158        0x80000003 0x22ec      1  Network-
LSA
                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age        Seq#       CkSum
0.0.0.3         10.10.10.10     1343        0x80000004 0x4fe8
0.0.0.5         10.10.10.10     1373        0x80000004 0x39fb
0.0.0.3         10.10.11.11     1290        0x80000004 0x72c1
0.0.0.4         10.10.11.11     1275        0x80000005 0xe1ea
0.0.0.3         10.10.13.13     1223        0x80000004 0x5ad6
0.0.0.4         10.10.13.13     1203        0x80000005 0x8f02
0.0.0.3         10.10.14.14     1161        0x80000004 0x2df8
0.0.0.5         10.10.14.14     1126        0x80000004 0x9c8c


R2#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                      Metric
     Next-hop
C  3ffe:10::/64                                        1
     directly connected, eth1, Area 0.0.0.0
O  3ffe:11::/64                                        2
     via fe80::a00:27ff:fe6e:21d8, eth1, Area 0.0.0.0
C  3ffe:12::/64                                      100
     directly connected, eth2, Area 0.0.0.0
O  3ffe:13::/64                                      101
     via fe80::a00:27ff:fe01:c94d, eth2, Area 0.0.0.0


R2#show ipv6 route
IPv6 Routing Table
```


© 2021 IP Infusion Inc. Proprietary

```
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:26:25
C      3ffe:10::/64 via ::, eth1, 00:54:14
O      3ffe:11::/64 [110/2] via fe80::a00:27ff:fe6e:21d8, eth1, 00:55:03
C      3ffe:12::/64 via ::, eth2, 00:53:58
O      3ffe:13::/64 [110/101] via fe80::a00:27ff:fe01:c94d, eth2, 00:52:43
C      fe80::/64 via ::, eth2, 01:20:38
K      ff00::/8 [0/256] via ::, eth2, 01:20:39
```

R3

```
R3#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DR         00:00:33    eth1       0
10.10.14.14       1   Full/Backup     00:00:38    eth2       0



R3#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10            1          10.10.10.10          eth1
10.10.11.11            2          10.10.10.10          eth1
10.10.13.13            --
10.10.14.14            102        10.10.10.10          eth1


R3#
R3#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.13.13) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.3         10.10.10.10     1591       0x80000003 0x4839      1
0.0.0.3         10.10.13.13     1468       0x80000003 0x5544      1

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.13.13     1448       0x80000003 0x9d29      1
0.0.0.3         10.10.14.14     1409       0x80000003 0x50cf      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10      780       0x80000008 0xabaf      2
```

```
0.0.0.0         10.10.11.11      689       0x80000009 0x24ce      2
0.0.0.0         10.10.13.13      673       0x80000009 0x9525      2
0.0.0.0         10.10.14.14      673       0x80000008 0x94b6      2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.10      780       0x80000003 0x4341
0.0.0.5         10.10.10.10      885       0x80000003 0xf88d
0.0.0.4         10.10.11.11      689       0x80000003 0x5a23
0.0.0.4         10.10.13.13      673       0x80000003 0x660f

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.1         10.10.10.10     1536       0x80000003 0xd34b      1  Network-
LSA
0.0.0.2         10.10.10.10     1466       0x80000003 0xcb53      1  Network-
LSA
0.0.0.2         10.10.11.11     1374       0x80000003 0xf91f      1  Network-
LSA
0.0.0.3         10.10.13.13     1403       0x80000003 0x22ec      1  Network-
LSA
               Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.10     1591       0x80000004 0x4fe8
0.0.0.5         10.10.10.10     1621       0x80000004 0x39fb
0.0.0.3         10.10.11.11     1539       0x80000004 0x72c1
0.0.0.4         10.10.11.11     1524       0x80000005 0xe1ea
0.0.0.3         10.10.13.13     1468       0x80000004 0x5ad6
0.0.0.4         10.10.13.13     1448       0x80000005 0x8f02
0.0.0.3         10.10.14.14     1409       0x80000004 0x2df8
0.0.0.5         10.10.14.14     1374       0x80000004 0x9c8c


R3#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                      Metric
     Next-hop
O  3ffe:10::/64                                       2
     via fe80::a00:27ff:fe7d:2a72, eth1, Area 0.0.0.0
C  3ffe:11::/64                                       1
     directly connected, eth1, Area 0.0.0.0
O  3ffe:12::/64                                     102
     via fe80::a00:27ff:fe7d:2a72, eth1, Area 0.0.0.0
O  3ffe:13::/64                                     103
     via fe80::a00:27ff:fe7d:2a72, eth1, Area 0.0.0.0


R3#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
```


© 2021 IP Infusion Inc. Proprietary

```
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:28:16
O      3ffe:10::/64 [110/2] via fe80::a00:27ff:fe7d:2a72, eth1, 00:58:14
C      3ffe:11::/64 via ::, eth1, 00:55:44
O      3ffe:12::/64 [110/102] via fe80::a00:27ff:fe7d:2a72, eth1, 00:56:36
C      3ffe:13::/64 via ::, eth2, 00:55:26
C      fe80::/64 via ::, eth1, 01:20:39
K      ff00::/8 [0/256] via ::, eth2, 01:21:40
```

R4

```
R4#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.13.13       1   Full/DR         00:00:30    eth1       0
10.10.11.11       1   Full/DR         00:00:30    eth3       0



R4#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10            2          10.10.11.11          eth3
                                  10.10.13.13          eth1
10.10.11.11            1          10.10.11.11          eth3
10.10.13.13            1          10.10.13.13          eth1
10.10.14.14            --


R4#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.14.14) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.13.13     1634       0x80000003 0x9d29      1
0.0.0.3         10.10.14.14     1592       0x80000003 0x50cf      1

                Link-LSA (Interface eth3)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.10.11.11     1708       0x80000003 0x802a      1
0.0.0.5         10.10.14.14     1557       0x80000003 0x4f29      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10      966       0x80000008 0xabaf      2
```

```
0.0.0.0         10.10.11.11      873       0x80000009 0x24ce      2
0.0.0.0         10.10.13.13      859       0x80000009 0x9525      2
0.0.0.0         10.10.14.14      857       0x80000008 0x94b6      2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.10      966       0x80000003 0x4341
0.0.0.5         10.10.10.10     1071       0x80000003 0xf88d
0.0.0.4         10.10.11.11      873       0x80000003 0x5a23
0.0.0.4         10.10.13.13      859       0x80000003 0x660f

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.1         10.10.10.10     1721       0x80000003 0xd34b      1  Network-
LSA
0.0.0.2         10.10.10.10     1651       0x80000003 0xcb53      1  Network-
LSA
0.0.0.2         10.10.11.11     1558       0x80000003 0xf91f      1  Network-
LSA
0.0.0.3         10.10.13.13     1589       0x80000003 0x22ec      1  Network-
LSA

  Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.10     1776       0x80000004 0x4fe8
0.0.0.5         10.10.10.10        6       0x80000005 0x37fc
0.0.0.3         10.10.11.11     1723       0x80000004 0x72c1
0.0.0.4         10.10.11.11     1708       0x80000005 0xe1ea
0.0.0.3         10.10.13.13     1654       0x80000004 0x5ad6
0.0.0.4         10.10.13.13     1634       0x80000005 0x8f02
0.0.0.3         10.10.14.14     1592       0x80000004 0x2df8
0.0.0.5         10.10.14.14     1557       0x80000004 0x9c8c



R4#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                      Metric
     Next-hop
O  3ffe:10::/64                                       2
     via fe80::a00:27ff:fe0d:fbe3, eth3, Area 0.0.0.0
O  3ffe:11::/64                                       2
     via fe80::a00:27ff:fecf:8873, eth1, Area 0.0.0.0
C  3ffe:12::/64                                       1
     directly connected, eth3, Area 0.0.0.0
C  3ffe:13::/64                                       1
     directly connected, eth1, Area 0.0.0.0


R4#show ipv6 route
```


© 2021 IP Infusion Inc. Proprietary

```
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C       ::1/128 via ::, lo, 01:32:01
O       3ffe:10::/64 [110/2] via fe80::a00:27ff:fe0d:fbe3, eth3, 01:02:49
O       3ffe:11::/64 [110/2] via fe80::a00:27ff:fecf:8873, eth1, 01:02:19
C       3ffe:12::/64 via ::, eth3, 00:58:46
C       3ffe:13::/64 via ::, eth1, 00:59:18
C       fe80::/64 via ::, eth1, 01:27:01
K       ff00::/8 [0/256] via ::, eth3, 01:27:31
```

Virtual Links

Virtual links are used to connect a temporarily-disjointed non-backbone area to the backbone area, or to repair a non-contiguous backbone area. In this example, the ABR R3 has temporarily lost connection to Area 0, in turn disconnecting Area 2 from the backbone area. The virtual link between ABR R1 and ABR R2 connects Area 2 to Area 0. Area 1 is used as a transit area.

Topology

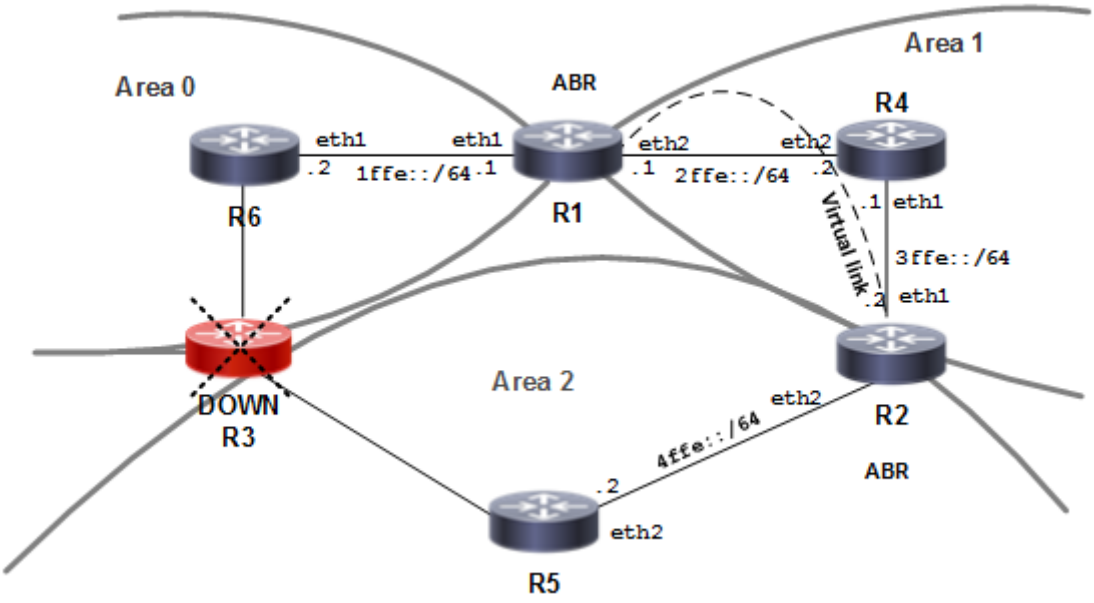


Figure 5-104: OSPFv3 Virtual Links

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Setup loopback interface
`(config-if)#ip address 1.1.1.1/32 secondary`	Specify loopback interface address
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on this interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 1`	Enable OSPFv3 routing on this interface, and assign the Area ID `(1)`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 1.1.1.1`	Specify a Router ID (`1.1.1.1`) for the OSPFv3 routing process.
`(config-router)#area 1 virtual-link 2.2.2.2`	Configure a virtual link between this router R1 and R2 (Router ID `2.2.2.2`) through transit area 1.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Setup loopback interface
`(config-if)#ip address 2.2.2.2/32 secondary`	Specify loopback interface address
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router ospf area 1`	Enable OSPFv3 routing on this interface, and assign the Area ID `(1)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router ospf area 2`	Enable OSPFv3 routing on this interface, and assign the Area ID `(2)`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 2.2.2.2`	Specify a Router ID (`2.2.2.2`) for the OSPFv3 routing process.
`(config-router)#area 1 virtual-link 1.1.1.1`	Configure a virtual link between this router R1 and R2 (Router ID `1.1.1.1`) through transit area 1.

R4

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.

© 2021 IP Infusion Inc. Proprietary

(config-if)#ipv6 router ospf area 1	Enable OSPFv3 routing on this interface, and assign the Area ID (1).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router ospf area 1	Enable OSPFv3 routing on this interface, and assign the Area ID (1).
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 4.4.4.4	Specify a Router ID (4.4.4.4) for the OSPFv3 routing process.

R5

#configure terminal	Enter configure mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router ospf area 2	Enable OSPFv3 routing on this interface, and assign the Area ID (2).
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 5.5.5.5	Specify a Router ID (5.5.5.5) for the OSPFv3 routing process.

R6

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on this interface, and assign the Area ID (0).
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 6.6.6.6	Specify a Router ID (6.6.6.6) for the OSPFv3 routing process.

Validation

R2

```
#show ipv6 ospf n
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/DR         00:00:31    eth1       0
3.3.3.3           1   Full/DR         00:00:32    eth2       0
2.2.2.2           1   Full/ -         inactive    VLINK2147479553 0


#show ipv6 ospf virtual-links
Virtual Link VLINK2147479553 to router 2.2.2.2 is up
```

```
  Transit area 0.0.0.1 via interface eth2, instance ID 0
  Hello suppression Enabled
  DoNotAge LSA allowed
  Local address 2ffe::11/128
  Remote address 3ffe::11/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in inactive
    Adajcency state Full


# show ipv6 ospf
 Routing Process "OSPFv3 (*null*)" with ID 1.1.1.1
 Process uptime is 5 minutes
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
 This router is an ASBR (injecting external routing information)
 SPF schedule delay initial 0.500 secs
 SPF schedule delay min 0.500 secs
 SPF schedule delay max 50.0 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 17
 Number of LSA received 50
 Number of areas in this router is 2
    Area BACKBONE(0)
        Number of interfaces in this area is 2(2)
        SPF algorithm executed 8 times
        Number of LSA 23.  Checksum Sum 0xB35D8
        Number of Unknown LSA 0
    Area 0.0.0.1
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 13 times
        Number of LSA 16.  Checksum Sum 0x7845A
        Number of Unknown LSA 0
 Dste Staus: Disabled


#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  1ffe::/64                                         1
     directly connected, eth1, Area 0.0.0.0
```


© 2021 IP Infusion Inc. Proprietary

```
C  2ffe::/64                                          1
     directly connected, eth2, TransitArea 0.0.0.1
C  2ffe::11/128                                       0
     directly connected, eth2, TransitArea 0.0.0.1
O  3ffe::/64                                          1
     directly connected, eth2, TransitArea 0.0.0.1
O  3ffe::11/128                                       2
     via fe80::5054:ff:fe6f:334d, eth2, TransitArea 0.0.0.1
IA 4ffe::/64                                          3
     via fe80::5054:ff:fe6f:334d, eth2, TransitArea 0.0.0.1
#
```

R3

```
#show ipv6 ospf n
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:00:35    eth1       0
2.2.2.2           1   Full/Backup     00:00:30    eth2       0


# show ipv6 ospf
 Routing Process "OSPFv3 (*null*)" with ID 3.3.3.3
 Process uptime is 5 minutes
 This router is an ASBR (injecting external routing information)
 SPF schedule delay initial 0.500 secs
 SPF schedule delay min 0.500 secs
 SPF schedule delay max 50.0 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 10
 Number of LSA received 23
 Number of areas in this router is 1
    Area 0.0.0.1
        Number of interfaces in this area is 2(2)
        SPF algorithm executed 14 times
        Number of LSA 16.  Checksum Sum 0x7845A
        Number of Unknown LSA 0
 Dste Staus: Disabled


#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                  Metric
```

```
     Next-hop
IA 1ffe::/64                                          2
     via fe80::5054:ff:feb7:cc69, eth1, TransitArea 0.0.0.1
C  2ffe::/64                                          1
     directly connected, eth2, TransitArea 0.0.0.1
O  2ffe::11/128                                       1
     via fe80::5054:ff:feb7:cc69, eth1, TransitArea 0.0.0.1
C  3ffe::/64                                          1
     directly connected, eth1, TransitArea 0.0.0.1
O  3ffe::11/128                                       1
     via fe80::5054:ff:fec5:2430, eth2, TransitArea 0.0.0.1
IA 4ffe::/64                                          2
     via fe80::5054:ff:fec5:2430, eth2, TransitArea 0.0.0.1
```

R4

```
#show ipv6 ospf n
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
3.3.3.3           1   Full/DR         00:00:31    eth1       0
1.1.1.1           1   Full/ -         inactive    VLINK2147479554 0


#show ipv6 ospf virtual-links
Virtual Link VLINK2147479554 to router 1.1.1.1 is up
  Transit area 0.0.0.1 via interface eth1, instance ID 0
  Hello suppression Enabled
  DoNotAge LSA allowed
  Local address 3ffe::11/128
  Remote address 2ffe::11/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in inactive
    Adajcency state Full


# show ipv6 ospf
 Routing Process "OSPFv3 (*null*)" with ID 2.2.2.2
 Process uptime is 4 minutes
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
 This router is an ASBR (injecting external routing information)
 SPF schedule delay initial 0.500 secs
 SPF schedule delay min 0.500 secs
 SPF schedule delay max 50.0 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 26
 Number of LSA received 37
```


© 2021 IP Infusion Inc. Proprietary

```
 Number of areas in this router is 3
    Area BACKBONE(0)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 3 times
        Number of LSA 23.  Checksum Sum 0xB35D8
        Number of Unknown LSA 0
    Area 0.0.0.1
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 11 times
        Number of LSA 16.  Checksum Sum 0x7845A
        Number of Unknown LSA 0
    Area 0.0.0.2
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 4 times
        Number of LSA 11.  Checksum Sum 0x5D8B7
        Number of Unknown LSA 0
 Dste Staus: Disabled


#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
O  1ffe::/64                                        3
     via fe80::5054:ff:fe1d:eace, eth1, TransitArea 0.0.0.1
O  2ffe::/64                                        1
     directly connected, eth1, TransitArea 0.0.0.1
O  2ffe::11/128                                     2
     via fe80::5054:ff:fe1d:eace, eth1, TransitArea 0.0.0.1
C  3ffe::/64                                        1
     directly connected, eth1, TransitArea 0.0.0.1
C  3ffe::11/128                                    0
     directly connected, eth1, TransitArea 0.0.0.1
C  4ffe::/64                                        1
     directly connected, eth2, Area 0.0.0.2
```

Multiple Instances

By using multiple OSPFv3 instances, OSPFv3 routes can be segregated, based on their instance number. Routes of one instance are stored differently from routes of another instance running in the same router.

To configure multiple OSPFv3 instances, refer to the topology diagram and follow the procedures below.

1. Enable OSPFv3 on an interface.
2. Enable multiple instances.

3. Configure redistribution among multiple instances.

   Note: Optionally, redistribution can be configured with the metric, type, or route-map options.

Topology

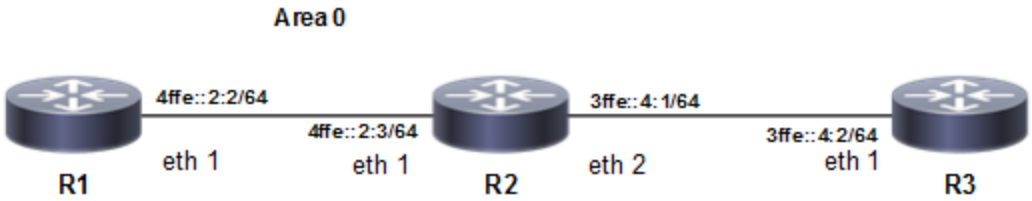


Figure 5-105: Multiple OSPFv3 Instances

Enable OSPFv3 on an Interface

This example shows how to enable OSPFv3 on an interface. R1 and R2 are two routers in Area 0 connecting to network 4ffe::2:/64.

R1

`(config)#router ipv6 ospf 10`	Configure an OSPFv3 instance with an instance ID of `10`.
`(config-router)#router-id 151.151.151.151`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit Router mode, and return to Interface mode.
`(config)#interface eth1`	Specify the interface on which OSPFv3 is to be enabled.
`(config-if)#ipv6 address 4ffe::2:2/64`	Configure the IPv6 address.
`(config-if)#ipv6 router ospf area 0 tag 10`	Configure the area number and instance value: match the instance ID with the instance ID created previously.
`(config-if)#no shutdown`	Activate the interface.

R2

`(config)#router ipv6 ospf 10`	Configure an OSPFv3 instance with an instance ID of `10`.
`(config-router)#router-id 152.152.152.152`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit Router mode, and return to Interface mode.
`(config)#interface eth1`	Specify the interface on which OSPFv3 is to be enabled.
`(config-if)#ipv6 address 4ffe::2:3/64`	Configure the IPv6 address.
`(config-if)#ipv6 router ospf area 0 tag 10`	Configure the area number and instance value: match the instance ID with the instance ID created previously.
`(config-if)#no shutdown`	Activate the interface.

Validation

R1

```
#show running-config
!
```


© 2021 IP Infusion Inc. Proprietary

```
!Last configuration change at 11:33:37 EDT Tue Mar 12 2019 by ocnos
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
feature telnet
feature ssh
snmp-server enable snmp
snmp-server view all .1 included
feature ntp
ntp enable
username ocnos role network-admin password encrypted
$1$qLd1Mdn0$rrz9r.00v.xla6xd2KDw91
feature rsyslog
!
interface lo
 ip address 127.0.0.1/8
 ip address 151.151.151.151/32 secondary
 ipv6 address ::1/128
 mtu 65536
!
interface eth0
 ip address 192.168.20.2/24
!
interface eth1
 ipv6 address 4ffe::2:2/64
 ipv6 router ospf area 0.0.0.0 tag 10
!
interface eth2
!
interface eth3
!
router ipv6 ospf 10
 router-id 151.151.151.151
!
line con 0
 login
line vty 0 39
 login
!
end

#show ipv6 interface brief
Interface            IPv6-Address                                  Admin-
Status
eth3                 fe80::5054:ff:fe44:c9f9                       [up/up]
eth2                 fe80::5054:ff:fe49:d3ec                       [up/up]
eth1                 4ffe::2:2
                     fe80::5054:ff:fef3:2245                       [up/up]
eth0                 fe80::5054:ff:fec8:55b1                       [up/up]
lo                   ::1                                           [up/up]

#show ipv6 ospf route
```

```
OSPFv3 Process (10)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                      Metric
     Next-hop
IA 3ffe::/64                                          2
     via fe80::5054:ff:fe22:ed80, eth1, Area 0.0.0.0
C  4ffe::/64                                          1
     directly connected, eth1, Area 0.0.0.0

#show ipv6 ospf neighbor
OSPFv3 Process (10)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.14.14       1   Full/DROther    00:00:34    eth1       0
152.152.152.152   1   Full/DR         00:00:34    eth1       0
```

R2

```
#show running-config
!
!Last configuration change at 12:34:42 EDT Tue Mar 12 2019 by ocnos
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
feature telnet
feature ssh
snmp-server enable snmp
snmp-server view all .1 included
feature ntp
ntp enable
username ocnos role network-admin password encrypted $1$YLcV3GI1$TV02h9a0/
z2oPtHU95f02/
feature rsyslog
!
interface lo
 ip address 127.0.0.1/8
 ip address 152.152.152.152/32 secondary
 ipv6 address ::1/128
 mtu 65536
!
interface eth0
 ip address 192.168.20.3/24
!
interface eth1
 ipv6 address 4ffe::2:3/64
 ipv6 router ospf area 0.0.0.0 tag 10
!
interface eth2
!
```


© 2021 IP Infusion Inc. Proprietary

```
router ipv6 ospf 10
 router-id 152.152.152.152
!
line con 0
 login
line vty 0 39
 login
!
end

#show ipv6 interface brief
Interface            IPv6-Address                                    Admin-
Status
eth2                 fe80::5054:ff:fe39:f13f                         [up/up]
eth1                 4ffe::2:3
                     fe80::5054:ff:febc:57d                          [up/up]
eth0                 fe80::5054:ff:fea2:3f3                          [up/up]
lo                   ::1                                             [up/up]

#show ipv6 ospf route
OSPFv3 Process (10)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
IA 3ffe::/64                                        2
     via fe80::5054:ff:fe22:ed80, eth1, Area 0.0.0.0
C  4ffe::/64                                        1
     directly connected, eth1, Area 0.0.0.0

#show ipv6 ospf neighbor
OSPFv3 Process (10)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.14.14       1   Full/DROther    00:00:39    eth1       0
151.151.151.151   1   Full/Backup     00:00:40    eth1       0
```

Enable Multiple OSPFv3 Instances on a Router Based on Tags

In this example, routers R1, R2, and R3 are in Area 0, and all run OSPFv3.

R1

`(config)#router ipv6 ospf 5`	Configure an OSPFv3 instance with an instance ID of `5`.
`(config-router)#router-id 5.5.5.5`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit Router mode, and return to Interface mode.
`(config)#interface eth1`	Specify the interface on which OSPFv3 is to be enabled.
`(config-if)#ipv6 address 4ffe::2:2/64`	Configure the IPv6 address.
`(config-if)#ipv6 router ospf area 0 tag 5`	Configure the area number and instance value: match the instance ID with the instance ID created previously.
`(config-if)#no shutdown`	Activate the interface.

R2

`(config)#router ipv6 ospf 5`	Configure an OSPFv3 instance with an instance ID of `5`.
`(config-router)#router-id 149.149.149.149`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit Router mode, and return to Interface mode.
`(config)#interface eth1`	Configure the interface to connect to R1.
`(config-if)#ipv6 address 4ffe::2:3/64`	Configure the IPv6 address.
`(config-if)#ipv6 router ospf area 0 tag 5`	Configure the area number and instance value: match the instance ID with the instance ID created previously.
`(config-if)#no shutdown`	Activate the interface.
`(config)#router ipv6 ospf 15`	Configure an OSPFv3 instance with an instance ID of `15`.
`(config-router)#router-id 159.159.159.159`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit Router mode, and return to Interface mode.
`(config)#interface eth2`	Configure the interface to connect to R3.
`(config-if)#ipv6 address 3ffe::4:1/64`	Configure the IPv6 address.
`(config-if)#no shutdown`	Activate the interface.
`(config-if)#ipv6 router ospf area 0 tag 15`	Configure the area number and instance value: match the instance ID with the instance ID created previously.

R3

`(config)#router ipv6 ospf 15`	Configure an OSPFv3 instance with an instance ID of `15`.
`(config-router)#router-id 152.152.152.152`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit Router mode, and return to Interface mode.
`(config)#interface eth1`	Specify the interface on which OSPFv3 is to be enabled.
`(config-if)#ipv6 address 3ffe::4:2/64`	Configure the IPv6 address.
`(config-if)#ipv6 router ospf area 0 tag 15`	Configure the area number and instance value: match the instance ID with the instance ID created previously.
`(config-if)#no shutdown`	Activate the interface.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                        1
     directly connected, eth1, Area 0.0.0.0

R1#show ipv6 ospf neighbor
OSPFv3 Process (5)
```


© 2021 IP Infusion Inc. Proprietary

```
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
149.149.149.149   1   Full/Backup     00:00:32    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth2, Area 0.0.0.0
O  3ffe:12::/64                                       1
     directly connected, eth2, Area 0.0.0.0
O  3ffe:13::/64                                       2
     via fe80::a00:27ff:fe01:c94d, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                        1
     directly connected, eth1, Area 0.0.0.0

R2#sh ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
152.152.152.152   1   Full/DR         00:00:35    eth2       0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
5.5.5.5           1   Full/DR         00:00:33    eth1       0
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth1, Area 0.0.0.0
O  3ffe:12::/64                                       1
     directly connected, eth1, Area 0.0.0.0
O  3ffe:13::/64                                       2
     via fe80::a00:27ff:fe01:c94d, eth1, Area 0.0.0.0



R3#sh ipv6 ospf neighbor
OSPFv3 Process (15)
```

```
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
159.159.159.159   1   Full/Backup     00:00:34    eth1       0
```

Redistribute among Multiple Instances

In this example, routes of one instance are redistributed to another instance to enable ping from R1 to R3 or vice versa; and R2 redistributes routes from one instance to another.

R2

(config)#router ipv6 ospf 15	Configure an OSPFv3 instance with instance ID 15.
(config-router)#router-id 159.159.159.159	Configure the router ID.
(config-router)#redistribute ospf 5	Redistribute instance 5 routes.
(config-router)#redistribute connected	Redistribute co routes to instance 15.
(config-router)#exit	Exit OSPF router mode.
(config)#router ipv6 ospf 5	Configure an OSPFv3 instance with instance ID 5.
(config-router)#router-id 149.149.149.149	Configure the router ID.
(config-router)#redistribute ospf 15	Redistribute instance 15 routes.
(config-router)#redistribute connected	Redistribute connected routes to instance 5.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
E2 3ffe:4::/64                                      1/20
     via fe80::a00:27ff:fef9:2432, eth1
C  4ffe:2::/64                                         1
     directly connected, eth1, Area 0.0.0.0


rtr1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
149.149.149.149   1   Full/Backup     00:00:32    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```


© 2021 IP Infusion Inc. Proprietary

```
   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                        1
     directly connected, eth1, Area 0.0.0.0

R2#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
152.152.152.152   1   Full/DR         00:00:34    eth2       0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
5.5.5.5           1   Full/DR         00:00:30    eth1       0
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth1, Area 0.0.0.0
E2 4ffe:2::/64                                      1/20
     via fe80::a00:27ff:fe0d:fbe3, eth1


R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
159.159.159.159   1   Full/Backup     00:00:33    eth1       0
```

Redistribute with Metric Option

In this example, on R3, R1 and R2 have each other's routes with a metric of 100.

R2

`(config)#router ipv6 ospf 15`	Configure an OSPFv3 instance with instance ID `15`.
`(config-router)#router-id 159.159.159.159`	Configure the router ID.

`(config-router)#redistribute ospf 5 metric 100`	Redistribute instance `15` routes with metric `100`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#router ipv6 ospf 5`	Redistribute routes into instance `5`.
`(config-router)#router-id 149.149.149.149`	Configure the router ID.
`(config-router)#redistribute ospf 15 metric 100`	Redistribute instance `15` routes with metric `100`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `5`.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
E2 3ffe:4::/64                                      1/20
     via fe80::a00:27ff:fef9:2432, eth1
C  4ffe:2::/64                                         1
     directly connected, eth1, Area 0.0.0.0

R1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
149.149.149.149   1   Full/Backup     00:00:36    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                         1
     directly connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                         1
```


© 2021 IP Infusion Inc. Proprietary

```
      directly connected, eth1, Area 0.0.0.0


R2#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
152.152.152.152   1   Full/DR         00:00:33    eth2       0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
5.5.5.5           1   Full/DR         00:00:40    eth1       0
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth1, Area 0.0.0.0
E2 4ffe:2::/64                                      1/20
     via fe80::a00:27ff:fe0d:fbe3, eth1


R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
159.159.159.159   1   Full/Backup     00:00:37    eth1       0
```

Redistribute with Type Option

In this example, on R3, R1 has R3 routes as type 2, and R2 has R1 routes as type 1.

R2

`(config)#router ipv6 ospf 15`	Configure an OSPFv3 instance with instance ID `15`.
`(config-router)#router-id 159.159.159.159`	Configure the router ID.
`(config-router)#redistribute ospf 5 metric-type 1`	Redistribute instance `15` routes as type `1`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#router ipv6 ospf 5`	Redistribute routes into instance `5`.
`(config-router)#router-id 149.149.149.149`	Configure the router ID.

`(config-router)#redistribute ospf 15 metric-type 2`	Redistribute instance `15` routes with type `2`.
`(config-router)#redistribute connected`	Redistribute instance `15` as type `2`.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
E2 3ffe:4::/64                                      1/20
     via fe80::a00:27ff:fef9:2432, eth1
C  4ffe:2::/64                                         1
     directly connected, eth1, Area 0.0.0.0


rtr1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
149.149.149.149   1   Full/Backup     00:00:32    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                         1
     directly connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                         1
     directly connected, eth1, Area 0.0.0.0

R2#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
```


© 2021 IP Infusion Inc. Proprietary

```
152.152.152.152   1   Full/DR         00:00:36    eth2       0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
5.5.5.5           1   Full/DR         00:00:32    eth1       0
```

R3

```
R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
159.159.159.159   1   Full/Backup     00:00:36    eth1       0
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1
     directly connected, eth1, Area 0.0.0.0
E2 4ffe:2::/64                                     1/20
     via fe80::a00:27ff:fe0d:fbe3, eth1


R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
159.159.159.159   1   Full/Backup     00:00:36    eth1       0
```

Redistribute with Route-Map Option

R2

`(config)#router ipv6 ospf 15`	Configure an OSPFv3 instance with instance ID `15`.
`(config-router)#router-id 159.159.159.159`	Configure the router ID.
`(config-router)#redistribute ospf 5 route-map 1`	Redistribute instance `5` routes with route map `1`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#router ipv6 ospf 5`	Redistribute routes into instance `5`.
`(config-router)#router-id 149.149.149.149`	Configure the router ID.
`(config-router)#redistribute ospf 15 route-map 1`	Redistribute instance `15` routes with route map `1`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
E2 3ffe:4::/64                                      1/20
     via fe80::a00:27ff:fef9:2432, eth1
C  4ffe:2::/64                                         1
     directly connected, eth1, Area 0.0.0.0


R1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
149.149.149.149   1   Full/DR         00:00:34    eth1       0
```

R2

```
R2#sh ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                         1
     directly connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                         1
     directly connected, eth1, Area 0.0.0.0

R2#sh ipv6  ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
152.152.152.152   1   Full/Backup     00:00:32    eth2       0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
5.5.5.5           1   Full/Backup     00:00:38    eth1       0
```

R3

```
R3#show ipv6 ospf route
```


© 2021 IP Infusion Inc. Proprietary

```
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                        Metric
     Next-hop
C  3ffe:4::/64                                           1
     directly connected, eth1, Area 0.0.0.0
E2 4ffe:2::/64                                         1/20
     via fe80::a00:27ff:fe0d:fbe3, eth1

R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
159.159.159.159   1   Full/DR         00:00:34    eth1       0
R3#
```

Graceful Restart

The possibility of maintaining a router's data forwarding capability while the router's control software restarts is called graceful restart or non-stop forwarding. After the router restarts and reloads, it must change its OSPF processing until it re-establishes full adjacencies with all its former fully adjacent neighbors. The time period between the restart/reload and re-establishment of adjacencies is called the grace period.

Essentially, the OSPF procedure for graceful restart is as follows:

- The router attempting a graceful restart originates link-local Opaque-LSAs, called Grace-LSAs, announcing its intention to perform a graceful restart within a specified amount of time (grace period).
- During the grace period, neighbors continue to announce the restarting router in their LSAs as if it were fully adjacent (OSPF neighbor state Full), but only if the network topology remains static (the contents of the LSAs in the link-state database that have LS types 1-5 and 7 remain unchanged, and periodic refreshes are allowed).

Topology

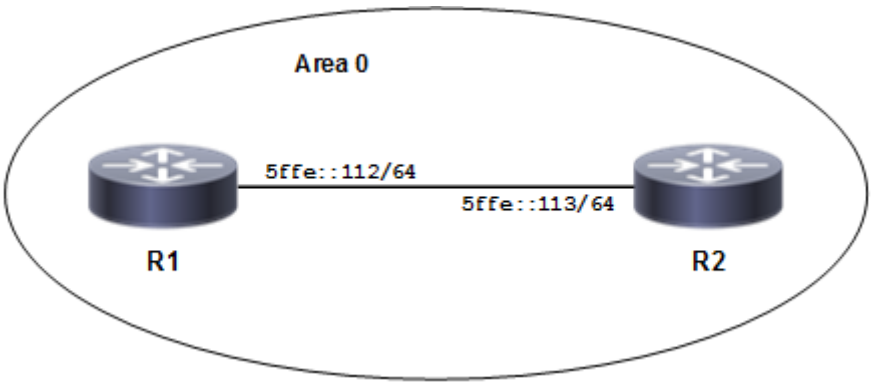


Figure 5-106: OSPFv3 Graceful Restart

Configure R1 for Graceful Restart

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 5ffe::112/64`	Assign the IPv6 address to the interface.
`(config-if)#ipv6 router ospf area 0 tag 1`	Configure the interface for OSPFv3 on area 0.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 1`	Create an OSPFv3 routing instance.
`(config-router)#router-id 1.1.1.1`	Specify a Router ID (`1.1.1.1`) for the OSPFv3 routing process.
`(config-router)#capability restart graceful`	Enable graceful restart capability.
`(config-router)#end`	Exit Configure mode and enter Privileged Exec mode.
`#write`	Save the configuration.
`#restart ipv6 ospf graceful grace-period 200`	Restart OSPFv3 with a 200-second grace period, so that the neighbor maintains adjacency and preserves the routes for 200 seconds.

Configure R2 as Restart Helper

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 5ffe::113/64`	Assign the IPv6 address to the interface.
`(config-if)#ipv6 router ospf area 0 tag 1`	Configure the interface for OSPFv3 on area 0.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 1`	Create an OSPFv3 routing instance.
`(config-router)#router-id 2.2.2.2`	Specify a Router ID (`2.2.2.2`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit Router mode and enter Configure mode.
`(config)#ipv6 ospf restart helper max-grace-period 300`	Configure R2 to act as the helper when the grace period is less than 300.

Remove Helper Configuration from R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 1`	Create an OSPFv3 routing instance.
`(config-router)#router-id 1.1.1.1`	Specify a Router ID (`1.1.1.1`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit Router mode and enter Configure mode.
`(config)#ipv6 ospf restart helper never`	Configure R2 to not work as the helper.

© 2021 IP Infusion Inc. Proprietary

Make R2 Helper when Restart Reason is Reload

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 1`	Create an OSPFv3 routing instance.
`(config-router)#router-id 1.1.1.1`	Specify a Router ID (`1.1.1.1`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit Router mode and enter Configure mode.

Make R2 Helper when Restart Reason is Upgrade

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 1`	Create an OSPFv3 routing instance.
`(config-router)#router-id 1.1.1.1`	Specify a Router ID (`1.1.1.1`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit Router mode and enter Configure mode.

Validation

R1 After Configuring Graceful Restart

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/DR         00:00:39    eth1       0


R1#show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                         1
     directly connected, eth1, Area 0.0.0.0


rtr1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 02:02:28
C      5ffe::/64 via ::, eth1, 00:23:16
C      fe80::/64 via ::, eth1, 01:25:04
```

```
K      ff00::/8 [0/256] via ::, eth0, 01:25:05


rtr1#show ipv6 ospf database grace

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
```

R1 After Graceful Restart (after starting ospf6d daemon manually)

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/DR         00:00:37    eth1       0


rtr1#show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                          1
     directly connected, eth1, Area 0.0.0.0


rtr1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 02:02:28
C      5ffe::/64 via ::, eth1, 00:23:16
C      fe80::/64 via ::, eth1, 01:25:04
K      ff00::/8 [0/256] via ::, eth1, 01:25:05


rtr1#show ipv6 ospf database grace

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
```

R2 Before Graceful Restart

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:00:40    eth1       0


R2#sh ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
```

 © 2021 IP Infusion Inc. Proprietary

```
1.1.1.1           1   Full/Backup     00:00:40    eth1       0
R2#
R2#show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                         1
     directly connected, eth1, Area 0.0.0.0


R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:54:20
C      5ffe::/64 via ::, eth1, 00:12:16
C      fe80::/64 via ::, eth2, 01:17:21
K      ff00::/8 [0/256] via ::, eth1, 01:19:12


R2#show ipv6 ospf database grace

            OSPFv3 Router with ID (2.2.2.2) (Process 1)
```

R2 During graceful restart

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:02:25*    eth1       0


R2#show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                         1
     directly connected, eth1, Area 0.0.0.0


R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
```

```
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:57:26
C      5ffe::/64 via ::, eth1, 00:15:22
C      fe80::/64 via ::, eth2, 01:20:27
K      ff00::/8 [0/256] via ::, eth1, 01:22:18


R2#show ipv6 ospf database grace

            OSPFv3 Router with ID (2.2.2.2) (Process 1)

                Grace-LSA (Interface eth1)

  LS age: 65
  LS Type: Grace LSA
  Link State ID: 0.0.0.3
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000001
  Checksum: 0x1660
  Length: 36

      Grace Period: 200
      Restart Reason:
           Software Restart
```

R2 After graceful restart

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:00:34    eth1       0



R2#show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                  Metric
     Next-hop
C  5ffe::/64                                       1
     directly connected, eth1, Area 0.0.0.0


R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime
```


© 2021 IP Infusion Inc. Proprietary

```
IP Route Table for VRF "default"
C       ::1/128 via ::, lo, 02:07:14
C       5ffe::/64 via ::, eth1, 00:25:10
C       fe80::/64 via ::, eth2, 01:30:15
K       ff00::/8 [0/256] via ::, eth2, 01:30:17

R2#show ipv6 ospf database grace

            OSPFv3 Router with ID (2.2.2.2) (Process 1)
```

Not-So-Stubby Area

This section contains OSPFv3 NSSA (Not-So-Stubby Area) configuration examples.

An NSSA allows external routes to be advertised into the OSPF autonomous system while retaining the characteristics of a stub area to the rest of the autonomous system. To do this, the ASBR in an NSSA will originate type 7 LSAs to advertise the external destinations. These NSSA external LSAs are flooded throughout the NSSA but are blocked at the ABR.

The NSSA external LSA has a flag in its header known as the P-bit. The NSSA ASBR has the option of setting or clearing the P-bit. If an NSSA's ABR receives a type 7 LSA with the P-bit set to one, it translates the type 7 LSA into a type 5 LSA and floods it throughout the other areas. If the P-bit is set to zero, no translation takes place and the destination in the type 7 LSA is not advertised outside of the NSSA.

Topology

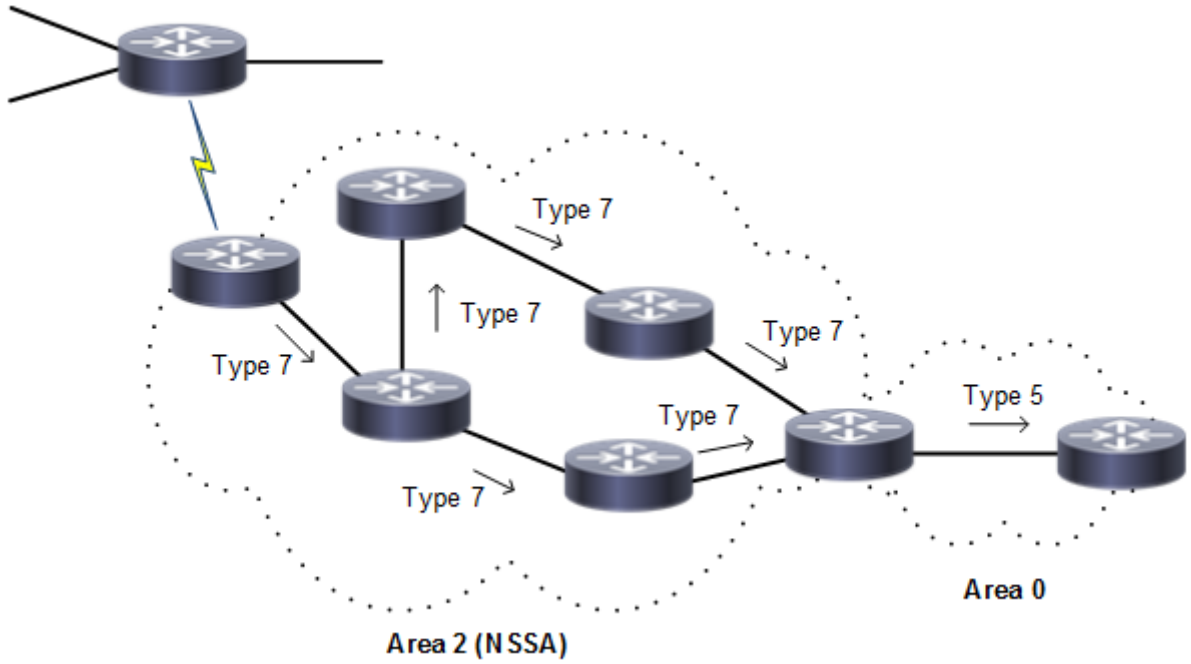


Figure 5-107: Translating Type 7 LSAs into Type 5 LSAs

NSSA with Route Options

This example shows the configuration to enable NSSA and to configure different route options for NSSA. There are three `area nssa` command options for originating default Type-3 LSA and default Type-7 LSA, and for blocking redistribution of Type-7 LSA into an NSSA:

- `no-summary`: The NSSA ABR blocks all type-3 and type-4 LSAs into the NSSA area and sends a single type-3 LSA into the area to advertise a default route
- `default-information-originate`: The NSSA ABR advertises a default route into the NSSA as a type-7 LSA.
- `no-redistribution`: The NSSA ABR bocks type-7 LSA from being redistributed into the NSSA area.

In Figure 5-108, R2 is an NSSA ABR as well as an NSSA ASBR that maps the router interfaces to two different areas and redistributes the connected routes of the loopback interface. Also, this example sets the `no-summary`, `no-redistribution`, and `default-information-originate` options on R2 to originate default Type-3 LSAs and default Type-7 LSAs into the NSSA and to block Type-7 LSAs.

Topology

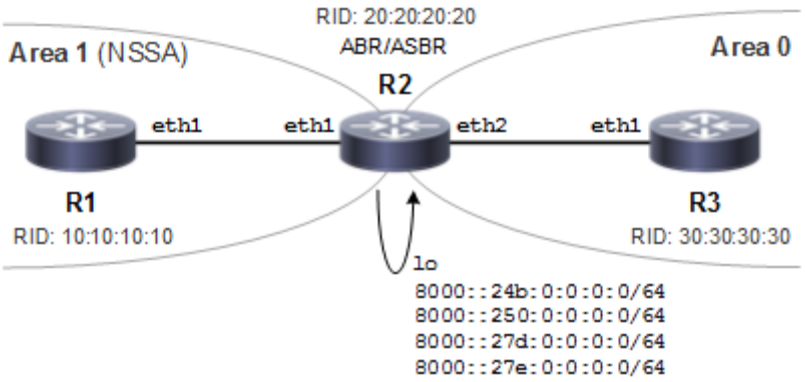


Figure 5-108: NSSA with Route Options

R1

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 10.10.10.10`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa`	Configure area as NSSA
`(config-router)#exit`	Exit interface mode

R2

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`

© 2021 IP Infusion Inc. Proprietary

(config-if)#ipv6 router ospf tag 100 area 0	Configure interface in backbone
(config-if)#interface lo	Enter interface mode for Loopback
(config-if)#ipv6 address 8000::24b:0:0:0:0/64	Assign IPv6 address to loopback interface
(config-if)#ipv6 address 8000::250:0:0:0:0/64	Assign IPv6 address to loopback interface
(config-if)#ipv6 address 8000::27d:0:0:0:0/64	Assign IPv6 address to loopback interface
(config-if)#ipv6 address 8000::27e:0:0:0:0/64	Assign IPv6 address to loopback interface
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 100	Configure the routing process and specify the tag (100).
(config-router)#router-id 20.20.20.20	Configure the router ID to use on this instance (100)
(config-router)#redistribute connected	Redistribute the configured loopback network into the NSSA
(config-router)#area 1 nssa no-redistribution default-information-originate no-summary	Configure the Router to originate default Type-3 LSAs and default Type-7 LSAs, and to block Type-7 LSAs into the NSSA
(config-router)#exit	Exit interface mode

R3

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ipv6 router ospf tag 100 area 0	Configure interface in an area assigned with the area ID (1).
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 100	Configure the routing process and specify the tag (100).
(config-router)#router-id 30.30.30.30	Configure the router ID to use on this instance (100)
(config-router)#exit	Exit interface mode

Validation 1

In the output of show ipv6 ospf neighbor below, verify that OSPFv3 adjacency is in state “full” for both R1 and R2 under the process identifier 100.

```
R1#sh ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
20.20.20.20       1   Full/DR         00:00:34    eth2       0

R2#sh ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/Backup     00:00:38    eth1       0
```

Validation 2

The output below shows originating default Type-3 LSAs into the NSSA with the no-summary option. The advertising router identifier is for R2 (20.20.20.20, the NSSA-ABR). Also, the prefix is ::/0 and the LS-Type is Inter-Area-Prefix-LSA for the default Type-3 LSA route into the NSSA.

```
R1#sh ipv6 ospf database inter-prefix

            OSPFv3 Router with ID (10.10.10.10) (Process 100)

                Inter-Area-Prefix-LSA (Area 0.0.0.1)

  LS age: 1234
  LS Type: Inter-Area-Prefix-LSA
  Link State ID: 0.0.0.6
  Advertising Router: 20.20.20.20
  LS Seq Number: 0x80000001
  Checksum: 0x17D0
  Length: 28
    Metric: 1
    Prefix: ::/0
    Prefix Options: 0
```

Validation 3

The output below shows originating default type-7 LSAs alone after setting the no-redistribution and default-information originate options. The advertising router identifier is for R2 (20.20.20.20, the NSSA-ABR). Also, the prefix is ::/0 and LS-Type is NSSA-external-LSA for the default Type-7 LSA route into the NSSA

```
R1#sh ipv6 ospf database nssa-external

            OSPFv3 Router with ID (10.10.10.10) (Process 100)

                NSSA-external-LSA (Area 0.0.0.1)

  LS age: 1758
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.20
  Advertising Router: 20.20.20.20
  LS Seq Number: 0x80000002
  Checksum: 0x6468
  Length: 32
    Metric Type: 2 (Larger than any link state path)
    Metric: 1
    Prefix: ::/0
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 0
```

NSSA with the Summary Address Option

Figure 5-109 shows the configuration to originate external LSAs (Type-7) and translate them into external LSAs (Type-5):

- R1 is an NSSA-ASBR configured with loopback IPv6 addresses that are redistributed into OSPFv3
- R2 is an NSSA-ABR
- R3 is backbone router

R1 originates Type-7 LSAs which are summarized into a single Type-7 into the NSSA by the `summary-address` option and this summarized Type-7 is converted to Type-5 LSA by R2.

© 2021 IP Infusion Inc. Proprietary

Also, the summarized route can be tagged using the `tag` command and the advertisement of summarized routes can be suppressed by the `not-advertise` option.

Topology

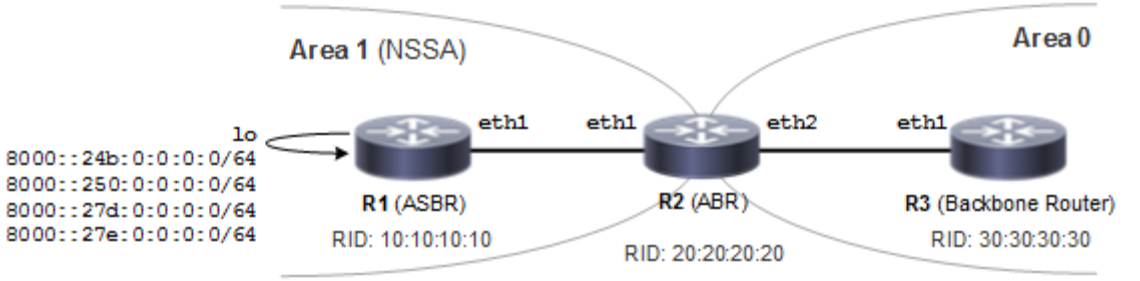


Figure 5-109: Using the summary-address Option

Configuration

R1

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config-if)#interface lo`	Enter interface mode for loopback
`(config-if)#ipv6 address 8000::24b:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::250:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::27d:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::27e:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 10.10.10.10`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa`	Configure the area as NSSA.
`(config-router)#redistribute connected`	Redistribute the configured loopback network into OSPFv3 NSSA. Note: Connected networks can be redistributed by setting the metric and metric type.
`(config-router)#summary-address 8000::/48 all-tag 10`	Summarize the address range and tag the summarized route
`(config-router)#exit`	Exit interface mode

R2

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone area (0)
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 20.20.20.20`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa`	Configure the Router in NSSA
`(config-router)#exit`	Exit interface mode

R3

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone area (0)
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 30.30.30.30`	Configure the router ID to use on this instance (100)
`(config-router)#exit`	Exit interface mode

In the configurations above, you can suppress the external route summarization by NSSA-ASBR by specifying the `not-advertise` parameter as shown below:

```
(config-router)#summary-address 8000::/48 not-advertise
```

Also, connected networks can be redistributed by setting the metric and metric type as shown below:

```
(config-router)#redistribute connected metric 20 metric-type 1
```

Validation 1

The output below shows the summarized route generated by NSSA-ASBR (R1) with a tag. The output has the LS Type as NSSA-external-LSA with advertising router identifier (10.10.10.10) of the NSSA-ASBR (R1). Also, check the Prefix which is summarized route and external route tag as configured.

```
R1#sh ipv6 ospf database nssa-external

            OSPFv3 Router with ID (10.10.10.10) (Process 100)

                NSSA-external-LSA (Area 0.0.0.1)

  LS age: 90
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.11
  Advertising Router: 10.10.10.10
  LS Seq Number: 0x80000003
  Checksum: 0x69B3
  Length: 40
    Metric Type: 2 (Larger than any link state path)
```


© 2021 IP Infusion Inc. Proprietary

```
    Metric: 21
    Prefix: 8000::/48
    Prefix Options: 8 (P|-|-|-)
    External Route Tag: 10
```

Validation 2

```
The output below on the NSSA-ABR that is translating Type-7 LSAs to Type-5
LSAs shows summarized address in Type-7 and Type-5 LSA. Check for the same
prefix, external route tag in both Type7 and Type-5 LSA.
R2#sh ipv6 ospf database nssa-external

            OSPFv3 Router with ID (20.20.20.20) (Process 100)

                NSSA-external-LSA (Area 0.0.0.1)

  LS age: 241
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.11
  Advertising Router: 10.10.10.10
  LS Seq Number: 0x80000003
  Checksum: 0x69B3
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 21
    Prefix: 8000::/48
    Prefix Options: 8 (P|-|-|-)
    External Route Tag: 10

R2#sh ipv6 ospf database external

            OSPFv3 Router with ID (20.20.20.20) (Process 100)

                AS-external-LSA

  LS age: 245
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.3
  Advertising Router: 20.20.20.20
  LS Seq Number: 0x80000003
  Checksum: 0x8660
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 21
    Prefix: 8000::/48
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 10
```

Validation 3

The output below on the backbone router shows the summarized address in the translated Type-5 LSA. The prefix and external route tag are the same as the summarized Type-7 LSA originated by R1.

```
R3#sh ipv6 ospf database external

            OSPFv3 Router with ID (30.30.30.30) (Process 100)
```

```
                AS-external-LSA

    LS age: 409
    LS Type: AS-External-LSA
    Link State ID: 0.0.0.3
    Advertising Router: 20.20.20.20
    LS Seq Number: 0x80000003
    Checksum: 0x8660
    Length: 40
      Metric Type: 2 (Larger than any link state path)
      Metric: 21
      Prefix: 8000::/48
      Prefix Options: 0 (-|-|-|-)
      External Route Tag: 10
```

NSSA with the Translator Role Option

Type-7 to Type-5 translation is done by an NSSA-ABR. If an NSSA has multiple NSSA-ABRs, only one will perform the translation. The NSSA-ABR translator role options are:

- Candidate (default)
- Always

In the topology in Figure 5-110:

- R1 is NSSA-ASBR
- R2 and R3 are NSSA-ABRs
- R4 is a backbone router

In this example, the NSSA translator role `candidate` is configured on both NSSA-ABRs (R2 and R3). The Type-7 to Type-5 translation is done by the router with the higher router identifier (R3).

Topology

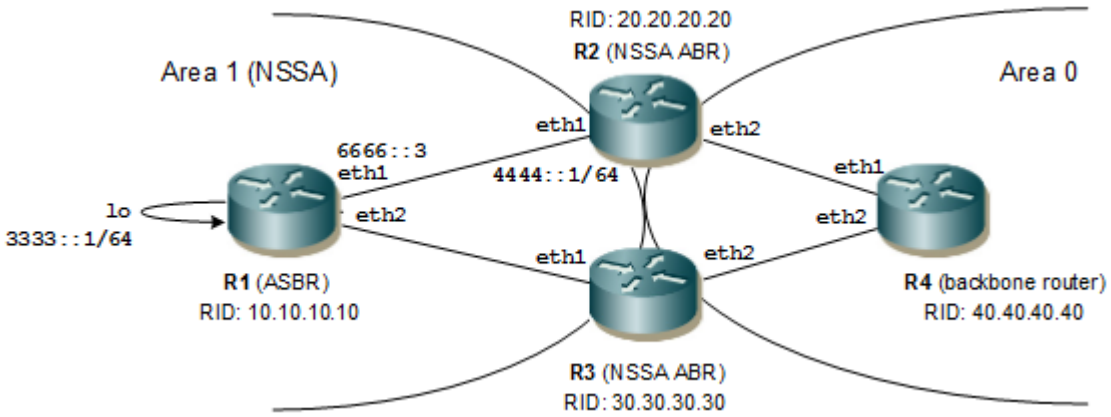


Figure 5-110: Using the translator-role Option

© 2021 IP Infusion Inc. Proprietary

Configuration

When one NSSA-ABR is configured with the translator role as `always` and the other as `candidate`, then translation is done by the router configured as `always`. In this scenario, the translation can be biased by setting the translator role to `always` on the router that has the lower router identifier.

R1

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config-if)#interface lo`	Enter interface mode for Loopback
`(config-if)#ipv6 address 3333::1/64`	Assign IPv6 address to loopback interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 10.10.10.10`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa`	Configure the area as NSSA.
`(config-router)#redistribute static`	Redistribute the static route configured into the OSPF NSSA
`(config-router)#redistribute connected`	Redistribute the connected network into OSPF NSSA
`(config-router)#exit`	Exit interface mode
`(config)#ipv6 route 4444::1:0:0:0:0/64 6666::3`	Configure the static route with the nexthop address as R2's `eth1` IPv6 address
`(config)#exit`	Exit interface mode.

R2

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone area (0)
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 20.20.20.20`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa translator-role candidate`	Configure the NSSA-ABR with the translator role candidate.
`(config-router)#exit`	Exit interface mode

© 2021 IP Infusion Inc. Proprietary

R3

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone area (0)
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 30.30.30.30`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa translator-role candidate`	Configure the NSSA-ABR with the translator role candidate.
`(config-router)#exit`	Exit interface mode

R4

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone area (0)
`(config)#interface eth2`	Enter interface mode for `eth2`
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone area (0)
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 40.40.40.40`	Configure the router ID to use on this instance (100)
`(config-router)#exit`	Exit interface mode

The command to configure the NSSA-Translator role as `always` is:

```
(config-router)#area 1 nssa translator-role always
```

The NSSA-ABR can continue to perform translation after its services are no longer required for the stability interval which is set using the command below on the NSSA-ABR.

```
(config-router)#area 1 nssa stability-interval 7777
```

Validation 1

The translation is done by the NSSA-ABR with the higher router identifier. In the output below, check the router identifier of the NSSA-ABR. Also, check the router which is elected and the router which is disabled.

```
R2#sh ipv6 ospf
 Routing Process "OSPFv3 (100)" with ID 20.20.20.20
 Process uptime is 21 minutes
 SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 4. Checksum Sum 0x1F816
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 28
 Number of LSA received 58
 Number of areas in this router is 2
```


© 2021 IP Infusion Inc. Proprietary

```
    Area BACKBONE(0)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 7 times
        Number of LSA 19.  Checksum Sum 0x7454D
        Number of Unknown LSA 0
    Area 0.0.0.1 (NSSA)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 14 times
        Number of LSA 19.  Checksum Sum 0xA4D18
        Number of Unknown LSA 0
        NSSA Translator State is disabled
R3#sh ipv6 ospf
 Routing Process "OSPFv3 (100)" with ID 30.30.30.30
 Process uptime is 19 minutes
 SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 4. Checksum Sum 0x1F816
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 31
 Number of LSA received 69
 Number of areas in this router is 2
    Area BACKBONE(0)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 15 times
        Number of LSA 19.  Checksum Sum 0x7454D
        Number of Unknown LSA 0
    Area 0.0.0.1 (NSSA)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 10 times
        Number of LSA 19.  Checksum Sum 0xA4D18
        Number of Unknown LSA 0
        NSSA Translator State is elected
```

Validation 2

The translated Type-5 LSA in R4 in area 0 has the advertising router identifier of R3. In the output below, the LS Type is AS-External-LSA and the advertising router has the higher router identifier.

```
R4#sh ipv6 ospf database external

            OSPFv3 Router with ID (40.40.40.40) (Process 100)

                AS-external-LSA

  LS age: 885
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.7
  Advertising Router: 30.30.30.30
  LS Seq Number: 0x80000001
  Checksum: 0xD3FE
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 3333::/64
```

```
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 0


LS age: 18
LS Type: AS-External-LSA
Link State ID: 0.0.0.8
Advertising Router: 30.30.30.30
LS Seq Number: 0x80000003
Checksum: 0x7457
Length: 56
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 4444::/64
  Prefix Options: 0 (-|-|-|-)
  Forwarding Address: 6666::3
  External Route Tag: 0
```

Link LSA Suppression

If link LSA suppression is enabled and the interface type is not broadcast or NBMA, the router will not originate a link-LSA for the link. This implies that other routers on that link will determine the router's next hop address using a mechanism other than the link LSA.

Topology

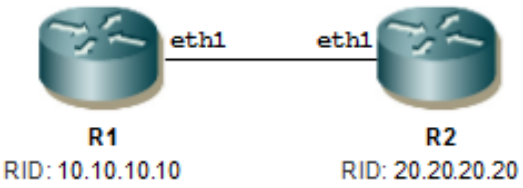


Figure 5-111: LSA Suppression

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100-ABC`) which uniquely identifies the routing process.
`(config-router)#router-id 10.10.10.10`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 router ospf tag 100-ABC area 1`	Configure interface in an area assigned with the area ID (1). The tag uniquely identifies the routing process.
`(config-if)#ipv6 ospf network point-to-point`	Configure the OSPF interface network type as point to point

© 2021 IP Infusion Inc. Proprietary

(config-if)#ipv6 ospf link-lsa-suppression enable	Enable the link LSA suppression mechanism
(config-if)#exit	Exit interface mode

R2

#configure terminal	Enter configure mode.
(config)#router ipv6 ospf 100-ABC	Configure the routing process and specify the tag (100-ABC) which uniquely identifies the routing process.
(config-router)#router-id 20.20.20.20	Configure the router ID to use on this instance.
(config-router)#exit	Exit OSPF router mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 router ospf tag 100-ABC area 1	Configure interface in an area assigned with the area ID (1). The tag uniquely identifies the routing process.
(config-if)#ipv6 ospf network point-to-point	Configure the OSPF interface network type as point to point
(config-if)#ipv6 ospf link-lsa-suppression enable	Enable the link LSA Suppression Mechanism
(config-if)#exit	Exit interface mode

Note: This is not applicable for broadcast and NBMA networks.

Validation 1

Verify that adjacency has been established.

```
R1#sh ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
20.20.20.20       1   Full/ -         00:00:37    eth2       0
```

Validation 2

Verify that DUT should not have the Link LSA in the Link state database.

Note: The output below is captured after link lsa suppression enabled which has not Link LSA in the LSDB.

```
DUT#sh ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.10) (Process 100)

                Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age  Seq#       CkSum    Link
0.0.0.0         10.10.10.10       15 0x80000004 0x3264      1
0.0.0.0         20.20.20.20       15 0x80000002 0xdbba      1

                Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age  Seq#       CkSum  Prefix  Reference
0.0.0.12        10.10.10.10       14 0x80000004 0xaab4      1  Router-LSA
0.0.0.13        20.20.20.20       15 0x80000002 0x8f7f      1  Router-LSA

                Intra-Area-Te-LSA (Area 0.0.0.1)
```

```
Link State ID   ADV Router      Age  Seq#       CkSum
0.0.0.4         10.10.10.10       15 0x80000004 0xa326
0.0.0.3         20.20.20.20       15 0x80000002 0xffec
R1#sh ipv6 ospf database link

            OSPFv3 Router with ID (10.10.10.10) (Process 100)
```

Originate Type-7 LSAs and Translate to Type-5

Figure 5-112 shows the configuration to originate Type-7 LSAs and translate them into Type-5 LSAs. R3 is an NSSA-ASBR that originates Type-7 LSAs into the NSSA which are converted to Type-5 LSAs by R2 which is an NSSA-ABR. R1 is a backbone router.

Topology

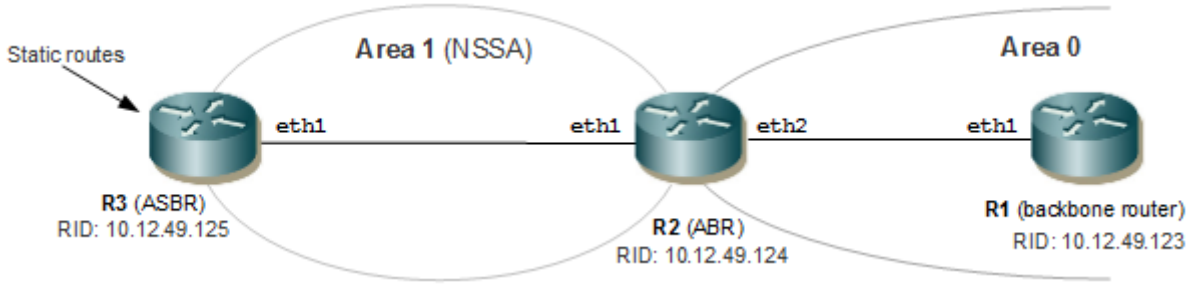


Figure 5-112: Originate Type-7 LSAs and Translate to Type-5 under Address Family IPv4

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100-ABC`) which uniquely identifies the routing process
`(config-router)#router-id 10.12.49.123`	Configure the router ID to use on this tag
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 31`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process and the instance identifier which is 0-31 for the IPv6 address family
`(config-if)#exit`	Exit interface mode

R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100-ABC`) which uniquely identifies the routing process.

© 2021 IP Infusion Inc. Proprietary

(config-router)#ip route 15.15.15.0/24 null	Configure the static route with the nexthop address set to null
(config-router)#router-id 10.12.49.125	Configure the router ID to use for this process
(config-router)#area 1 nssa	Configure the area 1 as NSSA.
(config-router)#exit	Exit OSPF router mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 31	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 0-31 for the IPv6 address family.
(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 30	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 0-31 for the IPv6 address family.
(config)#interface eth2	Enter interface mode
(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 30	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 0-31 for the IPv6 address family.
(config-if)#exit	Exit interface mode

R3

#configure terminal	Enter configure mode.
(config)#router ipv6 ospf 100-ABC	Configure the routing process and specify the tag (100-ABC) which uniquely identifies the routing process.
(config-router)#router-id 10.12.49.125	Configure the router ID to use for this process
(config-router)#area 1 nssa	Configure the area 1 as NSSA.
(config-router)#exit	Exit OSPF router mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 30	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 0-31 for the IPv4 address family.

Validation 1

Verify that adjacency has been established with the configured instance identifier.

```
DUT#sh ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface   Instance ID
10.12.49.123      1   Full/DR         00:00:31       eth1           31
10.12.49.124      1   Full/Backup     00:00:38       eth2           30
```

Validation 2

Verify that the ABR has External LSA Type 5 in its Database.

Note: Check that R3 has generated a Type 7 LSA.

```
R3#sh ipv6 ospf database external
```

```
            OSPFv3 Router with ID (10.12.49.129) (Process 1)

                AS-external-LSA

LS age: 1517
LS Type: AS-External-LSA
Link State ID: 0.0.0.1
Advertising Router: 10.12.49.124
LS Seq Number: 0x80000003
Checksum: 0x597D
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 10.12.49.0/24
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0


LS age: 991
LS Type: AS-External-LSA
Link State ID: 0.0.0.11
Advertising Router: 10.12.49.124
LS Seq Number: 0x80000001
Checksum: 0x4C60
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 21
  Prefix: 33.33.33.0/29
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0


LS age: 442
LS Type: AS-External-LSA
Link State ID: 0.0.0.13
Advertising Router: 10.12.49.129
LS Seq Number: 0x80000001
Checksum: 0x376B
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 33.33.33.1/32
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0


LS age: 442
LS Type: AS-External-LSA
Link State ID: 0.0.0.14
Advertising Router: 10.12.49.129
LS Seq Number: 0x80000001
Checksum: 0x3B65
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 33.33.33.2/32
  Prefix Options: 0 (-|-|-|-)
```

 © 2021 IP Infusion Inc. Proprietary

```
    External Route Tag: 0


  LS age: 442
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.15
  Advertising Router: 10.12.49.129
  LS Seq Number: 0x80000001
  Checksum: 0x3F5F
  Length: 36
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 33.33.33.3/32
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 0


  LS age: 442
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.16
  Advertising Router: 10.12.49.129
  LS Seq Number: 0x80000001
  Checksum: 0x4359
  Length: 36
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 33.33.33.4/32
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 0
```

Validation 3

Verify that FIB of backbone router has External Route as “O E2”.

```
R3#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

Gateway of last resort is 10.12.49.1 to network 0.0.0.0

K*      0.0.0.0/0 via 10.12.49.1, eth0
C       10.12.49.0/24 is directly connected, eth0
C       11.11.11.0/24 is directly connected, eth1
C       11.13.11.0/24 is directly connected, eth3
C       11.14.11.0/24 is directly connected, eth4
C       11.15.11.0/24 is directly connected, eth5
C       12.12.12.0/24 is directly connected, eth1
O IA    30.30.30.0/24 [110/2] via 12.12.12.12, eth1
O E2    33.33.33.0/29 [110/21] via 12.12.12.12, eth1
O E2    33.33.33.1/32 [110/20] via 12.12.12.12, eth1
O E2    33.33.33.2/32 [110/20] via 12.12.12.12, eth1
O E2    33.33.33.3/32 [110/20] via 12.12.12.12, eth1
```

```
O E2     33.33.33.4/32 [110/20] via 12.12.12.12, eth1
C        127.0.0.0/8 is directly connected, lo
K        169.254.0.0/16 is directly connected, eth0
```

Summarize Intra-Area and External Routes

Figure 5-113 shows the configuration to enable intra-area and external route summarization. The IPv4 address family is enabled on R1. R2 summarizes the internal OSPF routhes which R3 redistributes.

Topology

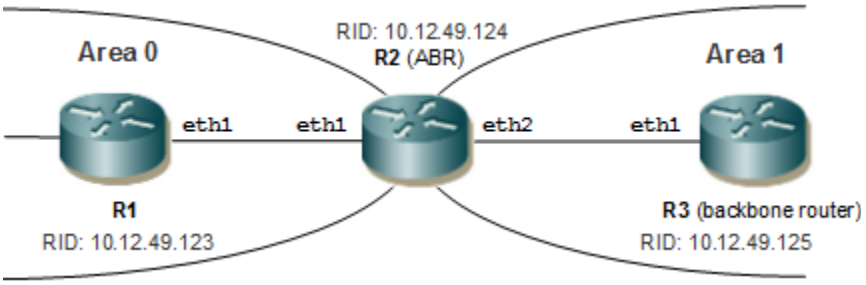


Figure 5-113: Enabling Intra-Area and External Route Summarization

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100-ABC`) which uniquely identifies the routing process
`(config-router)#router-id 10.12.49.123`	Configure the router ID to use for this process.
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 10.10.10.1/24`	Specify IP address for interface eth1
`(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 31`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process and the instance identifier which is 0-31 for the IPv6 address family.

© 2021 IP Infusion Inc. Proprietary

R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (100-ABC) which uniquely identifies the routing process
`(config-router)#router-id 10.12.49.124`	Configure the router ID to use for this process
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 10.10.10.2/24`	Specify an IP address for the interface
`(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 31`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process and the instance identifier which is 0-31 for the IPv6 address family.
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 20.20.20.1/24`	Specify an IP address for the interface
`(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 30`	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 0-31 for the IPv6 address family.
`(config-if)#exit`	Exit interface mode
`(config)#interface lo`	Enter interface mode
`(config-if)#ipv6 router ospf area 1 tag 101 instance-id 30`	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 0-31 for the IPv6 address family.
`(config-if)#exit`	Exit interface mode

R3

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (100-ABC) which uniquely identifies the routing process
`(config-router)#router-id 10.12.49.125`	Configure the router ID to use for this process
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 20.20.20.2/24`	Specify an IP address for the interface
`(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 30`	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 0-31 for the IPv6 address family.
`(config-if)#exit`	Exit interface mode

Inter Area Route Aggregation Validation

Validation 1: Verify that adjacency has been established with the configured instance identifier.

```
DUT#show ipv6 ospf neighbor
OSPFv3 Process (100-ABC)
Neighbor ID     Pri   State              Dead Time   Interface  Instance ID
10.12.49.123      1   Full/Backup     00:00:38       eth1       31
```

```
10.12.49.125      1   Full/DR           00:00:38       eth2       30
```

Validation 2: Verify that a single aggregated OSPF IA route is available in FIB of R1.

```
R1#show ipv6 ospf n
OSPFv3 Process (100-ABC)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.12.49.124      1   Full/DR         00:00:32    eth1       31
```

Validation 3: Verify that the Inter-Area-Prefix-LSA has one prefix in the R1 Link State Database.

```
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     10.10.10.0/24 is directly connected, eth1, 00:06:54
C     10.12.49.123/32 is directly connected, lo, 00:06:54
O E2  10.12.49.125/32 [110/20] via 10.10.10.2, eth1, 00:05:58
O IA  20.20.20.0/24 [110/20] via 10.10.10.2, eth1, 00:06:04
C     127.0.0.0/8 is directly connected, lo, 00:06:58
C     192.168.20.0/24 is directly connected, eth0, 00:06:54

Gateway of last resort is not set


R1#show ipv6 ospf database

            OSPFv3 Router with ID (10.12.49.123) (Process 100-ABC)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.3         10.12.49.123     787       0x80000001 0x1ed1      1
0.0.0.3         10.12.49.124     784       0x80000001 0x44a8      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.12.49.123     742       0x80000003 0x5610      1
0.0.0.0         10.12.49.124     739       0x80000003 0x5311      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.12.49.124     744       0x80000001 0x5763

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
```


© 2021 IP Infusion Inc. Proprietary

```
0.0.0.1         10.12.49.124     779       0x80000002 0x5db9

                Inter-Area-Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.1         10.12.49.124     733       0x80000001 0x91e0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.12.49.124     738       0x80000001 0x0df7      2  Network-
LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.12.49.123     738       0x80000003 0x8460
0.0.0.3         10.12.49.124     743       0x80000002 0xb231#show ipv6 ospf n
OSPFv3 Process (100-ABC)
Neighbor ID     Pri   State              Dead Time   Interface  Instance ID
10.12.49.123      1   Full/Backup        00:00:38       eth1       31
10.12.49.125      1   Full/DR            00:00:38       eth2       30
```

External Route Summarization Validation

Note: External route summarization is done at the ASBR.

Validation 1: Verify that single summarized external route in the ABR.

```
R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     10.10.10.0/24 is directly connected, eth1, 00:06:40
C     10.12.49.124/32 is directly connected, lo, 00:06:40
O E2  10.12.49.125/32 [110/20] via 20.20.20.2, eth2, 00:05:48
C     20.20.20.0/24 is directly connected, eth2, 00:06:40
C     127.0.0.0/8 is directly connected, lo, 00:06:45
C     192.168.20.0/24 is directly connected, eth0, 00:06:40

Gateway of last resort is not set
```

Validation 2: Verify that a single Type 5 LSA is in the ABR's Link State Data Base.

```
R2#show ipv6 ospf database

            OSPFv3 Router with ID (10.12.49.124) (Process 100-ABC)

                Link-LSA (Interface eth1)
```

```
Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.3         10.12.49.123     443       0x80000001 0x1ed1      1
0.0.0.3         10.12.49.124     438       0x80000001 0x44a8      1

                Link-LSA (Interface eth2)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.4         10.12.49.124     438       0x80000001 0xc2ee      1
0.0.0.4         10.12.49.125     434       0x80000001 0xe8c5      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.12.49.123     398       0x80000003 0x5610      1
0.0.0.0         10.12.49.124     393       0x80000003 0x5311      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.12.49.124     398       0x80000001 0x5763

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.1         10.12.49.124     433       0x80000002 0x5db9

                Inter-Area-Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.1         10.12.49.124     387       0x80000001 0x91e0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix  Reference
0.0.0.2         10.12.49.124     392       0x80000001 0x0df7      2  Network-
LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.12.49.123     393       0x80000003 0x8460
0.0.0.3         10.12.49.124     398       0x80000002 0xb231

                Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router      Age       Seq#       CkSum    Link
0.0.0.0         10.12.49.124     393       0x80000004 0x87d8      1
0.0.0.0         10.12.49.125     389       0x80000004 0x2a3d      1


                AS-external-LSA

Link State ID   ADV Router      Age       Seq#       CkSum   Route  Tag
0.0.0.1         10.12.49.125     779       0x80000001 0x64f1 E2      0
0.0.0.2         10.12.49.125     779       0x80000001 0xfba8 E2      0
```


© 2021 IP Infusion Inc. Proprietary

Distribute List

To filter the routes that Open Shortest Path First Version 3 (OSPFv3) installs in the Routing Information Base (RIB), use the `distribute-list in` command in an appropriate configuration mode.

To filter the routes redistributed into Open Shortest Path First Version 3 (OSPFv3) from other routing protocols, use the `distribute-list out` command in an appropriate configuration mode.

Topology

Figure 5-114 shows the configuration to illustrate the distribute-list support for OSPFv3

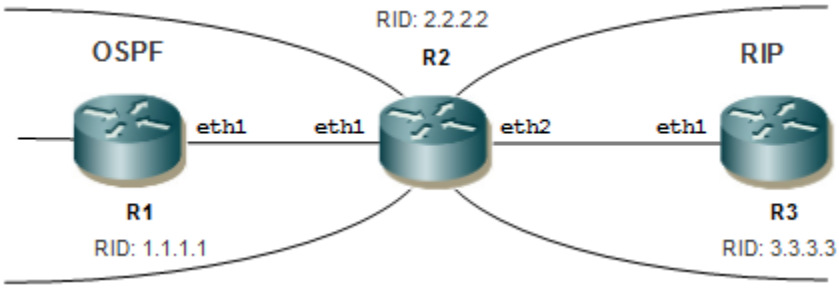


Figure 5-114: Basic Topology for Distribute-list

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2000::1/64`	Configure the IPv6 address of the interface.
`(config-if)#ipv6 router ospf area 0 tag proc1`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf proc1`	Configure the routing process
`(config-router)#router-id 1.1.1.1`	Configure router-id to uniquely identify the router
`(config-router)#end`	Exit router mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2000::50/64`	Configure the IPv6 address of the interface
`(config-if)#ipv6 router ospf area 0 tag proc1`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process

`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ipv6 address 4000::50/64`	Configure the IPv6 address of the interface.
`(config-if)#ipv6 router ospf area 0 tag proc1`	Configure the interface in an area assigned with the area ID
`(config-if)#ipv6 router rip`	Configure rip instance under interface
`(config-if)#exit`	Exit interface mode
`(config)#router ipv6 rip`	Configure the rip routing process
`(config-router)#neighbor fe80::5054:ff:fe85:19bc eth1`	Configure RIP neighbor peer
`(config-router)#exit`	Exit router mode.
`(config)#ipv6 access-list 1 permit 7777::/64`	Configure access list to permit 7777::/64 and deny 8888::/64
`(config)#router ipv6 ospf proc1`	Configure the routing process
`(config-router)#router-id 2.2.2.2`	Configure router-id to uniquely identify the router
`(config-router)#redistribute rip`	Redistribute rip routes
`(config-router)#distribute-list 1 out rip`	Configure distribute list to allow the permitted routes
`(config-router)#exit`	Exit router mode
`(config)#ipv6 access-list 1`	Enter access-list mode
`(config-ipv6-acl)#permit ipv6 8888::1/64 any`	Configure access-list
`(config-ipv6-acl)#exit`	Exit access-list mode
`(config)#exit`	Exit configure mode

R3

`#configure terminal`	Enter configure mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 address 4000::51/64`	Configure the IPv6 address of the interface.
`(config-if)#ipv6 router rip`	Configure rip instance under interface
`(config-if)#exit`	Exit interface mode
`(config)#router ipv6 rip`	Configure the rip routing process
`(config-router)#neighbor fe80::5054:ff:fec6:69f eth2`	Configure rip neighbor peer
`(config-router)#exit`	Exit router mode
`(config)#ipv6 route 7777::/64 eth2`	Configure static route
`(config)#ipv6 route 8888::/64 eth3`	Configure static route
`(config)#router ipv6 rip`	Configure the rip routing process

© 2021 IP Infusion Inc. Proprietary

(config-router)#redistribute static	Redistribute configured static routes
(config-router)#end	Exit router mode

Validation 1

Verify OSPF neighborship is up between R1and R2

R2

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (Proc1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:00:38    eth1       0
```

Validation 2

Check if permitted route 7777::/64 is present in route table and denied route 8888::/64 is not present.

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (Proc1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
   Destination     Metric           Next-hop
C  2000::/64         1             directly connected, eth1, Area 0.0.0.0
E2 7777::/64        1/20   via    fe80::5054:ff:fe1e:269d, eth1
```

Validation 3

Check both the routes 7777::/64 and 8888::/64 are present after 8888::/64 is permitted

R1

```
rtr1#show ipv6 ospf route
OSPFv3 Process (Proc1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination    Metric    Next-hop
C  2000::/64         1      directly connected, eth1, Area 0.0.0.0
E2 7777::/64        1/20   via fe80::5054:ff:fe1e:269d, eth1
E2 8888::/64        1/20   via fe80::5054:ff:fe1e:269d, eth1
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 6 IS-IS IPv4

This chapter contains basic IS-IS (Intermediate System to Intermediate System) configuration examples.

Enable IS-IS on an Interface

This example shows the minimum configuration required for enabling IS-IS on an interface. R1 and R2 are two routers in the `ABC` instance connecting to the network 10.10.10.0/24. After enabling IS-IS on an interface, create a routing instance, and specify the Network Entity Title (NET). IS-IS explicitly specifies a NET to begin routing. NET is comprised of the area address and the system ID of the router.

Topology

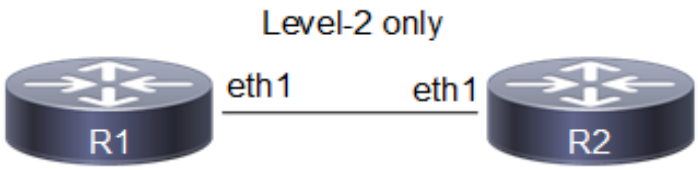


Figure 6-115: Basic IS-IS Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config)#ip address 21.21.21.2/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC)`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (`ABC`).
`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#net 49.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config)#ip address 21.21.21.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC)`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area `49 (ABC)`.

`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#net 49.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     24        L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     6         L2   IS-IS

R1#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0002 eth1        Up     L2   64        0000.0000.0001.01

R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0001 eth1        Up     L2   64        0000.0000.0001.01

R1#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.00dc.0b76
    IP interface address:
      21.21.21.2/24
    IPv6 interface address:
      fe80::5054:ff:fedc:b76/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 0 milliseconds

R2#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
```


© 2021 IP Infusion Inc. Proprietary

```
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.002a.230a
    IP interface address:
      21.21.21.1/24
    IPv6 interface address:
      fe80::5054:ff:fe2a:230a/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 1 seconds

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    21.21.21.0/24       10          --                  eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    21.21.21.0/24       10          --                  eth1            0

R1#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       eth1
5254.002a.230a

R2#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       10         0000.0000.0001       eth1
5254.00dc.0b76
0000.0000.0002       --

R1#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000009   0x6C2D        980               0/0/0
```

```
0000.0000.0001.01-00* 0x00000003   0x1DBB        980               0/0/0
0000.0000.0002.00-00  0x0000000A   0x5444        980               0/0/0


R2#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000009   0x6C2D        942               0/0/0
0000.0000.0001.01-00  0x00000003   0x1DBB        942               0/0/0
0000.0000.0002.00-00* 0x0000000A   0x5444        944               0/0/0
```

Set Priority

This example describes how to set the priority for an interface. Set a high priority for a router to make it the Designated IS (DIS). Router R2 is configured to have a priority of 125, this is higher than the default priority (64) of R1. This makes R2 the DIS..

Topology

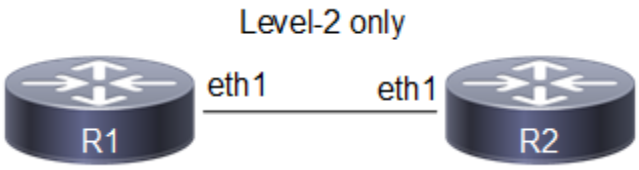


Figure 6-116: Set IS-IS Priority

Configuration

R1

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC)`.
`(config)#ip address 21.21.21.2/24`	Configure IP address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area `49` (`ABC`).
`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#net 49.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`(config)#interface eth1`	Enter interface mode.
`(config)#ip address 21.21.21.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC)`.

© 2021 IP Infusion Inc. Proprietary

`(config-if)#isis priority 125`	Specify the router priority to a higher priority (125) to make R2 the designated IS (DIS).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area `49` (`ABC`).
`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#net 49.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#show clns neighbors
Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     6         L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     21        L2   IS-IS

R1#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0002 eth1        Up     L2   125       0000.0000.0002.01

R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0001 eth1        Up     L2   64        0000.0000.0002.01

R1#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.00dc.0b76
    IP interface address:
      21.21.21.2/24
    IPv6 interface address:
      fe80::5054:ff:fedc:b76/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0002.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
```

```
    Next IS-IS LAN Level-2 Hello in 1 seconds

R2#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.002a.230a
    IP interface address:
      21.21.21.1/24
    IPv6 interface address:
      fe80::5054:ff:fe2a:230a/64
    Level-2 Metric: 10/10, Priority: 125, Circuit ID: 0000.0000.0002.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 737 milliseconds
```

Dynamic hostname

This example shows how to configure Dynamic Hostname for an ISIS instance. Dynamic hostname is the method of mapping name-to-systemID. It allows the routing protocol to advertise symbolic names in the IS-IS PDUs. This is done by the addition of a new TLV which allows the IS-IS routers to include the name-to-systemID mapping data in their LSPs. This allows for simple and reliable transport of name mapping across IS-IS networks. Dynamic hostname can be either the hostname of the node or the tag of the configured ISIS instance.

Note: Dynamic-hostname has to be configured on all nodes for it to take effect.

Topology

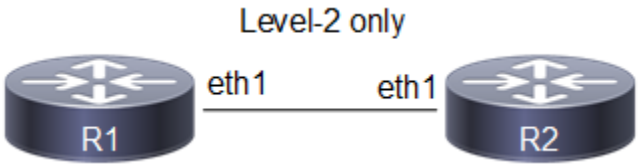


Figure 6-117: Basic dynamic hostname topology

© 2021 IP Infusion Inc. Proprietary

Configuration

R1

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config)#ip address 21.21.21.2/24`	Configure IP address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.

R2

`(config)#interface eth1`	Enter interface mode.
`(config)#ip address 21.21.21.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R2             eth1        5254.002a.230a  Up     28        L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1             eth1        5254.00dc.0b76  Up     7         L2   IS-IS

R1#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
```

```
R2             eth1        Up     L2   64        0000.0000.0001.01

R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
R1             eth1        Up     L2   64        0000.0000.0001.01

R1#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   --
R2                   10         R2       eth1        5254.002a.230a

R2#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   10         R1       eth1        5254.00dc.0b76
R2                   --

R1#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x0000000B   0x1D6B        1170              0/0/0
R1.01-00            * 0x00000004   0x1BBC        538               0/0/0
R2.00-00              0x0000000C   0x0D79        1166              0/0/0

R2#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x0000000B   0x1D6B        1078              0/0/0
R1.01-00              0x00000004   0x1BBC        445               0/0/0
R2.00-00            * 0x0000000C   0x0D79        1075              0/0/0
```

Redistribute Routes into IS-IS

In this example, the configuration causes OSPF routes to be imported into the IS-IS routing table, and advertised into the `ABC` instance.

© 2021 IP Infusion Inc. Proprietary

Topology

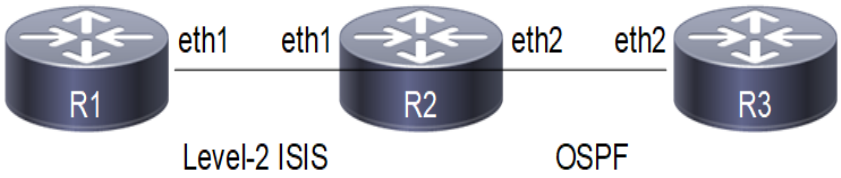


Figure 6-118: Redistribute Routes Into IS-IS

Configuration

R1

(config)#interface eth1	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config)#ip address 21.21.21.2/24	Configure IP address on interface.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0001.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#dynamic-hostname	Configure the hostname to be advertised for an ISIS instance.

R2

(config)#interface eth1	Enter interface mode.
(config)#ip address 21.21.21.1/24	Configure IP address on interface.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config)#ip address 31.31.31.1/24	Configure IP address on interface.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#redistribute ospf	Specify redistributing routes from other routing protocol (OSPF) into IS-IS.
(config-router)#dynamic-hostname	Configure the hostname to be advertised for an ISIS instance.
(config-router)#exit	Exit interface mode.
(config)#interface lo	Configure interface lo
(config-if)#ip address 2.2.2.2/32 secondary	Configure secondary IP address to loopback interface
(config-if)#exit	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

`(config)#router ospf 100`	Configure OSPF routing process and specify the tag (100) which uniquely identifies the routing process
`(config-router)#ospf router-id 2.2.2.2`	Specify a Router ID (2.2.2.2) for the OSPF routing process.
`(config-router)#network 2.2.2.2/32 area 0.0.0.0`	Advertising 2.2.2.2 network
`(config-router)#network 31.31.31.0/24 area 0.0.0.0`	Advertising 31 network
`(config-router)#exit`	Exit router mode.

R3

`(config)#interface eth2`	Enter interface mode.
`(config)#ip address 31.31.31.2/24`	Configure IP address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Configure interface lo
`(config-if)#ip address 3.3.3.3/32 secondary`	Configure secondary IP address to loopback interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure OSPF routing process and specify the tag (100) which uniquely identifies the routing process
`(config-router)#ospf router-id 3.3.3.3`	Specify a Router ID (3.3.3.3) for the OSPF routing process.
`(config-router)#network 3.3.3.3/32 area 0.0.0.0`	Advertising 3.3.3.3 network
`(config-router)#network 31.31.31.0/24 area 0.0.0.0`	Advertising 31 network

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R2             eth1        5254.002a.230a      Up     25        L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1             eth1        5254.00dc.0b76      Up     6         L2   IS-IS

R1#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
R2             eth1        Up     L2   64        0000.0000.0001.01
```


© 2021 IP Infusion Inc. Proprietary

```
R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
R1             eth1        Up     L2   64        0000.0000.0001.01

R1#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   --
R2                   10         R2       eth1        5254.002a.230a

R2#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   10         R1       eth1        5254.00dc.0b76
R2                   --

R1#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x00000003   0x2D63        1096              0/0/0
R1.01-00            * 0x00000002   0x1FBA        1096              0/0/0
R2.00-00              0x00000004   0xEF02        1108              0/0/0

R2#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x00000003   0x2D63        1021              0/0/0
R1.01-00              0x00000002   0x1FBA        1021              0/0/0
R2.00-00            * 0x00000004   0xEF02        1035              0/0/0


R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L2   2.2.2.2/32          10          21.21.21.1          eth1            0
L2   3.3.3.3/32          10          21.21.21.1          eth1            0
C    21.21.21.0/24       10          --                  eth1            0
L2   31.31.31.0/24       10          21.21.21.1          eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid
```

© 2021 IP Infusion Inc. Proprietary

```
Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
E    2.2.2.2/32          0           --                  --             0
E    3.3.3.3/32          0           --                  --             0
C    21.21.21.0/24       10          --                  eth1            0
E    31.31.31.0/24       0           --                  --             0

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
i L2         2.2.2.2/32 [115/10] via 21.21.21.1, eth1, 00:16:54
i L2         3.3.3.3/32 [115/10] via 21.21.21.1, eth1, 00:16:43
C            10.12.30.0/24 is directly connected, eth0, 00:24:28
C            21.21.21.0/24 is directly connected, eth1, 00:18:37
i L2         31.31.31.0/24 [115/10] via 21.21.21.1, eth1, 00:16:54
C            127.0.0.0/8 is directly connected, lo, 00:24:28

Gateway of last resort is not set

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            2.2.2.2/32 is directly connected, lo, 00:21:31
O            3.3.3.3/32 [110/2] via 31.31.31.2, eth2, 00:20:14
C            10.12.30.0/24 is directly connected, eth0, 00:27:36
C            21.21.21.0/24 is directly connected, eth1, 00:21:31
C            31.31.31.0/24 is directly connected, eth2, 00:21:31
C            127.0.0.0/8 is directly connected, lo, 00:27:36

Gateway of last resort is not set

R2#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address         Interface
Instance ID
3.3.3.3          1   Full/Backup    00:00:35   31.31.31.2      eth2
0
```


© 2021 IP Infusion Inc. Proprietary

```
R3#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
2.2.2.2           1   Full/DR         00:00:32    31.31.31.1      eth2
0

R2#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       OSPF LFA attributes:
       P - Primary, SP - Secondary-Path, LP - Link Protecting,
       NP - Node Protecting, BID - Broadcast Link Protecting

C  2.2.2.2/32 [1] is directly connected, lo, Area 0.0.0.0
O  3.3.3.3/32 [2] via 31.31.31.2, eth2, Area 0.0.0.0
C  31.31.31.0/24 [1] is directly connected, eth2, Area 0.0.0.0

R3#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       OSPF LFA attributes:
       P - Primary, SP - Secondary-Path, LP - Link Protecting,
       NP - Node Protecting, BID - Broadcast Link Protecting

O  2.2.2.2/32 [2] via 31.31.31.1, eth2, Area 0.0.0.0
C  3.3.3.3/32 [1] is directly connected, lo, Area 0.0.0.0
C  31.31.31.0/24 [1] is directly connected, eth2, Area 0.0.0.0

R3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
O            2.2.2.2/32 [110/2] via 31.31.31.1, eth2, 00:19:47
C            3.3.3.3/32 is directly connected, lo, 00:20:40
C            10.12.30.0/24 is directly connected, eth0, 00:26:28
C            31.31.31.0/24 is directly connected, eth2, 00:20:40
C            127.0.0.0/8 is directly connected, lo, 00:26:28

Gateway of last resort is not set
```

Metric

You can make a route the preferred route by changing its metric. In this example, the cost has been configured to make R3 the next hop for R1.

The default metric for each interface is 10. Interface eth3 on R2 has a metric of 20, and Interface eth2 on R3 has a metric of 30. The total cost to reach 10.10.14.0/24 (R4) through R2 and R3 is computed as follows:

R2: 10+20 = 30

R3: 10+30 = 40

In this topology, R1 chooses R2 as its next hop for destination 10.10.14.0/24.

Note: Below configuration is applicable for narrow (non-wide) metric-style. Wide metric can be configured by using the CLI's "metric-style wide" under isis instance and "isis wide-metric < 1-16777214>" under interface mode.

Topology

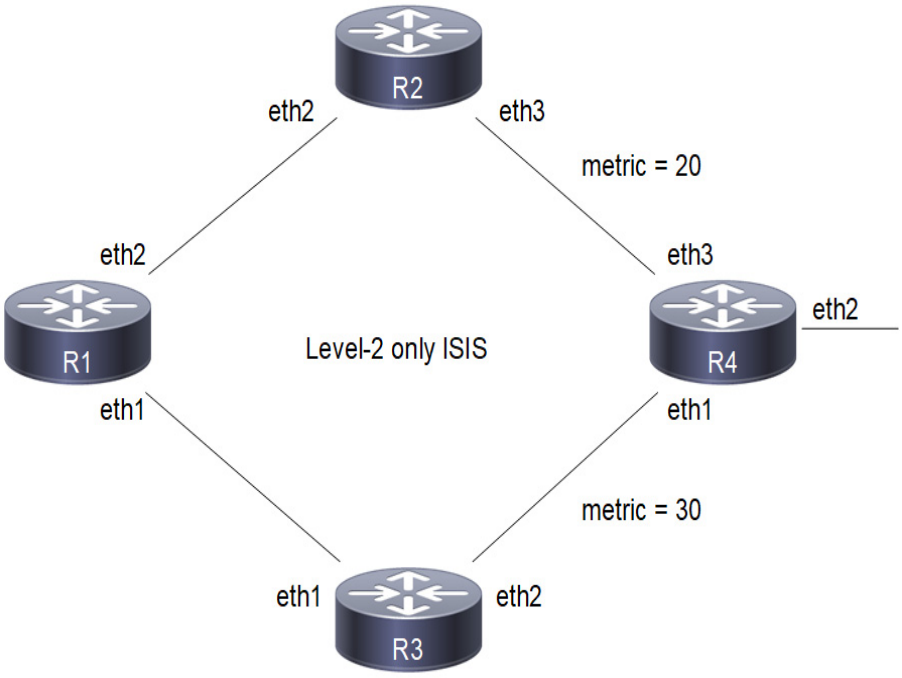


Figure 6-119: Configure IS-IS Metric

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

(config)#interface eth2	Enter interface mode.
(config-if)#ip address 30.30.30.1/24	Configure IP address on interface.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#dynamic-hostname	Configure the hostname to be advertised for an ISIS instance.
(config-router)#net 49.0000.0000.0001.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

(config)#interface eth2	Enter interface mode.
(config-if)#ip address 30.30.30.2/24	Configure IP address on interface.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ip address 40.40.40.1/24	Configure IP address on interface.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis metric 20	Set the value of IS-IS metric (on eth3) to 20.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#dynamic-hostname	Configure the hostname to be advertised for an ISIS instance.
(config-router)#net 49.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R3

(config)#interface eth1	Enter interface mode.
(config-if)#ip address 20.20.20.2/24	Configure IP address on interface.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#ip address 50.50.50.1/24	Configure IP address on interface.
(config-if)#isis metric 30	Set the value of IS-IS metric (on eth2) to 30.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).

`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`(config-router)#net 49.0000.0000.0003.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R4

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC).`
`(config-if)#ip address 50.50.50.2/24`	Configure IP address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth3`	Enter interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC).`
`(config-if)#ip address 40.40.40.2/24`	Configure IP address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area `49` (`ABC`).
`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`(config-router)#net 49.0000.0000.0004.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R3             eth1        5254.00dc.2f11  Up     5         L2   IS-IS
R2             eth2        5254.007e.5ade  Up     20        L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1             eth2        5254.00a1.6afe  Up     7         L2   IS-IS
R4             eth3        5254.00b1.d6fb  Up     8         L2   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
```


© 2021 IP Infusion Inc. Proprietary

```
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1             eth1        5254.00dc.0b76  Up     20        L2   IS-IS
R4             eth2        5254.00f5.35a4  Up     8         L2   IS-IS

R4#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R3             eth1        5254.00a8.940d  Up     25        L2   IS-IS
R2             eth3        5254.0049.c509  Up     25        L2   IS-IS

R1#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   --
R2                   10         R2       eth2        5254.007e.5ade
R3                   10         R3       eth1        5254.00dc.2f11
R4                   30         R2       eth2        5254.007e.5ade

R2#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   10         R1       eth2        5254.00a1.6afe
R2                   --
R3                   20         R1       eth2        5254.00a1.6afe
R4                   20         R4       eth3        5254.00b1.d6fb

R3#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   10         R1       eth1        5254.00dc.0b76
R2                   20         R1       eth1        5254.00dc.0b76
R3                   --
R4                   30         R4       eth2        5254.00f5.35a4

R4#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   20         R2       eth3        5254.0049.c509
                                R3       eth1        5254.00a8.940d
R2                   10         R2       eth3        5254.0049.c509
R3                   10         R3       eth1        5254.00a8.940d
R4                   --

R1#show ip isis route
```

```
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
C    30.30.30.0/24       10          --                  eth2            0
L2   40.40.40.0/24       30          30.30.30.2          eth2            0
L2   50.50.50.0/24       40          30.30.30.2          eth2            0
                                     20.20.20.2          eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L2   20.20.20.0/24       20          30.30.30.1          eth2            0
C    30.30.30.0/24       10          --                  eth2            0
C    40.40.40.0/24       20          --                  eth3            0
L2   50.50.50.0/24       30          40.40.40.2          eth3            0


R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
L2   30.30.30.0/24       20          20.20.20.1          eth1            0
L2   40.40.40.0/24       40          20.20.20.1          eth1            0
                                     50.50.50.2          eth2            0
C    50.50.50.0/24       30          --                  eth2            0

R4#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L2   20.20.20.0/24       20          50.50.50.1          eth1            0
L2   30.30.30.0/24       20          40.40.40.1          eth3            0
C    40.40.40.0/24       10          --                  eth3            0
C    50.50.50.0/24       10          --                  eth1            0

R1#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
```


© 2021 IP Infusion Inc. Proprietary

```
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.00dc.0b76
    IP interface address:
      20.20.20.1/24
    IPv6 interface address:
      fe80::5054:ff:fedc:b76/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0003.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 5 seconds
eth2 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x02
    Extended Local circuit ID: 0x00000004
    Local SNPA: 5254.00a1.6afe
    IP interface address:
      30.30.30.1/24
    IPv6 interface address:
      fe80::5054:ff:fea1:6afe/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.02
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 183 milliseconds

R2#show isis interface
eth2 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000004
    Local SNPA: 5254.007e.5ade
    IP interface address:
      30.30.30.2/24
    IPv6 interface address:
      fe80::5054:ff:fe7e:5ade/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.02
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 706 milliseconds
eth3 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x02
    Extended Local circuit ID: 0x00000005
    Local SNPA: 5254.0049.c509
    IP interface address:
      40.40.40.1/24
    IPv6 interface address:
      fe80::5054:ff:fe49:c509/64
    Level-2 Metric: 20/10, Priority: 64, Circuit ID: 0000.0000.0004.02
```

```
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 2 seconds

R3#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.00dc.2f11
    IP interface address:
      20.20.20.2/24
    IPv6 interface address:
      fe80::5054:ff:fedc:2f11/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0003.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 2 seconds
eth2 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x02
    Extended Local circuit ID: 0x00000004
    Local SNPA: 5254.00a8.940d
    IP interface address:
      50.50.50.1/24
    IPv6 interface address:
      fe80::5054:ff:fea8:940d/64
    Level-2 Metric: 30/10, Priority: 64, Circuit ID: 0000.0000.0004.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 3 seconds

R4#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000003
    Local SNPA: 5254.00f5.35a4
    IP interface address:
      50.50.50.2/24
    IPv6 interface address:
      fe80::5054:ff:fef5:35a4/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0004.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 0 milliseconds
eth3 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x02
```

 © 2021 IP Infusion Inc. Proprietary

```
Extended Local circuit ID: 0x00000005
Local SNPA: 5254.00b1.d6fb
IP interface address:
  40.40.40.2/24
IPv6 interface address:
  fe80::5054:ff:feb1:d6fb/64
Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0004.02
Number of active level-2 adjacencies: 1
Level-2 LSP MTU: 1492
Next IS-IS LAN Level-2 Hello in 0 milliseconds
```

L1-L2 Area Routing with a Single Instance

IS-IS supports a two-level hierarchy for handling and scaling the functionality of large networks. The Level-1 (L1) area is mainly for Leaf networks, and the Level-2 (L2) area is the backbone area connecting Level-1 areas. In this example, R3 and R4 are configured as Level-1 routers, and reside in the Level-1 area. R1 and R2 are configured as Level-1-2 routers, and connect these two Level-1 areas with a backbone Level-2 area. You can configure Level-1-2 routers with single or multiple instances: This configuration shows the single-instance version of the Level-1-2 router.

Topology

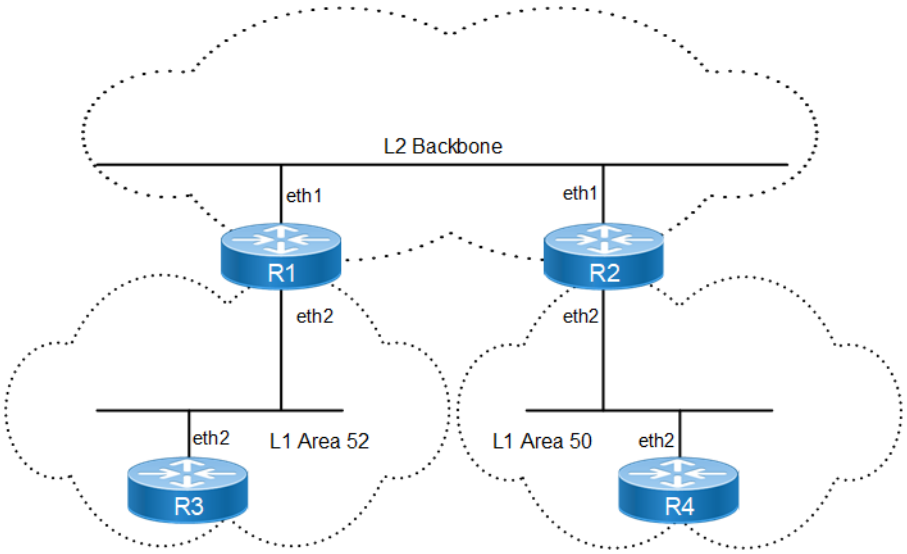


Figure 6-120: Single-Instance L1-L2 Area Routing

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on the interface `eth1` for area `ABC`.

`#configure terminal`	Enter configure mode.
`(config-if)#isis circuit-type level-2-only`	Set the circuit type for the interface `eth1`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 30.30.30.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on the interface `eth2` for area `ABC`.
`(config-if)#isis circuit-type level-1`	Set the circuit type for interface `eth2` to level 1.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area `ABC`.
`(config-router)#net 52.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip router isis bb`	Enable IS-IS routing on the interface `eth1` for area `bb`.
`(config-if)#ip address 20.20.20.2/24`	Configure IP address on interface.
`(config-if)#isis circuit-type level-2-only`	Set the circuit type for the interface `eth1` to level-2 only.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 40.40.40.1/24`	Configure IP address on interface.
`(config-if)#ip router isis bb`	Enable IS-IS routing on interface `eth2` for area `bb`.
`(config-if)#isis circuit-type level-1`	Set the circuit type for interface `eth2` to level 1.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis bb`	Create an IS-IS routing instance for area `bb`.
`(config-router)#net 50.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R3

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 30.30.30.2/24`	Configure IP address on interface.
`(config-if)#ip router isis xyz`	Enable IS-IS routing on the interface `eth2` for area `xyz`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis xyz`	Create an IS-IS routing instance for area `xyz`.
`(config-router)#is-type level-1`	Set the IS level for this area (`xyz`) as `level-1`.
`(config-router)#net 52.0000.0000.0003.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R4

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 40.40.40.2/24`	Configure IP address on interface.

© 2021 IP Infusion Inc. Proprietary

`(config-if)#ip router isis aa`	Enable IS-IS routing on the interface `eth2` for area `aa`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis aa`	Create an IS-IS routing instance for area `aa`.
`(config-router)#is-type level-1`	Set the IS level for this area (`aa`) as `level-1`.
`(config-router)#net 50.0000.0000.0004.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     20        L2   IS-IS
0000.0000.0003 eth2        5254.00a8.940d  Up     6         L1   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag bb:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     8         L2   IS-IS
0000.0000.0004 eth2        5254.00e2.aece  Up     7         L1   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag xyz:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth2        5254.00a1.6afe  Up     23        L1   IS-IS

R4#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag aa:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2        5254.007e.5ade  Up     25        L1   IS-IS

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid
```

```
Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
C    30.30.30.0/24       10          --                  eth2            0
L2   40.40.40.0/24       20          20.20.20.2          eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag bb:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
L2   30.30.30.0/24       20          20.20.20.1          eth1            0
C    40.40.40.0/24       10          --                  eth2            0

R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag xyz:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L1   0.0.0.0/0           10          30.30.30.1          eth2            0
C    30.30.30.0/24       10          --                  eth2            0

R4#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag aa:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L1   0.0.0.0/0           10          40.40.40.1          eth2            0
C    40.40.40.0/24       10          --                  eth2            0

R1#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop            Interface   SNPA
0000.0000.0001       --
0000.0000.0003       10         0000.0000.0003      eth2
5254.00a8.940d

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop            Interface   SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002      eth1
5254.002a.230a

R2#show isis topology
```


© 2021 IP Infusion Inc. Proprietary

```
Tag bb:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0002       --
0000.0000.0004       10         0000.0000.0004       eth2
5254.00e2.aece

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       10         0000.0000.0001       eth1
5254.00dc.0b76
0000.0000.0002       --

R3#show isis topology

Tag xyz:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       10         0000.0000.0001       eth2
5254.00a1.6afe
0000.0000.0003       --

R4#show isis topology

Tag aa:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0002       10         0000.0000.0002       eth2
5254.007e.5ade
0000.0000.0004       --

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.12.30.0/24 is directly connected, eth0, 00:27:08
C            20.20.20.0/24 is directly connected, eth1, 00:16:57
C            30.30.30.0/24 is directly connected, eth2, 00:15:48
i L2         40.40.40.0/24 [115/20] via 20.20.20.2, eth1, 00:15:05
C            127.0.0.0/8 is directly connected, lo, 00:27:08

Gateway of last resort is not set

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
```

```
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.12.30.0/24 is directly connected, eth0, 00:27:17
C            20.20.20.0/24 is directly connected, eth1, 00:17:13
i L2         30.30.30.0/24 [115/20] via 20.20.20.1, eth1, 00:16:18
C            40.40.40.0/24 is directly connected, eth2, 00:15:36
C            127.0.0.0/8 is directly connected, lo, 00:27:17

Gateway of last resort is not set

R3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 30.30.30.1 to network 0.0.0.0

i*L1         0.0.0.0/0 [115/10] via 30.30.30.1, eth2, 00:16:47
C            10.12.30.0/24 is directly connected, eth0, 00:27:46
C            30.30.30.0/24 is directly connected, eth2, 00:16:52
C            127.0.0.0/8 is directly connected, lo, 00:27:46

R4#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 40.40.40.1 to network 0.0.0.0

i*L1         0.0.0.0/0 [115/10] via 40.40.40.1, eth2, 00:16:26
C            10.12.30.0/24 is directly connected, eth0, 00:27:20
C            40.40.40.0/24 is directly connected, eth2, 00:16:36
C            127.0.0.0/8 is directly connected, lo, 00:27:20

R1#show isis database
Tag ABC:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000005   0xE66E        1165              1/0/0
0000.0000.0003.00-00  0x00000004   0xDC80        1164              0/0/0
0000.0000.0003.01-00  0x00000002   0x10C8        1163              0/0/0

IS-IS Level-2 Link State Database:
```


© 2021 IP Infusion Inc. Proprietary

```
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000005   0xD0D8        1148              0/0/0
0000.0000.0001.01-00* 0x00000002   0x1FBA        1109              0/0/0
0000.0000.0002.00-00  0x00000005   0x7219        1189              0/0/0

R2#show isis database
Tag bb:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x00000005   0x9583        1179              1/0/0
0000.0000.0004.00-00  0x00000004   0x8B95        1177              0/0/0
0000.0000.0004.01-00  0x00000002   0x2FA6        1177              0/0/0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000005   0xD0D8        1116              0/0/0
0000.0000.0001.01-00  0x00000002   0x1FBA        1078              0/0/0
0000.0000.0002.00-00* 0x00000005   0x7219        1160              0/0/0

R3#show isis database
Tag xyz:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000005   0xE66E        1094              1/0/0
0000.0000.0003.00-00* 0x00000004   0xDC80        1095              0/0/0
0000.0000.0003.01-00* 0x00000002   0x10C8        1094              0/0/0

R4#show isis database
Tag aa:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00  0x00000005   0x9583        1105              1/0/0
0000.0000.0004.00-00* 0x00000004   0x8B95        1105              0/0/0
0000.0000.0004.01-00* 0x00000002   0x2FA6        1105              0/0/0
```

L1-L2 Area Routing with Multiple Instances

IS-IS supports a two-level hierarchy for handling and scaling the functionality of large networks. The Level-1 (L1) area is mainly for Leaf networks, and the Level-2 (L2) area is the backbone area connecting Level-1 areas. In this example, R3 and R4 are configured as Level-1 routers, and reside in the Level-1 area. R1 and R2 are configured as Level-1-2 routers, and connect these two Level-1 areas with a backbone Level-2 area. You can configure Level-1-2 routers with single or multiple instances: This configuration shows the multiple-instance version of the Level-1-2 router.

Topology

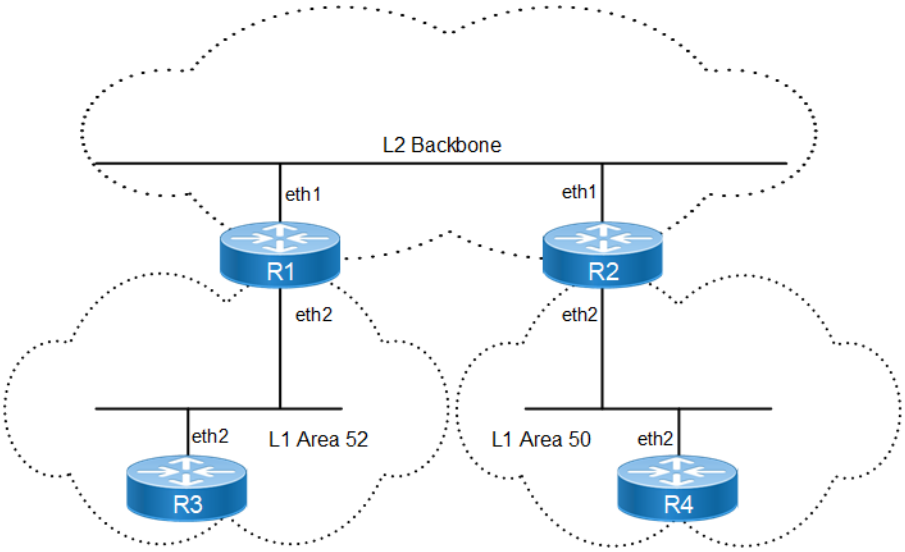


Figure 6-121: Multiple-Instance L1-L2 Area Routing

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure IP address on interface.
`(config-if)#ip router isis aaa`	Enable IS-IS routing on interface `eth1` for area `aaa`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis aaa`	Create an IS-IS routing instance for area `aaa`.
`(config-router)#is-type level-2-only`	Set the IS level for this area (`aaa`) as `level-2-only`.
`(config-router)#net bb.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 30.30.30.1/24`	Configure IP address on interface.
`(config-if)#ip router isis ccc`	Enable IS-IS routing on interface `eth2` for area `ccc`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ccc`	Create an IS-IS routing instance for area `ccc`.
`(config-router)#is-type level-1`	Set the IS level for this area (`ccc`) as `level-1`.
`(config-router)#net cc.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

© 2021 IP Infusion Inc. Proprietary

R2

(config)#interface eth1	Enter interface mode.
(config-if)#ip address 20.20.20.2/24	Configure IP address on interface.
(config-if)#ip router isis bb	Enable IS-IS routing on interface eth1 for area bb.
(config-if)#exit	Exit interface mode.
(config)#router isis bb	Create an IS-IS routing instance for area bb.
(config-router)#is-type level-2-only	Set the IS level for this area (bb) as level-2-only.
(config-router)#net bb.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 40.40.40.1/24	Configure IP address on interface.
(config-if)#ip router isis ABC	Enable IS-IS routing on interface eth2 for area ABC.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area ABC.
(config-router)#is-type level-1	Set the IS level for this area (ABC) as level-1.
(config-router)#net cc.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R3

(config)#interface eth2	Enter interface mode.
(config-if)#ip address 30.30.30.2/24	Configure IP address on interface.
(config-if)#ip router isis xyz	Enable IS-IS routing on interface eth2 for area xyz.
(config-if)#exit	Exit interface mode.
(config)#router isis xyz	Create an IS-IS routing instance for area xyz.
(config-router)#is-type level-1	Set the IS level for this area (xyz) as level-1.
(config-router)#net 52.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R4

(config)#interface eth2	Enter interface mode.
(config-if)#ip address 40.40.40.2/24	Configure IP address on interface.
(config-if)#ip router isis aa	Enable IS-IS routing on interface eth2 for area aa.
(config-if)#exit	Exit interface mode.
(config)#router isis aa	Create an IS-IS routing instance for area aa.
(config-router)#is-type level-1	Set the IS level for this area (aa) as level-1.
(config-router)#net 52.0000.0000.0004.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

© 2021 IP Infusion Inc. Proprietary

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag aaa:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     25        L2   IS-IS

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 0
Total number of adjacencies: 0
Tag ccc:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 0
Total number of adjacencies: 0
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag bb:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     6         L2   IS-IS

R1#show clns is-neighbors

Tag aaa:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0002 eth1        Up     L2   64        0000.0000.0001.01

Tag ccc:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id

R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id

Tag bb:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0001 eth1        Up     L2   64        0000.0000.0001.01

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid
```


© 2021 IP Infusion Inc. Proprietary

```
Tag aaa:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0


Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ccc:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    30.30.30.0/24       10          --                  eth2            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag ABC:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    40.40.40.0/24       10          --                  eth2            0


Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag bb:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0

R1#show isis topology

Tag aaa:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       eth1
5254.002a.230a


Tag ccc:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0002       --

R2#show isis topology

Tag ABC:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0003       --


Tag bb:  VRF : default
IS-IS paths to level-2 routers
```

```
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       10         0000.0000.0001       eth1
5254.00dc.0b76
0000.0000.0002       --

R1#show isis database
Tag aaa:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000002   0x181D        1003              0/0/0
0000.0000.0001.01-00* 0x00000001   0x21B9        1003              0/0/0
0000.0000.0002.00-00  0x00000005   0x1818        1080              0/0/0

Tag ccc:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x00000001   0xDFA5        685               0/0/0

R2#show isis database
Tag ABC:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0003.00-00* 0x00000002   0xD571        696               0/0/0

Tag bb:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000002   0x181D        938               0/0/0
0000.0000.0001.01-00  0x00000001   0x21B9        938               0/0/0
0000.0000.0002.00-00* 0x00000005   0x1818        1017              0/0/0

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.12.30.0/24 is directly connected, eth0, 01:37:50
C            20.20.20.0/24 is directly connected, eth1, 00:10:13
C            30.30.30.0/24 is directly connected, eth2, 00:10:13
C            127.0.0.0/8 is directly connected, lo, 01:37:50

Gateway of last resort is not set

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
```


© 2021 IP Infusion Inc. Proprietary

```
        * - candidate default

IP Route Table for VRF "default"
C            10.12.30.0/24 is directly connected, eth0, 01:37:26
C            20.20.20.0/24 is directly connected, eth1, 00:05:03
C            40.40.40.0/24 is directly connected, eth2, 00:08:52
C            127.0.0.0/8 is directly connected, lo, 01:37:26

Gateway of last resort is not set
```

Route Leaking

Route leaking is defined in RFC 2966. For Level-1 (L1) routers, only level-1 routes are populated in the routing table. The L1 router has a default route to the nearest Level-1/Level-2 (L1/L2) router: This could result in sub-optimal routing in certain scenarios. Route leaking causes an L1/L2 router to advertise the level-2 routes in its database to the L1 router, thus allowing the L1 router to acknowledge the prefixes advertised by the Level-2 (L2) router. In this way, the L1 router has the ability to learn the true cost to reach other areas.

In the following example, R1 is the L1 router, R2 is the L1/L2 router doing the route leaking, and R3 is the L2 router. The following configuration is given only for R2, assuming that the adjacency with R1 and R3 are already up, and the route tables with appropriate routes are already populated.

Topology

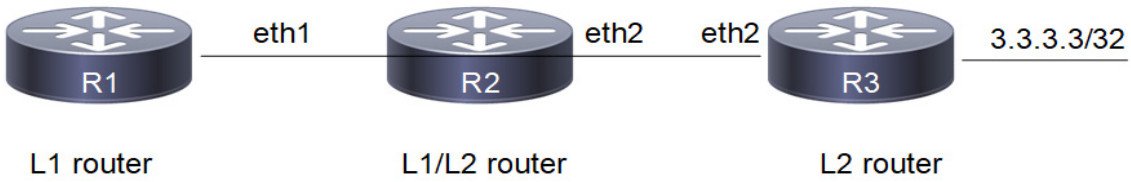


Figure 6-122: Route Leaking Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0000.0001.00`	Define the NET address.
`(config-router)#is-type level-1`	Configure instance as level-1-only routing.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Specify the interface (eth1)to configure and enter Interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure IP address on interface.
`(config-if)#isis circuit-type level-1`	Set the circuit type as level-1 for the interface
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R2).

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (eth1)to configure and enter Interface mode.
`(config-if)#ip address 20.20.20.2/24`	Configure IP address on interface.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R1).
`(config-if)#isis circuit-type level-1`	Configure instance as level-1-only routing.
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#interface eth2`	Specify the interface (eth2)to configure and enter Interface mode.
`(config-if)#ip address 30.30.30.1/24`	Configure IP address on interface.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth2 (connected to R3).
`(config-if)#isis circuit-type level-2-only`	Configure instance as level-2-only routing.
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0000.0002.00`	Define the NET address.
`(config-router-af)#redistribute isis level-2 into level-1`	Enable redistribution of isis routes from level-2 into level-1

R3

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface (lo)to configure and enter Interface mode.
`(config-if)#ip address 3.3.3.3/32 secondary`	Configure IP address on loopback interface.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface lo
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0001.0000.0000.0003.00`	Define the NET address.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth2`	Specify the interface (eth2)to configure and enter Interface mode.
`(config-if)#ip address 30.30.30.2/24`	Configure IP address on interface.
`(config-if)#isis circuit-type level-2-only`	Set the circuit type as level-2-only for the interface
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R2).

© 2021 IP Infusion Inc. Proprietary

In the example, route, `i ia 3.3.3.3/32 [115/30] via 20.20.20.2, eth1, 00:12:29`, is the L2 route leaked by the L1/L2 router into the L1 router.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a      Up     21        L1   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76      Up     5         L1   IS-IS
0000.0000.0003 eth2        5254.00a8.940d      Up     6         L2   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2        5254.007e.5ade      Up     21        L2   IS-IS

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
ia   3.3.3.3/32          30          20.20.20.2          eth1            0
C    20.20.20.0/24       10          --                  eth1            0
ia   30.30.30.0/24       20          20.20.20.2          eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid
```

```
Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L2   3.3.3.3/32          20          30.30.30.2          eth2            0
C    20.20.20.0/24       10          --                  eth1            0
C    30.30.30.0/24       10          --                  eth2            0

R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    3.3.3.3/32          10          --                  lo            0
L2   20.20.20.0/24       20          30.30.30.1          eth2            0
C    30.30.30.0/24       10          --                  eth2            0

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
i ia         3.3.3.3/32 [115/30] via 20.20.20.2, eth1, 00:20:53
C            10.12.30.0/24 is directly connected, eth0, 01:02:10
C            20.20.20.0/24 is directly connected, eth1, 00:48:08
i ia         30.30.30.0/24 [115/20] via 20.20.20.2, eth1, 00:23:30
C            127.0.0.0/8 is directly connected, lo, 01:02:10

Gateway of last resort is not set

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
i L2         3.3.3.3/32 [115/20] via 30.30.30.2, eth2, 00:21:07
```


© 2021 IP Infusion Inc. Proprietary

```
C            10.12.30.0/24 is directly connected, eth0, 01:01:55
C            20.20.20.0/24 is directly connected, eth1, 00:48:12
C            30.30.30.0/24 is directly connected, eth2, 00:48:12
C            127.0.0.0/8 is directly connected, lo, 01:01:55

Gateway of last resort is not set

R3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            3.3.3.3/32 is directly connected, lo, 00:21:25
C            10.12.30.0/24 is directly connected, eth0, 01:01:26
i L2         20.20.20.0/24 [115/20] via 30.30.30.1, eth2, 00:24:06
C            30.30.30.0/24 is directly connected, eth2, 00:48:13
C            127.0.0.0/8 is directly connected, lo, 01:01:26

Gateway of last resort is not set

R1#show isis database
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x0000000C   0xE4B5        642               0/0/0
0000.0000.0001.01-00* 0x00000007   0x13C3        642               0/0/0
0000.0000.0002.00-00  0x00000012   0x8AC8        804               0/0/0

R2#show isis database
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000003   0xF6AC        304               0/0/0
0000.0000.0001.01-00  0x00000002   0x1DBE        304               0/0/0
0000.0000.0002.00-00* 0x00000009   0x2ECA        358               0/0/0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x00000007   0x2F5A        353               0/0/0
0000.0000.0003.00-00  0x00000003   0x25E6        347               0/0/0
0000.0000.0003.02-00  0x00000002   0x24B0        347               0/0/0

R3#show isis database
Tag 1:  VRF : default
```

```
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00  0x00000007   0x2F5A        335               0/0/0
0000.0000.0003.00-00* 0x00000003   0x25E6        331               0/0/0
0000.0000.0003.02-00* 0x00000002   0x24B0        331               0/0/0


R1#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       eth1        5254.002a.230a

R2#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       10         0000.0000.0001       eth1        5254.00dc.0b76
0000.0000.0002       --

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0002       --
0000.0000.0003       10         0000.0000.0003       eth2        5254.00a8.940d

R3#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0002       10         0000.0000.0002       eth2        5254.007e.5ade
0000.0000.0003       --
```

Route Summarization

Route summarization makes the routing table smaller, but still allows complete IP connectivity, if everything is configured properly.

The following example consists of a three-router topology, in which R2 is doing the summarization. In this example, R1 is the L1 router, R2 is the L1/L2 router doing the summarization, and R3 is the L2 router. The following configuration is given only for R2, assuming that the adjacencies with R1 and R3 are already up, and the route tables with the appropriate routes are already populated.

© 2021 IP Infusion Inc. Proprietary

Topology

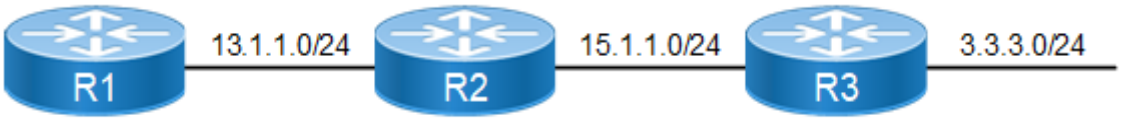


Figure 6-123: Route Summarization Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0000.0001.00`	Define the NET address.
`(config-router)#is-type level-1`	Configure instance as level-1.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Specify the interface (eth1)to configure and enter Interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure IP address on interface.
`(config-if)#isis circuit-type level-1`	Set the circuit type as level-1 for the interface
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R2).

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (eth1)to configure and enter Interface mode.
`(config-if)#isis circuit-type level-1`	Set the circuit type as level-1 for the interface
`(config-if)#ip address 20.20.20.2/24`	Configure IP address on interface.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R1).
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#interface eth2`	Specify the interface (eth2)to configure and enter Interface mode.
`(config-if)#ip address 30.30.30.1/24`	Configure IP address on interface.
`(config-if)#isis circuit-type level-2-only`	Set the circuit type as level-2-only for the interface
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth2 (connected to R3).
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0000.0002.00`	Define the NET address.

© 2021 IP Infusion Inc. Proprietary

`(config-router-af)#redistribute isis level-2 into level-1`	Enable redistribution of isis routes from level-2 into level-1
`(config-router-af)#summary-address 66.66.66.0/24 level-1 metric 50`	Configure the summary address to summarize IP reachability information.

R3

`#configure terminal`	Enter configure mode.
`(config)#ip route 66.66.66.1/32 eth2`	Configure ip static route.
`(config)#ip route 66.66.66.2/32 eth2`	Configure ip static route.
`(config)#ip route 66.66.66.3/32 eth2`	Configure ip static route.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0001.0000.0000.0003.00`	Define the NET address.
`(config-router)#redistribute static`	Enable redistribution of static routes into ISIS instance.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth2`	Specify the interface (eth2)to configure and enter Interface mode.
`(config-if)#ip address 30.30.30.2/24`	Configure IP address on interface.
`(config-if)#isis circuit-type level-2-only`	Set the circuit type as level-2-only for the interface
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R2).

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     20        L1   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     6         L1   IS-IS
0000.0000.0003 eth2        5254.00a8.940d  Up     7         L2   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 0
```


© 2021 IP Infusion Inc. Proprietary

```
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2        5254.007e.5ade      Up     21        L2   IS-IS

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
ia   30.30.30.0/24       20          20.20.20.2          eth1            0
ia   66.66.66.0/24       60          20.20.20.2          eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0
C    30.30.30.0/24       10          --                  eth2            0
D    66.66.66.0/24       0           --                  --
L2   66.66.66.1/32       10          30.30.30.2          eth2            0
L2   66.66.66.2/32       10          30.30.30.2          eth2            0
L2   66.66.66.3/32       10          30.30.30.2          eth2            0

R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L2   20.20.20.0/24       20          30.30.30.1          eth2            0
C    30.30.30.0/24       10          --                  eth2            0
E    66.66.66.1/32       0           --                  --              0
E    66.66.66.2/32       0           --                  --              0
E    66.66.66.3/32       0           --                  --              0


R1#show isis database verbose
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000004   0xF4AD        850               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.1
  Metric:   10         IS 0000.0000.0001.01
```

```
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0001.01-00* 0x00000003   0x1BBF        850               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00  0x00000010   0xB5E0        1165              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.2
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 20.20.20.0 255.255.255.0
  Metric:   10         IP-Interarea 30.30.30.0 255.255.255.0
  Metric:   50         IP-External 66.66.66.0     255.255.255.0


R2#show isis database verbose
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000004   0xF4AD        820               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.1
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0001.01-00  0x00000003   0x1BBF        820               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000010   0xB5E0        1137              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.2
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 20.20.20.0 255.255.255.0
  Metric:   10         IP-Interarea 30.30.30.0 255.255.255.0
  Metric:   50         IP-External 66.66.66.0     255.255.255.0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x00000005   0x1577        838               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.1
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IP 30.30.30.0 255.255.255.0
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0003.00-00  0x0000000B   0xFED3        1160              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IP 30.30.30.0 255.255.255.0
  Metric:   0          IP-External 66.66.66.1     255.255.255.255
  Metric:   0          IP-External 66.66.66.2     255.255.255.255
  Metric:   0          IP-External 66.66.66.3     255.255.255.255
0000.0000.0003.01-00  0x00000003   0x29AB        837               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00
```


© 2021 IP Infusion Inc. Proprietary

```
R3#show isis database verbose
Tag 1:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00  0x00000005   0x1577        818               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.1
  Metric:   10          IS 0000.0000.0003.01
  Metric:   10          IP 30.30.30.0 255.255.255.0
  Metric:   10          IP 20.20.20.0 255.255.255.0
0000.0000.0003.00-00* 0x0000000B   0xFED3        1142              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.2
  Metric:   10          IS 0000.0000.0003.01
  Metric:   10          IP 30.30.30.0 255.255.255.0
  Metric:   0           IP-External 66.66.66.1     255.255.255.255
  Metric:   0           IP-External 66.66.66.2     255.255.255.255
  Metric:   0           IP-External 66.66.66.3     255.255.255.255
0000.0000.0003.01-00* 0x00000003   0x29AB        819               0/0/0
  Metric:   0           IS 0000.0000.0003.00
  Metric:   0           IS 0000.0000.0002.00
```

IS-IS Distance

Administrative distance in IS-IS can be configured for a specified source ID or for all routes.

This example shows configuring the IS-IS administrative distance for the IPv4 address family.

Topology

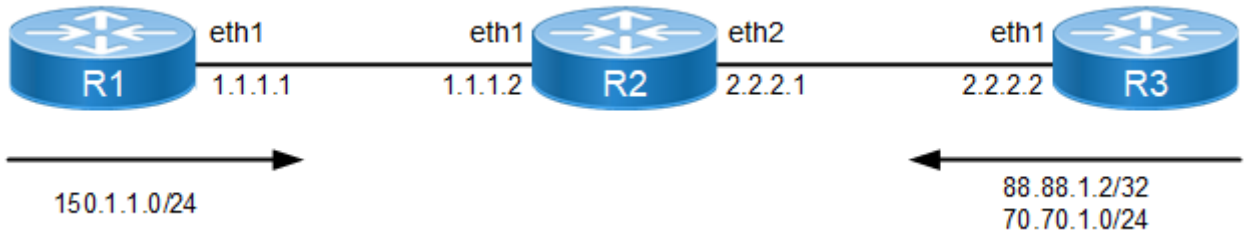


Figure 6-124: IS-IS Distance Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 1.1.1.1/24`	Assign the IP address on this interface (`eth1`).

(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1.
(config-if)#exit	Exit interface mode.
(config)#ip route 150.1.1.0/24 eth1	Configure static routes.
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#net 49.0001.0000.0001.00	Set a Network Entity Title (NET) for this instance, specifying the address and the system ID.
(config-router)#redistribute static	Redistribute the static routes.

R2

#configure terminal	Enter configure mode
(config)#ip access-list DIST	Enter access list mode
(config-ip-acl)#permit ipip 88.88.1.2/32 any	Create an access list to permit the 88.88.1.2/32 route from R3.
(config-ip-acl)#exit	Exit access list mode
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 1.1.1.2/24	Assign the IP address on this interface (eth1).
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 2.2.2.1/24	Assign the IP address on this interface (eth2).
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth2
(config-if)#exit	Exit interface mode
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#net 49.0001.0000.0002.00	Specify the NET address.
(config-router)#distance 100	Configure the administrative distance for all routes received from R1 and R2.
(config-router)#distance 20 0001.0000.0001	Configure the administrative distance for all routes received from R1. This command overwrites the applied distance, 100, and will apply distance 20 for all routes received from R1.
(config-router)#distance 30 0001.0000.0003 DIST	Configure the distance, 30, to the route, 88.88.1.2/32, received from R3. All other routes from R3 (for example, 70.70.1.0/24) will have the distance applied as 100. If the distance, 100, is not configured, all other routes will have a default distance of 115.

R3

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 2.2.2.2/24	Assign the IP address on this interface (eth1).
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1.
(config-if)#exit	Exit interface mode.
(config)#ip route 88.88.1.2/32 eth2	Configure static routes
(config)#ip route 70.70.1.0/24 eth2	Configure static routes

© 2021 IP Infusion Inc. Proprietary

(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#net 49.0001.0000.0003.00	Specify the NET address.
(config-router)#redistribute static	Redistribute the static routes.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0001.0000.0002 eth1        5254.002a.230a  Up     18        L1   IS-IS
                                           Up     18        L2   IS-IS
R2#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 2
Total number of adjacencies: 4
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0001.0000.0001 eth1        5254.00dc.0b76  Up     7         L1   IS-IS
                                           Up     7         L2   IS-IS
0001.0000.0003 eth2        5254.00a8.940d  Up     8         L1   IS-IS
                                           Up     8         L2   IS-IS
R3#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0001.0000.0002 eth2        5254.007e.5ade  Up     20        L1   IS-IS
                                           Up     20        L2   IS-IS
R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    1.1.1.0/24          10          --                  eth1            0
L1   2.2.2.0/24          20          1.1.1.2             eth1            0
L2   70.70.1.0/24        20          1.1.1.2             eth1            0
L2   88.88.1.2/32        20          1.1.1.2             eth1            0
E    150.1.1.0/24        0           --                  --             0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid
```

```
Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    1.1.1.0/24          10          --                  eth1            0
C    2.2.2.0/24          10          --                  eth2            0
L2   70.70.1.0/24        10          2.2.2.2             eth2            0
L2   88.88.1.2/32        10          2.2.2.2             eth2            0
L2   150.1.1.0/24        10          1.1.1.1             eth1            0

R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L1   1.1.1.0/24          20          2.2.2.1             eth2            0
C    2.2.2.0/24          10          --                  eth2            0
E    70.70.1.0/24        0           --                  --             0
E    88.88.1.2/32        0           --                  --             0
L2   150.1.1.0/24        20          2.2.2.1             eth2            0



R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            1.1.1.0/24 is directly connected, eth1, 00:30:56
i L1         2.2.2.0/24 [115/20] via 1.1.1.2, eth1, 00:26:01
C            10.12.30.0/24 is directly connected, eth0, 00:33:46
i L2         70.70.1.0/24 [115/20] via 1.1.1.2, eth1, 00:21:39
i L2         88.88.1.2/32 [115/20] via 1.1.1.2, eth1, 00:15:04
C            127.0.0.0/8 is directly connected, lo, 00:33:46
S            150.1.1.0/24 [1/0] is directly connected, eth1, 00:29:03

Gateway of last resort is not set

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            1.1.1.0/24 is directly connected, eth1, 00:26:46
```


© 2021 IP Infusion Inc. Proprietary

```
C            2.2.2.0/24 is directly connected, eth2, 00:26:30
C            10.12.30.0/24 is directly connected, eth0, 00:33:21
i L2         70.70.1.0/24 [100/10] via 2.2.2.2, eth2, 00:21:55
i L2         88.88.1.2/32 [30/10] via 2.2.2.2, eth2, 00:15:09
C            127.0.0.0/8 is directly connected, lo, 00:33:21
i L2         150.1.1.0/24 [10/10] via 1.1.1.1, eth1, 00:25:53

Gateway of last resort is not set

R3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
i L1         1.1.1.0/24 [115/20] via 2.2.2.1, eth2, 00:22:56
C            2.2.2.0/24 is directly connected, eth2, 00:23:01
C            10.12.30.0/24 is directly connected, eth0, 00:33:57
S            70.70.1.0/24 [1/0] is directly connected, eth2, 00:23:01
S            88.88.1.2/32 [1/0] is directly connected, eth2, 00:16:07
C            127.0.0.0/8 is directly connected, lo, 00:33:57
i L2         150.1.1.0/24 [115/20] via 2.2.2.1, eth2, 00:22:42

Gateway of last resort is not set

R1#show isis database
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00* 0x00000003   0x2AEC        448               0/0/0
0001.0000.0001.01-00* 0x00000002   0x32A4        448               0/0/0
0001.0000.0002.00-00  0x00000004   0x5A80        698               0/0/0
0001.0000.0003.00-00  0x00000006   0xE820        702               0/0/0
0001.0000.0003.01-00  0x00000002   0x3E94        698               0/0/0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00* 0x00000008   0xB20F        703               0/0/0
0001.0000.0001.01-00* 0x00000002   0x32A4        448               0/0/0
0001.0000.0002.00-00  0x00000004   0x5A80        698               0/0/0
0001.0000.0003.00-00  0x0000000A   0xB2CE        1108              0/0/0
0001.0000.0003.01-00  0x00000002   0x3E94        698               0/0/0

R2#show isis database
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00  0x00000003   0x2AEC        402               0/0/0
0001.0000.0001.01-00  0x00000002   0x32A4        401               0/0/0
0001.0000.0002.00-00* 0x00000004   0x5A80        653               0/0/0
0001.0000.0003.00-00  0x00000006   0xE820        656               0/0/0
0001.0000.0003.01-00  0x00000002   0x3E94        652               0/0/0
```

```
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00  0x00000008   0xB20F        657               0/0/0
0001.0000.0001.01-00  0x00000002   0x32A4        401               0/0/0
0001.0000.0002.00-00* 0x00000004   0x5A80        653               0/0/0
0001.0000.0003.00-00  0x0000000A   0xB2CE        1062              0/0/0
0001.0000.0003.01-00  0x00000002   0x3E94        652               0/0/0

R3#show isis database
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00  0x00000003   0x2AEC        317               0/0/0
0001.0000.0001.01-00  0x00000002   0x32A4        317               0/0/0
0001.0000.0002.00-00  0x00000004   0x5A80        568               0/0/0
0001.0000.0003.00-00* 0x00000006   0xE820        573               0/0/0
0001.0000.0003.01-00* 0x00000002   0x3E94        569               0/0/0

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0001.0000.0001.00-00  0x00000008   0xB20F        573               0/0/0
0001.0000.0001.01-00  0x00000002   0x32A4        317               0/0/0
0001.0000.0002.00-00  0x00000004   0x5A80        568               0/0/0
0001.0000.0003.00-00* 0x0000000A   0xB2CE        979               0/0/0
    0001.0000.0003.01-00* 0x00000002   0x3E94        569               0/0/0

R1#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       --
0001.0000.0002       10         0001.0000.0002       eth1
5254.002a.230a
0001.0000.0003       20         0001.0000.0002       eth1
5254.002a.230a

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       --
0001.0000.0002       10         0001.0000.0002       eth1
5254.002a.230a
0001.0000.0003       20         0001.0000.0002       eth1
5254.002a.230a

R2#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       10         0001.0000.0001       eth1
5254.00dc.0b76
0001.0000.0002       --
0001.0000.0003       10         0001.0000.0003       eth2
5254.00a8.940d

IS-IS paths to level-2 routers
```


© 2021 IP Infusion Inc. Proprietary

```
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       10         0001.0000.0001       eth1
5254.00dc.0b76
0001.0000.0002       --
0001.0000.0003       10         0001.0000.0003       eth2
5254.00a8.940d

R3#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       20         0001.0000.0002       eth2
5254.007e.5ade
0001.0000.0002       10         0001.0000.0002       eth2
5254.007e.5ade
0001.0000.0003       --

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0001.0000.0001       20         0001.0000.0002       eth2
5254.007e.5ade
0001.0000.0002       10         0001.0000.0002       eth2
5254.007e.5ade
0001.0000.0003       --
```

Passive Interface

In ISP and large enterprise networks, many of the distribution routers have more than 200 interfaces. Before the Default Passive-Interface feature, there were two possibilities for obtaining routing information from all of these interfaces:

- Configure a routing protocol on the backbone interfaces and redistribute connected interfaces.
- Configure the routing protocol on all interfaces and manually set most of them as passive, which was time consuming.

The solution to this problem was to configure the routing protocol on all interfaces and manually set the `passive-interface` command on the interfaces where adjacency was not desired. In certain networks, this meant coding 200 or more passive-interface statements. With the Default Passive Interface feature, this problem is solved by allowing all interfaces to be set as passive by default using a single `passive-interface` default command, then configuring individual interfaces in which adjacencies are desired using the `passive-interface <interface-name> disable` command.

Usage

1. When a specific interface is configured as passive using the `passive-interface <interface-name>` command:
   - The interface loses its adjacency on that interface, for example, eth1.
   - The interface (eth1) is still advertised by other IS-IS speaking interfaces to their neighbors.
2. When a specific interface is configured as passive using `passive-interface <interface-name>` command followed by removing the configuration using `no passive-interface <interface-name>` command:
   - The interface is IS-IS disabled and must be enabled using the `ip router isis` command (for example, `ip router isis 1`).

- If IS-IS is not configured, the interface (for example, eth1) will not be advertised by other IS-IS speaking interfaces to their neighbors.

3. When an interface is configured with the `passive interface` command:
   - All IS-IS enabled interfaces lose their adjacency.
   - All IS-IS enabled interfaces in the system will be made passive.
   - To establish adjacency on a particular interface, the `passive interface <interface-name> disable` command must be enabled.
   - All interfaces which were made passive are advertised by the active IS-IS speaking interface to its neighbors.
4. When an interface is configured with the `no passive interface` command:
   - All interfaces which are currently passive, will become active.
   - If IS-IS is configured on those interface, it will start sending out IS-IS packets and attempt to form adjacency.
   - If IS-IS is not configured on those interfaces, it will not be advertised by the active IS-IS speaking interface to its neighbors.

Topology

Figure 6-125 shows a passive-interface configuration example.



Figure 6-125: IS-IS Passive Interface

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance `(1)`.
`(config-router)#net 49.0001.0000.0000.0001.00`	Define the NET address.
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure and enter Interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure IP address on interface.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth1` (connected to R2).

© 2021 IP Infusion Inc. Proprietary

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (eth1)to configure and enter Interface mode.
`(config-if)#ip address 20.20.20.2/24`	Configure IP address on interface.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R1).
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#interface eth2`	Specify the interface (eth2)to configure and enter Interface mode.
`(config-if)#ip address 30.30.30.1/24`	Configure IP address on interface.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth2 (connected to R3).
`(config-if)#exit`	Exit interface mode and return to Configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#net 49.0001.0000.0000.0002.00`	Define the NET address.
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#passive-interface eth1`	Configure the eth1 interface as passive.

R3

`#configure terminal`	Enter configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (1).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0001.0000.0000.0003.00`	Define the NET address.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth2`	Specify the interface (eth2)to configure and enter Interface mode.
`(config-if)#ip address 30.30.30.2/24`	Configure IP address on interface.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface eth1 (connected to R2).

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 0
Total number of adjacencies: 0
Tag 1:  VRF : default
System Id      Interface   SNPA                State  Holdtime  Type Protocol

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 1:  VRF : default
```

```
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0003 eth2        5254.00a8.940d  Up     9         L2   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2        5254.007e.5ade  Up     19        L2   IS-IS

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       10          --                  eth1            0

R2#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    20.20.20.0/24       0           --                  eth1            0
C    30.30.30.0/24       10          --                  eth2            0

R3#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
L2   20.20.20.0/24       10          30.30.30.1          eth2            0
C    30.30.30.0/24       10          --                  eth2            0

R1#show isis database verbose
Tag 1:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000004   0x3A02        923               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.1
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0001.01-00* 0x00000001   0xF108        0 (923)           0/0/0

R2#show isis database verbose
Tag 1:  VRF : default
```


© 2021 IP Infusion Inc. Proprietary

```
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000002   0x3EFF        887               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.1
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0001.01-00  0x00000001   0x21B9        888               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000003   0x3761        906               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.1
  Metric:   10         IS 0000.0000.0003.01
  Metric:   0          IP 20.20.20.0 255.255.255.0
  Metric:   10         IP 30.30.30.0 255.255.255.0
0000.0000.0003.00-00  0x00000002   0x530E        909               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IP 30.30.30.0 255.255.255.0
0000.0000.0003.01-00  0x00000001   0x2DA9        905               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00

R3#show isis database verbose
Tag 1:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000002   0x3EFF        883               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   20.20.20.1
  Metric:   10         IP 20.20.20.0 255.255.255.0
0000.0000.0001.01-00  0x00000001   0x21B9        884               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00  0x00000003   0x3761        901               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.1
  Metric:   10         IS 0000.0000.0003.01
  Metric:   0          IP 20.20.20.0 255.255.255.0
  Metric:   10         IP 30.30.30.0 255.255.255.0
0000.0000.0003.00-00* 0x00000002   0x530E        906               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   30.30.30.2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IP 30.30.30.0 255.255.255.0
0000.0000.0003.01-00* 0x00000001   0x2DA9        902               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00
```

© 2021 IP Infusion Inc. Proprietary

```
R1#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       --

R2#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       **
0000.0000.0002       --
0000.0000.0003       10         0000.0000.0003       eth2
5254.00a8.940d

R3#show isis topology

Tag 1:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       **
0000.0000.0002       10         0000.0000.0002       eth2
5254.007e.5ade
0000.0000.0003       --
```

IS-IS IPv4 Loop-Free Alternate Fast Reroute

This section contains IS-IS (Intermediate System to Intermediate System) Loop-Free Alternate Fast Reroute (LFA-FRR) configuration examples.

For details about the commands used in these examples, see the *Intermediate System to Intermediate System Command Reference*.

OSPF LFA and ISIS LFA along with MPLS is not supported. Do not configure OSPF LFA or ISIS LFA, if MPLS is configured or vice-versa.

Overview

When a primary next-hop fails, LFA-FRR reduces the failure reaction time to tens of milliseconds using a pre-computed alternate next- hop, so that the alternate can be rapidly used when the failure is detected. A network with this feature experiences less traffic loss and less micro-looping of packets than a network without LFA-FRR.

After you enable LFA-FRR, routers calculate a backup path for each primary path to reach the destination. The backup path is calculated based on the attributes such as node protecting, link protecting, and broadcast link protecting. If there is an ECMP path to reach prefixes, the backup is selected from the same primary set by default; if a secondary tie-breaker is enabled, and if a secondary path is available, the backup will be selected from the secondary path.

© 2021 IP Infusion Inc. Proprietary

Basic Configuration

Topology

Figure 6-126 shows the configuration to enable the basic ISIS LFA feature.

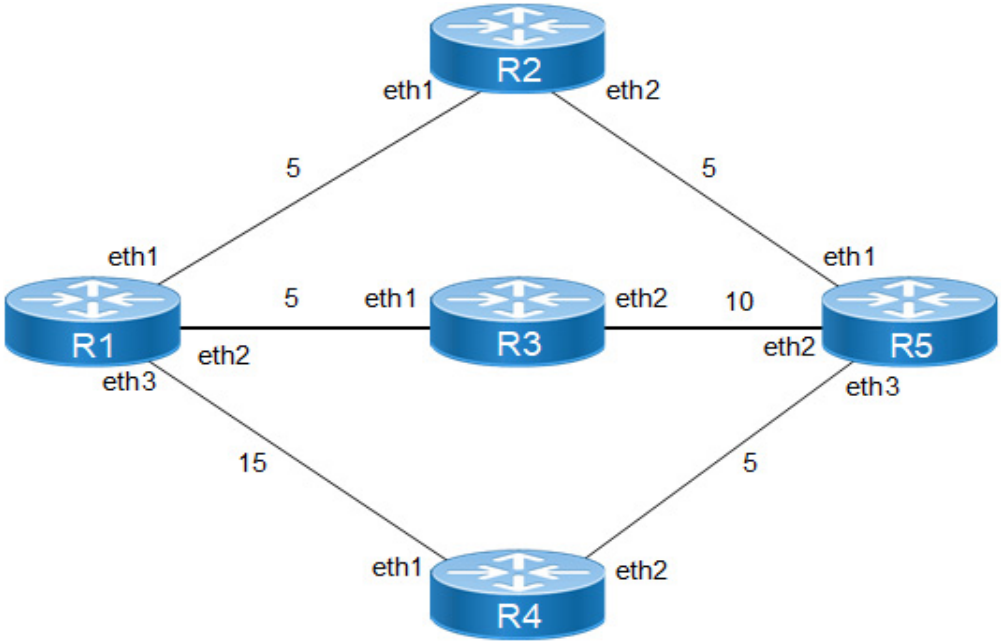


Figure 6-126: ISIS LFA-FRR

R1

`#configure terminal`	Enter configure mode.
`(config)#int eth1`	Enter interface mode.
`(config-if)#ip address 10.10.10.142/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#isis metric 5`	Configure isis metric value for interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth2`	Enter interface mode.
`(config-if)#ip address 20.20.20.142/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#isis metric 5`	Configure isis metric value for interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth3`	Enter interface mode.
`(config-if)#ip address 30.30.30.142/24`	Configure the IP address of the interface.

(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#isis metric 15	Configure isis metric value for interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0001.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#fast-reroute per-prefix level-1 proto ipv4 all	Configure LFA-FRR to calculate the available backup path for all L1 ipv4 prefixes learnt
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

R2

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 10.10.10.141/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#isis metric 5	Configure isis metric value for interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 40.40.40.141/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#isis metric 5	Configure isis metric value for interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0002.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

R3

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 20.20.20.143/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1

© 2021 IP Infusion Inc. Proprietary

(config-if)#isis metric 5	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 50.50.50.143/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 10	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0003.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

R4

#configure terminal	Enter configure mode.
(config)#int eth1	Enter interface mode.
(config-if)#ip address 30.30.30.144/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 15	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#int eth2	Enter interface mode.
(config-if)#ip address 60.60.60.144/24	Configure the IP address of the interface.
(config-if)#ip router isis 1	Enable ISIS routing on interface for area 49 with instance 1
(config-if)#isis metric 5	Configure isis metric value for interface
(config-if)#isis circuit-type level-1	Enable circuit type on interface
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance for area 49 with instance 1
(config-router)#net 49.0000.0000.0004.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#bfd all-interfaces	Enable BFD for ISIS on all interfaces
(config-router)#exit	Exit router mode.
(config)#exit	Exit config mode.

R5

`#configure terminal`	Enter configure mode.
`(config)#int eth1`	Enter interface mode.
`(config-if)#ip address 40.40.40.145/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 5`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth2`	Enter interface mode.
`(config-if)#ip address 50.50.50.145/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int eth3`	Enter interface mode.
`(config-if)#ip address 60.60.60.145/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 5`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area `49` with instance 1
`(config-router)#net 49.0000.0000.0005.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#bfd all-interfaces`	Enable BFD for ISIS on all interfaces
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

Validation

R1

ISIS neighborship:

```
R1#show clns neighbors

Total number of L1 adjacencies: 3
Total number of L2 adjacencies: 0
Total number of adjacencies: 3
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     27        L1   IS-IS
0000.0000.0003 eth2        5254.00dc.2f11  Up     7         L1   IS-IS
0000.0000.0004 eth3        5254.00f5.35a4  Up     7         L1   IS-IS
```


© 2021 IP Infusion Inc. Proprietary

```
R2#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00dc.0b76  Up     6         L1   IS-IS
0000.0000.0005 eth2        5254.00b3.110c  Up     7         L1   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.00a1.6afe  Up     22        L1   IS-IS
0000.0000.0005 eth2        5254.0056.7a3d  Up     27        L1   IS-IS

R4#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.0011.a028  Up     21        L1   IS-IS
0000.0000.0005 eth2        5254.00d3.fb41  Up     21        L1   IS-IS


R5#show clns neighbors

Total number of L1 adjacencies: 3
Total number of L2 adjacencies: 0
Total number of adjacencies: 3
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.007e.5ade  Up     27        L1   IS-IS
0000.0000.0003 eth2        5254.00a8.940d  Up     6         L1   IS-IS
0000.0000.0004 eth3        5254.00e2.aece  Up     7         L1   IS-IS
```

Check the ISIS route installation with primary and backup paths in the ISIS table and RIB table.

Primary paths:

```
R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    10.10.10.0/24       5           --                  eth1            0
C    20.20.20.0/24       5           --                  eth2            0
C    30.30.30.0/24       15          --                  eth3            0
```

```
L1   40.40.40.0/24       10          10.10.10.141        eth1            0
L1   50.50.50.0/24       15          20.20.20.143        eth2            0
L1   60.60.60.0/24       15          10.10.10.141        eth1            0

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.10.10.0/24 is directly connected, eth1, 00:43:14
C            10.12.30.0/24 is directly connected, eth0, 01:42:55
C            20.20.20.0/24 is directly connected, eth2, 00:43:14
C            30.30.30.0/24 is directly connected, eth3, 00:43:14
i L1         40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:16:42
i L1         50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:16:55
i L1         60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:16:42
C            127.0.0.0/8 is directly connected, lo, 01:42:55

Gateway of last resort is not set
```

R1#FRR backup paths:

```
R1#show ip isis route fast-reroute

Tag   : 1  VRF : default
Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
        D - discard, LP - Link Protecting, NP - Node Protecting,
        BP - Broadcast Interface Disjoint, Pri - Primary Path,
        Sec - Secondary Path, DP - Downstream Path

L1  40.40.40.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 25
    Protection Provided : LP NP BP

L1  50.50.50.0/24
    Primary Path via    : 20.20.20.143, eth2
    FRR Backup Path via : 10.10.10.141, eth1
    FRR Metric          : 20
    Protection Provided : LP NP BP

L1  60.60.60.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 20
    Protection Provided : LP NP BP DP

R1#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

 © 2021 IP Infusion Inc. Proprietary

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
i L1    40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:18:01
                      [FRR-NH] via 30.30.30.144, eth3

i L1    50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:18:14
                      [FRR-NH] via 10.10.10.141, eth1

i L1    60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:18:01
                      [FRR-NH] via 30.30.30.144, eth3
```

It is not mandatory that for all primary paths, there exists an LFA backup path only if inequality equation satisfies according to attributes configured on routers, backup path will be calculated.

To prohibit an interface from being used as a repair path, disable fast reroute calculation on the interface:

`R1(config-if)#interface eth1`	Enter interface.
`(config-if)#isis fast-reroute per-prefix candidate disable level-1`	Disable fast reroute calculation on the interface.
`(config-if)#end`	Exit.

Verify that the `eth1` interface is not used for backup path calculation.

```
R1#show ip isis route fast-reroute

Tag   : 1  VRF : default
Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
        D - discard, LP - Link Protecting, NP - Node Protecting,
        BP - Broadcast Interface Disjoint, Pri - Primary Path,
        Sec - Secondary Path, DP - Downstream Path

L1  40.40.40.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 25
    Protection Provided : LP NP BP

L1  50.50.50.0/24
    Primary Path via    : 20.20.20.143, eth2
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 30
    Protection Provided : LP NP BP

L1  60.60.60.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 20
    Protection Provided : LP NP BP DP

R1#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
i L1    40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:20:22
                      [FRR-NH] via 30.30.30.144, eth3

i L1    50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:20:35
                      [FRR-NH] via 30.30.30.144, eth3

i L1    60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:20:22
                      [FRR-NH] via 30.30.30.144, eth3

R1#
```

Backup Path based on Route-Map Prefixes

R1

Route-map and access-list configuration:

`(config)#ip access-list 1`	Create an access-list
`(config-ip-acl)#permit any 40.40.40.0 0.0.0.255 any`	Configuring rule to permit only one prefix
`(config)#route-map rmap1 permit 1`	Create a route-map
`(config-route-map)#match ip address 1`	Apply above created access-list in route-map
`(config)#exit`	Exit config mode.

Apply the above created route-map with fast-reroute:

`(config)#router isis 1`	Create an IS-IS routing instance for area `49` with instance 1
`(config-router)#fast-reroute per-prefix level-1 proto ipv4 route-map rmap1`	Configure LFA-FRR to calculate the available backup path for routes allowed through route-map
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

Validation

```
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
```


© 2021 IP Infusion Inc. Proprietary

```
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.10.10.0/24 is directly connected, eth1, 01:02:04
C            10.12.30.0/24 is directly connected, eth0, 02:01:45
C            20.20.20.0/24 is directly connected, eth2, 01:02:04
C            30.30.30.0/24 is directly connected, eth3, 01:02:04
i L1         40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:35:32
i L1         50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:35:45
i L1         60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:35:32
C            127.0.0.0/8 is directly connected, lo, 02:01:45

Gateway of last resort is not set

R1#show ip isis route fast-reroute

Tag   : 1  VRF : default
Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
        D - discard, LP - Link Protecting, NP - Node Protecting,
        BP - Broadcast Interface Disjoint, Pri - Primary Path,
        Sec - Secondary Path, DP - Downstream Path

L1  40.40.40.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 25
    Protection Provided : LP NP BP

R1#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
i L1    40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:35:48
                      [FRR-NH] via 30.30.30.144, eth3  FRR Table has only
allowed prefix through route-map , for remaining prefixes, FRR not present
```

LFA Tie-Breaker

Based on the index values configured, if inequalities are satisfied, protections will be provided:

- Lower the index will have the highest priority, The path which provides protection with highest priority will be selected. If there are multiple paths providing the highest priority protection then we will check which of the path provides the protection which has 2nd highest priority and so on.
- If all the paths provide same priority, then the LFA route is chosen on the basis of path cost.
- If none of the paths provides the protection with highest priority, then we will see which path provides the 2nd highest priority and so on.

The show command below displays default values for tie-breaker, by default maximum protection (link, node, broadcast, if ecmp, ecmp backup path) will be provided.

After configuring tie-breaker with index, values will be changed accordingly.

```
R1#show ip isis lfa-config level-1

TIE-Breaker Preference values
-----------------------------------------------
 Primary Path                 : 20
 Link Protecting              : 60
 Node Protecting              : 30
 Broadcast Interface Disjoint : 70
 Secondary Path               : 255
 Downstream Path              : 90

 Termination Hold On Interval : 1000 ms
```

R1

To change index values, below configurations should be used, with the lower the index highest the priority.

`(config)#router isis 1`	Create an IS-IS routing instance for area `49` with instance 1
`(config-router)#fast-reroute per-prefix level-1 proto ipv4 all`	Configure LFA-FRR to calculate the available backup path for all L1 ipv4 prefixes learned
`(config-router)#fast-reroute tie-break level-1 proto ipv4 interface-disjoint index 1`	Configure index value to change priority for link protection
`(config-router)#fast-reroute tie-break level-1 proto ipv4 node-protecting index 2`	Configure index value to change priority for node protection
`(config-router)#fast-reroute tie-break level-1 proto ipv4 broadcast-interface-disjoint index 3`	Configure index value to change priority for broadcast link protection
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

Validation

```
R1#show ip isis lfa-config level-1

TIE-Breaker Preference values
-----------------------------------------------
 Primary Path                 : 20
 Link Protecting              : 1
 Node Protecting              : 2
 Broadcast Interface Disjoint : 3
 Secondary Path               : 255
 Downstream Path              : 90

 Termination Hold On Interval : 1000 ms
```


© 2021 IP Infusion Inc. Proprietary

```
R1#show ip isis route fast-reroute

Tag   : 1  VRF : default
Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
        D - discard, LP - Link Protecting, NP - Node Protecting,
        BP - Broadcast Interface Disjoint, Pri - Primary Path,
        Sec - Secondary Path, DP - Downstream Path

L1  40.40.40.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 25
    Protection Provided : LP NP BP

L1  50.50.50.0/24
    Primary Path via    : 20.20.20.143, eth2
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 20
    Protection Provided : LP NP BP

L1  60.60.60.0/24
    Primary Path via    : 10.10.10.141, eth1
    FRR Backup Path via : 30.30.30.144, eth3
    FRR Metric          : 20
    Protection Provided : LP NP BP DP

R1#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info
       * - candidate default

IP Route Table for VRF "default"
i L1    40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:45:16
                      [FRR-NH] via 30.30.30.144, eth3

i L1    50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:45:29
                      [FRR-NH] via 30.30.30.144, eth3

i L1    60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:45:16
                      [FRR-NH] via 30.30.30.144, eth3
```

LFA Termination

A router MUST limit the amount of time an alternate next-hop is used after the primary next-hop has become unavailable. This ensures that the router will start using the new primary next-hops.

LFA termination avoids a micro looping in topology, when particular network goes down, LFA backup path will be installed and if termination interval is configured, LFA backup will be still used till the interval and it is used in order to verify new primary path is loop free.

R1

Configure termination interval on R1 in router mode:

`(config)#router isis 1`	Create an IS-IS routing instance for area `49` with instance 1
`(config-router)#fast-reroute terminate-hold-on interval 100000`	Configure LFA termination interval
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

Validation

```
R1#show ip isis lfa-config level-1

TIE-Breaker Preference values
-------------------------------------------------
 Primary Path                 : 20
 Link Protecting              : 1
 Node Protecting              : 2
 Broadcast Interface Disjoint : 3
 Secondary Path               : 255
 Downstream Path              : 90

 Termination Hold On Interval : 100000 ms

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.10.10.0/24 is directly connected, eth1, 01:19:46
C            10.12.30.0/24 is directly connected, eth0, 02:19:27
C            20.20.20.0/24 is directly connected, eth2, 01:19:46
C            30.30.30.0/24 is directly connected, eth3, 01:19:46
i L1         40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:53:14
i L1         50.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:53:27
i L1         60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:53:14
C            127.0.0.0/8 is directly connected, lo, 02:19:27

Gateway of last resort is not set
```

Shut down one of the primary nexthops, here eth2 of R1:

`(config)#interface eth2`	Enter interface mode
`(config-if)#shutdown`	Shutdown the interface

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit interface mode
(config)exit	Exit config mode

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.002a.230a  Up     27        L1   IS-IS
0000.0000.0004 eth3        5254.00f5.35a4  Up     7         L1   IS-IS
```

Here, eth1 has become a primary path, which was originally a backup path:

```
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            10.10.10.0/24 is directly connected, eth1, 01:24:47
C            10.12.30.0/24 is directly connected, eth0, 02:24:28
C            30.30.30.0/24 is directly connected, eth3, 01:24:47
i L1         40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:02:01
i L1         50.50.50.0/24 [115/20] via 10.10.10.141, eth1, 00:02:01
i L1         60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:02:01
C            127.0.0.0/8 is directly connected, lo, 02:24:28

Gateway of last resort is not set

R1#show ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
       ** - invalid

Tag 1:  VRF : default
     Destination         Metric      Next-Hop            Interface      Tag
C    10.10.10.0/24       5           --                  eth1            0
C    30.30.30.0/24       15          --                  eth3            0
L1   40.40.40.0/24       10          10.10.10.141        eth1            0
L1   50.50.50.0/24       20          10.10.10.141        eth1            0
L1   60.60.60.0/24       15          10.10.10.141        eth1            0

R1#show ip isis route fast-reroute

Tag   : 1  VRF : default
Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
```

```
          D - discard, LP - Link Protecting, NP - Node Protecting,
          BP - Broadcast Interface Disjoint, Pri - Primary Path,
          Sec - Secondary Path, DP - Downstream Path

    L1  40.40.40.0/24
        Primary Path via    : 10.10.10.141, eth1
        FRR Backup Path via : 30.30.30.144, eth3
        FRR Metric          : 25
        Protection Provided : LP NP BP

    L1  50.50.50.0/24
        Primary Path via    : 10.10.10.141, eth1
        FRR Backup Path via : 30.30.30.144, eth3
        FRR Metric          : 30
        Protection Provided : LP NP BP DP

    L1  60.60.60.0/24
        Primary Path via    : 10.10.10.141, eth1
        FRR Backup Path via : 30.30.30.144, eth3
        FRR Metric          : 20
        Protection Provided : LP NP BP DP

    R1#show ip route fast-reroute
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
    area ,p - stale info
           * - candidate default

    IP Route Table for VRF "default"

    i L1    40.40.40.0/24 [115/10] via 10.10.10.141, eth1, 00:02:19
                          [FRR-NH] via 30.30.30.144, eth3

    i L1    50.50.50.0/24 [115/20] via 10.10.10.141, eth1, 00:02:19
                          [FRR-NH] via 30.30.30.144, eth3

    i L1    60.60.60.0/24 [115/15] via 10.10.10.141, eth1, 00:02:19
                          [FRR-NH] via 30.30.30.144, eth3
```

LFA For ECMP Paths

Equal-Cost Multi-Path Routing (ECMP) is a routing technique where next-hop packet forwarding to a single destination can occur over multiple “best-paths” that tie in routing metric calculations. Because it is a per-hop decision limited to a single router, it can increase bandwidth by load-balancing traffic over multiple paths.

Here, we provide configuration capabilities for Loop-Free Alternate (LFA) Fast Reroute (FRR) along with ECMP.

Topology

Figure 6-127 shows the configuration to enable the ISIS LFA feature with ECMP.

© 2021 IP Infusion Inc. Proprietary

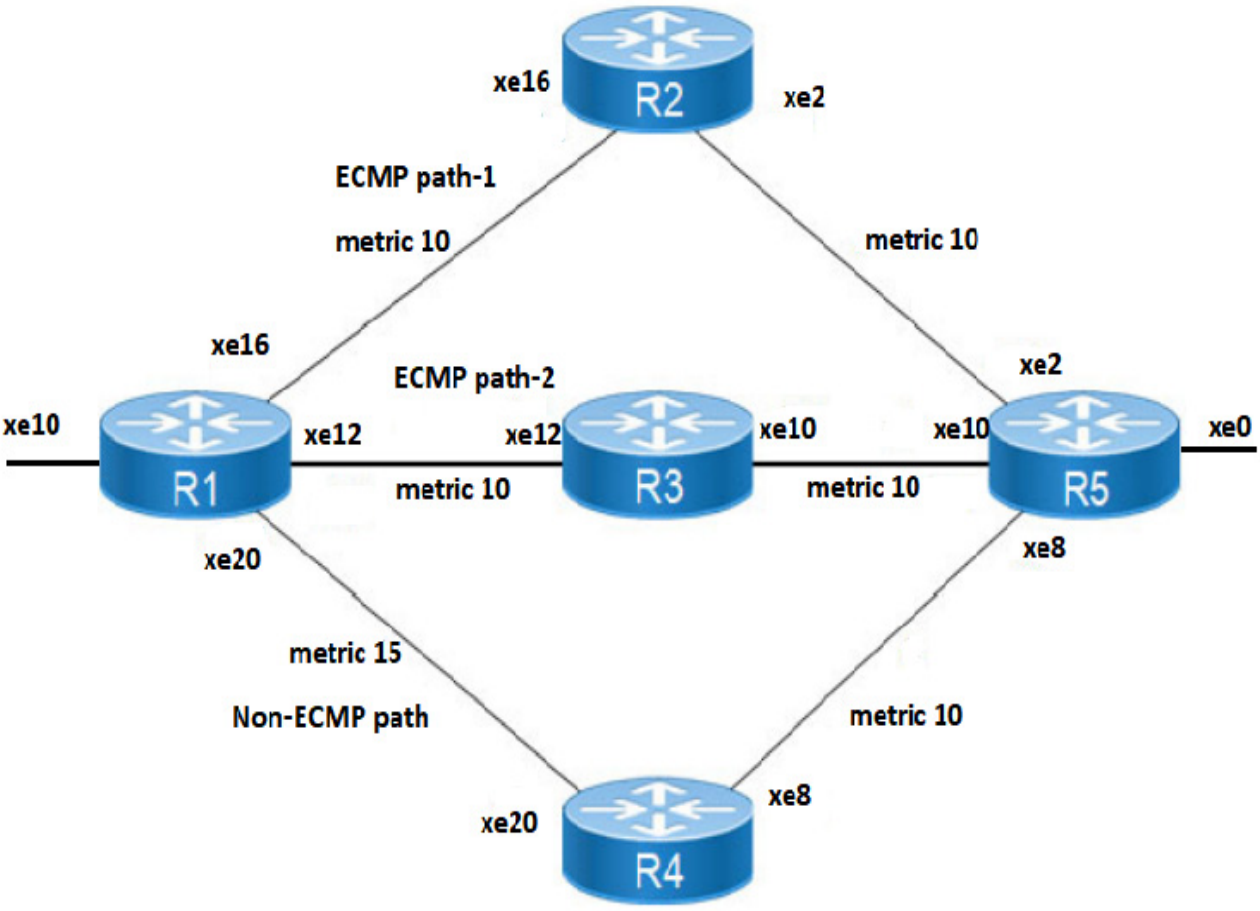


Figure 6-127: ISIS LFA-FRR ECMP

R1

`#configure terminal`	Enter configure mode.
`(config)#int xe16`	Enter interface mode.
`(config-if)#ip address 10.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int xe12`	Enter interface mode.
`(config-if)#ip address 20.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int xe20`	Enter interface mode.
`(config-if)#ip address 30.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 15`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int xe10`	Enter interface mode.
`(config-if)#ip address 31.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 with instance 1
`(config-router)# net 49.0001.0000.0000.0001.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#bfd all-interfaces`	Enable BFD for ISIS on all interfaces
`(config-router)#fast-reroute per-prefix level-1 proto ipv4 all`	Configure LFA-FRR to calculate the available backup path for all L1 ipv4 prefixes learnt
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

© 2021 IP Infusion Inc. Proprietary

R2

`#configure terminal`	Enter configure mode.
`(config)#int xe16`	Enter interface mode.
`(config-if)#ip address 10.1.1.2/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int xe2`	Enter interface mode.
`(config-if)#ip address 40.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 with instance 1
`(config-router)# net 49.0001.0000.0000.0002.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#bfd all-interfaces`	Enable BFD for ISIS on all interfaces
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

© 2021 IP Infusion Inc. Proprietary

R3

`#configure terminal`	Enter configure mode.
`(config)#int xe12`	Enter interface mode.
`(config-if)#ip address 20.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int xe10`	Enter interface mode.
`(config-if)#ip address 50.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 with instance 1
`(config-router)# net 49.0001.0000.0000.0003.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#bfd all-interfaces`	Enable BFD for ISIS on all interfaces
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

© 2021 IP Infusion Inc. Proprietary

R4

`#configure terminal`	Enter configure mode.
`(config)#int xe20`	Enter interface mode.
`(config-if)#ip address 30.1.1.2/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1g`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int xe8`	Enter interface mode.
`(config-if)#ip address 60.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 with instance 1
`(config-router)# net 49.0001.0000.0000.0004.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#bfd all-interfaces`	Enable BFD for ISIS on all interfaces
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

© 2021 IP Infusion Inc. Proprietary

RTR5

`#configure terminal`	Enter configure mode.
`(config)#int xe2`	Enter interface mode.
`(config-if)#ip address 40.1.1.2/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int xe10`	Enter interface mode.
`(config-if)#ip address 50.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int xe8`	Enter interface mode.
`(config-if)#ip address 60.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#int xe0`	Enter interface mode.
`(config-if)#ip address 21.1.1.1/24`	Configure the IP address of the interface.
`(config-if)#ip router isis 1`	Enable ISIS routing on interface for area 49 with instance 1
`(config-if)#isis metric 10`	Configure isis metric value for interface
`(config-if)#isis circuit-type level-1`	Enable circuit type on interface
`(config-if)#exit`	Exit interface mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area 49 with instance 1
`(config-router)# net 49.0001.0000.0000.0005.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#bfd all-interfaces`	Enable BFD for ISIS on all interfaces
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

Validation

```
R1 (Source):
The backup path will be selected by default from same Primary/ECMP set and
"Pri" indicates backup selected from ECMP set.
R1#show clns neighbors

Total number of L1 adjacencies: 3
Total number of L2 adjacencies: 0
```


© 2021 IP Infusion Inc. Proprietary

```
Total number of adjacencies: 3
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0003 xe12        e8c5.7a6b.732a  Up     21        L1   IS-IS
0000.0000.0002 xe16        e8c5.7a7d.532e  Up     21        L1   IS-IS
0000.0000.0004 xe20        e8c5.7a25.2752  Up     19        L1   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0005 xe2         e8c5.7a76.5820  Up     28        L1   IS-IS
0000.0000.0001 xe16        e8c5.7af5.ef2e  Up     7         L1   IS-IS

R3#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0005 xe10        e8c5.7a76.5828  Up     8         L1   IS-IS
0000.0000.0001 xe12        e8c5.7af5.ef2a  Up     5         L1   IS-IS

R4#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 0
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0005 xe8         e8c5.7a76.5826  Up     8         L1   IS-IS
0000.0000.0001 xe20        e8c5.7af5.ef32  Up     8         L1   IS-IS

R5#show clns neighbors

Total number of L1 adjacencies: 3
Total number of L2 adjacencies: 0
Total number of adjacencies: 3
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 xe2         e8c5.7a7d.5320  Up     8         L1   IS-IS
0000.0000.0004 xe8         e8c5.7a25.2746  Up     29        L1   IS-IS
0000.0000.0003 xe10        e8c5.7a6b.7328  Up     26        L1   IS-IS

R1#show ip isis route fast-reroute

Tag   : 1  VRF : default
Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
        D - discard, LP - Link Protecting, NP - Node Protecting,
        BP - Broadcast Interface Disjoint, Pri - Primary Path,
        Sec - Secondary Path, DP - Downstream Path

L1  21.1.1.0/24
```

```
    Primary Path via    : 10.1.1.2, xe16
    FRR Backup Path via : 20.1.1.2, xe12
    FRR Metric          : 30
    Protection Provided : LP NP BP Pri DP  >>> Here Pri indicates backup
selected from ECMP set

    Primary Path via    : 20.1.1.2, xe12
    FRR Backup Path via : 10.1.1.2, xe16
    FRR Metric          : 30
    Protection Provided : LP NP BP Pri DP

L1  40.1.1.0/24
    Primary Path via    : 10.1.1.2, xe16
    FRR Backup Path via : 20.1.1.2, xe12
    FRR Metric          : 30
    Protection Provided : LP NP BP

L1  50.1.1.0/24
    Primary Path via    : 20.1.1.2, xe12
    FRR Backup Path via : 10.1.1.2, xe16
    FRR Metric          : 30
    Protection Provided : LP NP BP

L1  60.1.1.0/24
    Primary Path via    : 30.1.1.2, xe20
    FRR Backup Path via : 20.1.1.2, xe12
    FRR Metric          : 30
    Protection Provided : LP NP BP DP

R1#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info, E - EVPN
       * - candidate default

IP Route Table for VRF "default"
i L1    21.1.1.0/24 [115/30] via 20.1.1.2, xe12, 00:00:57
                    [FRR-NH] via 10.1.1.2, xe16

                   [115/30] via 10.1.1.2, xe16
                    [FRR-NH] via 20.1.1.2, xe12

i L1    40.1.1.0/24 [115/20] via 10.1.1.2, xe16, 00:07:52
                    [FRR-NH] via 20.1.1.2, xe12

i L1    50.1.1.0/24 [115/20] via 20.1.1.2, xe12, 00:07:12
                    [FRR-NH] via 10.1.1.2, xe16

i L1    60.1.1.0/24 [115/25] via 30.1.1.2, xe20, 00:06:44
                    [FRR-NH] via 20.1.1.2, xe12

R1#show ip isis lfa-config level-1

TIE-Breaker Preference values
```


© 2021 IP Infusion Inc. Proprietary

```
------------------------------------------------
 Primary Path                 : 20
 Link Protecting              : 60
 Node Protecting              : 30
 Broadcast Interface Disjoint : 70
 Secondary Path               : 255
 Downstream Path              : 90

 Termination Hold On Interval : 1000 ms
```

Backup Path for ECMP Path from Non-ECMP Path

To select Backup path from secondary/Non-ECMP path, configure the below command in R1 with lowest index value.

If no backup path available from non-ecmp set , then backup path is installed from primary set.

`(config)#router isis 1`	Create an IS-IS routing instance for area `49` with instance 1
`(config-router)#net 49.0000.0000.0001.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#fast-reroute tie-break level-1 proto ipv4 secondary-path index 1`	Configure secondary path tie-breaker to select backup path from Non-ECMP path
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit config mode.

Validation

```
R1#show ip isis lfa-config level-1

TIE-Breaker Preference values
------------------------------------------------
 Primary Path                 : 20
 Link Protecting              : 60
 Node Protecting              : 30
 Broadcast Interface Disjoint : 70
 Secondary Path               : 1
 Downstream Path              : 90

 Termination Hold On Interval : 1000 ms

R1#Below, "Sec" indicates the backup path is from the Non-ECMP path
R1#show ip isis route fast-reroute

Tag   : 1  VRF : default
Codes : L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
        D - discard, LP - Link Protecting, NP - Node Protecting,
        BP - Broadcast Interface Disjoint, Pri - Primary Path,
        Sec - Secondary Path, DP - Downstream Path

L1  21.1.1.0/24
    Primary Path via    : 10.1.1.2, xe16
    FRR Backup Path via : 30.1.1.2, xe20
    FRR Metric          : 35
```

```
    Protection Provided : LP NP BP Sec DP >>> Sec indicates backup path is
from Non-ecmp path

    Primary Path via    : 20.1.1.2, xe12
    FRR Backup Path via : 30.1.1.2, xe20
    FRR Metric          : 35
    Protection Provided : LP NP BP Sec DP

L1  40.1.1.0/24
    Primary Path via    : 10.1.1.2, xe16
    FRR Backup Path via : 20.1.1.2, xe12
    FRR Metric          : 30
    Protection Provided : LP NP BP

L1  50.1.1.0/24
    Primary Path via    : 20.1.1.2, xe12
    FRR Backup Path via : 10.1.1.2, xe16
    FRR Metric          : 30
    Protection Provided : LP NP BP

L1  60.1.1.0/24
    Primary Path via    : 30.1.1.2, xe20
    FRR Backup Path via : 20.1.1.2, xe12
    FRR Metric          : 30
    Protection Provided : LP NP BP DP

R1#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area ,p - stale info, E - EVPN
       * - candidate default

IP Route Table for VRF "default"
i L1    21.1.1.0/24 [115/30] via 20.1.1.2, xe12, 00:02:48
                    [FRR-NH] via 30.1.1.2, xe20

                   [115/30] via 10.1.1.2, xe16
                    [FRR-NH] via 30.1.1.2, xe20

i L1    40.1.1.0/24 [115/20] via 10.1.1.2, xe16, 00:09:43
                    [FRR-NH] via 20.1.1.2, xe12

i L1    50.1.1.0/24 [115/20] via 20.1.1.2, xe12, 00:09:03
                    [FRR-NH] via 10.1.1.2, xe16

i L1    60.1.1.0/24 [115/25] via 30.1.1.2, xe20, 00:08:35
                    [FRR-NH] via 20.1.1.2, xe12
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 7 IS-IS IPv6 Configuration

This chapter contains basic IS-IS (Intermediate System to Intermediate System) on IPv6 configuration examples.

Enable IS-ISv6 on an Interface

This example shows the minimum configuration required for enabling IS-IS on IPv6 on an interface. R1 and R2 are two routers in the ABC instance connecting to the network 1000::/64. After enabling IS-IS on an interface, create a routing instance, and specify the Network Entity Title (NET). IS-IS explicitly specifies a NET to begin routing. NET is comprised of the area address and the system ID of the router.

Note: ISISv6 session will come up even if IPv6 address is not configured, as it will use the link local address present on the interfaces.

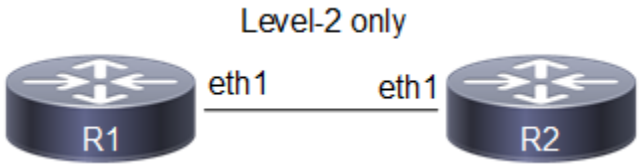


Figure 7-128: Figure 4-46: Basic IS-IS v6 Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::2/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        b86a.97c4.31c5  Up     27        L2   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        b86a.97cb.3ec5  Up     7         L2   IS-IS
R2#

R1#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
C    1000::/64 [10]
      via ::, eth1

R1#

R2#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
C    1000::/64 [10]
      via ::, eth1

R2#

R1#
R1#show ipv6 isis topology
```


© 2021 IP Infusion Inc. Proprietary

```
Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       --
0000.0000.0002       10         0000.0000.0002       eth1        b86a.97c4.31c5

R1#

R2#show ipv6 isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
0000.0000.0001       10         0000.0000.0001       eth1        b86a.97cb.3ec5
0000.0000.0002       --
```

Set Priority

This example describes how to set the priority for an interface. Set a high priority for a router to make it the Designated IS (DIS). Router R3 is configured to have a priority of 70, this is higher than the default priority (64) of R1 and R2. This makes R3 the DIS.

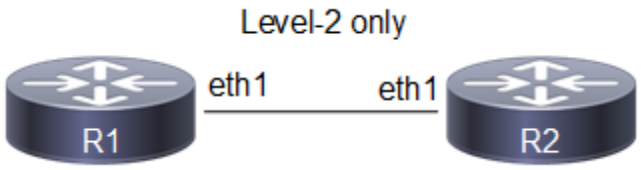


Figure 7-129: Set IS-IS Priority

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::2/64`	Configure IPv6 address on interface.
`(config-if)#isis priority 125`	Specify the router priority to a higher priority (125) to make R2 the designated IS (DIS).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        b86a.97c4.31c5      Up     8         L2   IS-IS
R1#

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        b86a.97cb.3ec5      Up     26        L2   IS-IS
R2#


R1#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0002 eth1        Up     L2   125       0000.0000.0002.01
R1#

R2#show clns is-neighbors

Tag ABC:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
```


© 2021 IP Infusion Inc. Proprietary

```
0000.0000.0001 eth1        Up     L2   64        0000.0000.0002.01
R2#


R1#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00002722
    Local SNPA: b86a.97cb.3ec5
    IP interface address:
    IPv6 interface address:
      1000::1/64
      fe80::ba6a:97ff:fecb:3ec5/64
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0002.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 0 milliseconds
R1#

R2#show isis interface
eth1 is up, line protocol is up
  Routing Protocol: IS-IS (ABC)
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00002722
    Local SNPA: b86a.97c4.31c5
    IP interface address:
    IPv6 interface address:
      1000::2/64
      fe80::ba6a:97ff:fec4:31c5/64
    Level-2 Metric: 10/10, Priority: 125, Circuit ID: 0000.0000.0002.01
    Number of active level-2 adjacencies: 1
    Level-2 LSP MTU: 1492
    Next IS-IS LAN Level-2 Hello in 1 seconds
R2#
```

Dynamic hostname

This example shows how to configure Dynamic Hostname for an ISIS IPv6 instance. Dynamic hostname is the method of mapping name-to-systemID. It allows the routing protocol to advertise symbolic names in the IS-IS PDUs. This is done by the addition of a new TLV which allows the IS-IS routers to include the name-to-systemID mapping data in their LSPs. This allows for simple and reliable transport of name mapping across IS-IS networks.

Dynamic hostname can be either the hostname of the node or the tag of the configured ISISv6 instance.

Note: Dynamic-hostname has to be configured on all nodes for it to take effect.

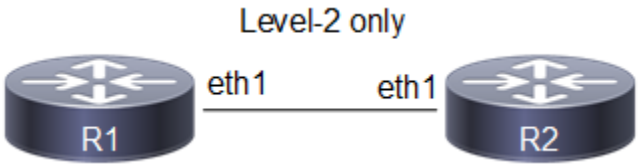


Figure 7-130: Basic dynamic hostname topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`(config-router)#end`	Exit the current mode and enter privilege mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::2/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`(config-router)#end`	Exit the current mode and enter privilege mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
```


© 2021 IP Infusion Inc. Proprietary

```
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R2             eth1        b86a.97c4.31c5  Up     20        L2   IS-IS
R1#

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1             eth1        b86a.97cb.3ec5  Up     8         L2   IS-IS
R2#



R1#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x00000008   0xFB86        1144              0/0/0
R1.01-00            * 0x00000005   0x19BD        1141              0/0/0
R2.00-00              0x00000007   0x245C        1140              0/0/0

R1#

R2#show isis database
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x00000008   0xFB86        1144              0/0/0
R1.01-00              0x00000005   0x19BD        1140              0/0/0
R2.00-00            * 0x00000007   0x245C        1140              0/0/0
R2.01-00            * 0x00000002   0xE710        0 (1132)          0/0/0

R2#



R1#show ipv6 isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   --
R2                   10         R2       eth1        b86a.97c4.31c5

R1#
```

```
R2#show ipv6 isis topology

Tag ABC:  VRF : default
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
R1                   10         R1       eth1        b86a.97cb.3ec5
R2                   --

R2#
```

Redistribute Routes into IS-IS

In this example, the configuration causes OSPFv3 routes to be imported into the IS-ISv6 routing table, and advertised into the ABC instance.



Topology

Figure 7-131: Redistribute Routes into IS-IS

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::2/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.

© 2021 IP Infusion Inc. Proprietary

(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface and assign the Area ID 0.
(config-if)#ipv6 address 2000::1/64	Configure IPv6 address on interface.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0005.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#address-family ipv6	Enter 'address-family ipv6' mode, where users can configure IPv6 routing specific configuration
(config-router-af)#redistribute ospf	Enable redistribution of routes from ospf into the ISIS routing table.
(config-router-af)#exit-address-family	Exit address family mode.
(config-router)#exit	Exit router mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 2.2.2.2	Specify a Router ID (2.2.2.2) for the OSPFv3 routing process.
(config-router)#end	Exit the current mode and enter privilege mode.

R3

#configure terminal	Enter configure mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface and assign the Area ID 0.
(config-if)#ipv6 address 2000::2/64	Configure IPv6 address on interface.
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 3.3.3.3	Specify a Router ID (3.3.3.3) for the OSPFv3 routing process.
(config-router)#end	Exit the current mode and enter privilege mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        b86a.97c4.31c5  Up     27        L2   IS-IS
R1#

R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
```

```
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        b86a.97cb.3ec5      Up     8         L2   IS-IS
R2#

R2#show ipv6 ospf neighbor

Total number of full neighbors: 1
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
3.3.3.3           1   Full/DR         00:00:34    eth2        0
R2#


R1#show ipv6 route isis
IP Route Table for VRF "default"
i L2   2000::/64 [115/10] via fe80::ba6a:97ff:fec4:31c5, eth1, 00:21:19
R1#


R1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:33:07
C      1000::/64 via ::, eth1, 01:13:36
i L2   2000::/64 [115/10] via fe80::ba6a:97ff:fec4:31c5, eth1, 00:21:29
C      fe80::/64 via ::, xe8, 00:39:44
R1#
```

Interface Metric

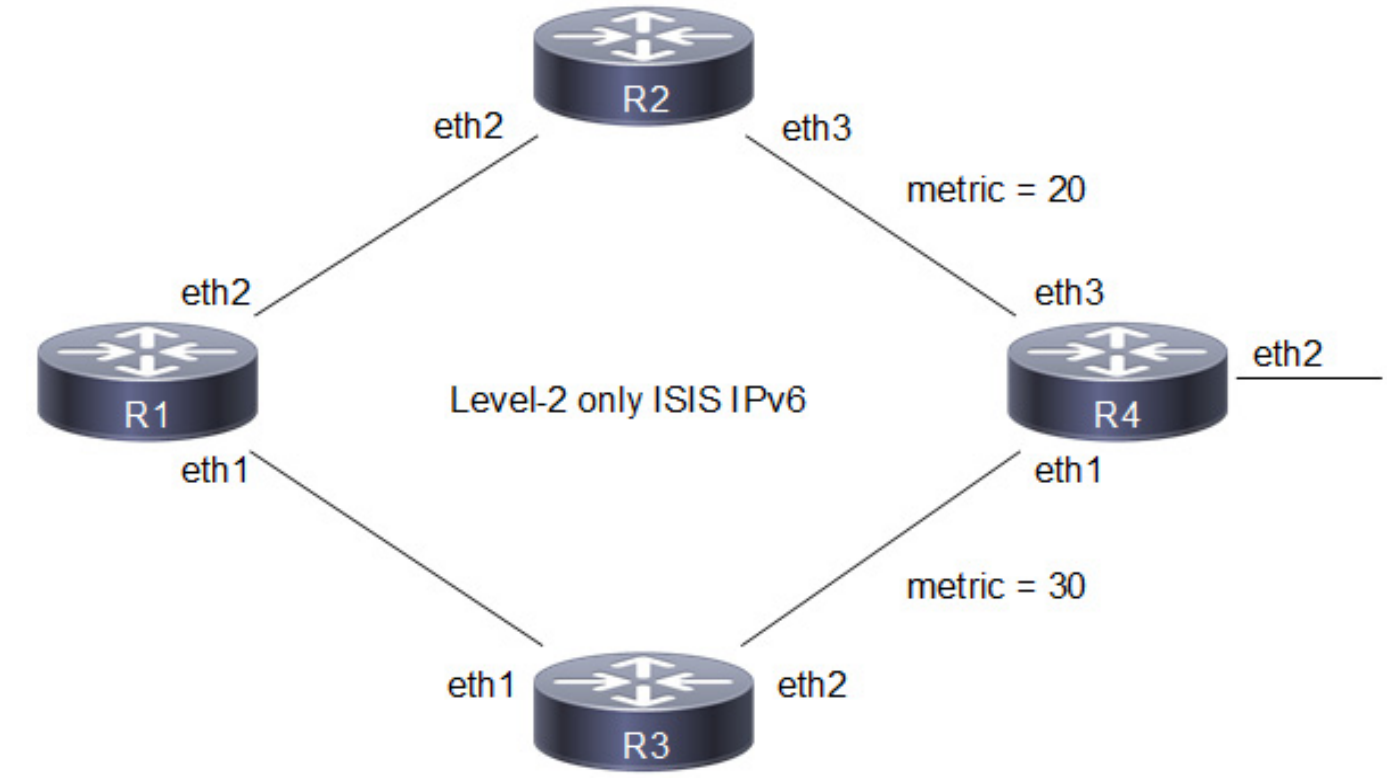
You can make a route the preferred route by changing its metric. In this example, the cost has been configured to make R3 the next hop for R1.

The default metric for each interface is 10. Interface eth2 on R2 has a metric of 20, and Interface eth2 on R3 has a metric of 30. The total cost to reach 9999::/64 (R4) through R2 and R3 is computed as follows: R2: 10+20 = 30 R3: 10+30 = 40

In this topology, R1 chooses R2 as its next hop for destination 9999::/64.

Note: Below configuration is applicable for narrow (non-wide) metric-style. Use the "metric-style wide" under isis instance and "isis wide-metric < 1-16777214>" under interface mode CLI’s to configure Wide metric.

© 2021 IP Infusion Inc. Proprietary



gy

Figure 7-132: Configure IS-IS Metric

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-IS routing on an interface for area 49(ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-IS routing on an interface for area 49(ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0100.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#end`	Exit current mode and enter privilege mode.

R2

`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).

`(config-if)#exit`	Exit interface mode.
`(config)#interface eth3`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#isis metric 20`	Set the value of IS-IS metric (on eth2) to 20.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0100.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R3

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#isis metric 30`	Set the value of IS-IS metric (on eth2) to 30.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0100.0000.0000.0003.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R4

`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 address 9999::1/64`	Configure ipv6 address in eth2
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth3`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-IS routing on an interface for area 49 (ABC).
`(config-if)#ipv6 address 2000::2/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0100.0000.0000.0004.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#address-family ipv6`	Enter ipv6 address family.
`(config-router-af)#redistribute connected`	Enable redistribution of connected routes into ISIS process
`(config-router-af)#end`	Exit current mode and enter privilege mode

© 2021 IP Infusion Inc. Proprietary

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2        b86a.97c4.31c5      Up     25        L2   IS-IS
0000.0000.0003 eth1         b86a.97c9.3cc5      Up     26        L2   IS-IS
R1#


R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0004 eth3         b86a.97c7.32c5      Up     7         L2   IS-IS
0000.0000.0001 eth2        b86a.97cb.3ec5      Up     6         L2   IS-IS
R2#

R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0004 eth2        b86a.97c7.32c5      Up     22        L2   IS-IS
0000.0000.0001 eth1         b86a.97cb.3ec5      Up     7         L2   IS-IS
R3#

R4#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 2
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth3         b86a.97c4.31c5      Up     22        L2   IS-IS
0000.0000.0003 eth1        b86a.97c9.3cc5      Up     7         L2   IS-IS
R4#

R1#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
C    1000::/64 [10]
      via ::, ce0
L2   2000::/64 [30]
      via fe80::ce37:abff:fe87:3a74, ce0
C    3000::/64 [10]
      via ::, xe14
L2   4000::/64 [40]
      via fe80::ba6a:97ff:fecf:3ad4, xe14
      via fe80::ce37:abff:fe87:3a74, ce0
L2   9999::/64 [30]
      via fe80::ce37:abff:fe87:3a74, ce0
R1#
```

Route Summarization

Route summarization makes the routing table smaller, but still allows complete IP connectivity.

The following example consists of a three-router topology, in which R2 is doing the summarization. In this example, R1 is the L1 router, R2 is the L1/L2 router doing the summarization, and R3 is the L2 router. The following configuration is given only for R2, assuming that the adjacencies with R1 and R3 are already up, and the route tables with the appropriate routes are already populated.

Topology



Figure 7-133: Route Summarization Topology

Configuration

R1

h

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000 ::1/64`	Configure IPv6 address on interface.
`(config-if)#isis circuit-type level-1`	Set the circuit type as level-1 for the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).

© 2021 IP Infusion Inc. Proprietary

(config-if)#ipv6 address 1000 ::1/64	Configure IPv6 address on interface.
(config-router)#is-type level-1	Configure instance as level-1 routing.
(config-router)#net 49.0001.0000.0000.0001.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-ISv6 routing on an interface for area 49(ABC).
(config-if)#ipv6 address 1000 ::2/64	Configure IPv6 address on interface.
(config-if)#isis circuit-type level-1	Set the circuit type as level-1 for the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-ISv6 routing on an interface for area 49(ABC).
(config-if)#ipv6 address 2000 ::1/64	Configure IPv6 address on interface.
(config-if)#isis circuit-type level-2-only	Set the circuit type as level-2-only for the interface.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#net 49.0001.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#address-family ipv6	Enter 'address-family ipv6' mode, where users can configure IPv6 routing specific configuration.
(config-router-af)#redistribute isis level-2 into level-1	Enable redistribution of isis routes from level-2 into level-1
(config-router-af)#summary-prefix 11:1:1:1::/64 level-1 metric 58	Configure the summary prefix to summarize IPv6 reachability information.
(config-router-af)#exit-address-family	Exit address family mode.
(config-router)#exit	Exit router mode.

R3

#configure terminal	Enter configure mode.
(config)#ipv6 route 11:1:1:1:1:1::/96 eth2	Configure ipv6 static route.
(config)#ipv6 route 11:1:1:1:2:1::/96 eth2	Configure ipv6 static route.
(config)#ipv6 route 11:1:1:1:3:1::/96 eth2	Configure ipv6 static route.
(config)#interface ethh2	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-ISv6 routing on an interface for area 49(ABC).
(config-if)#ipv6 address 2000 ::2/64	Configure IPv6 address on interface.
(config-if)#isis circuit-type level-2-only	Set the circuit type as level-2-only for the interface.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#net 49.0001.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

(config-router)#is-type level-2-only	Configure instance as level-2 -onlyrouting.
(config-router)#address-family ipv6	Enter 'address-family ipv6' mode, where users can configure IPv6 routing specific configuration.
(config-router-af)#redistribute static	Enable redistribution of static routes into ISIS instance.
(config-router-af)#end	Exit the current mode and enter privilege mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        b86a.97c4.31c5      Up     21        L1   IS-IS
R1#


R2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0003 eth2         b86a.97c7.32c5      Up     8         L2   IS-IS
0000.0000.0001 eth1        b86a.97cb.3ec5      Up     8         L1   IS-IS
R2#


R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth2         b86a.97c4.31c5      Up     20        L2   IS-IS
R3#



R1#show ipv6 route isis
IP Route Table for VRF "default"
i ia   11:1:1:1::/64 [115/68] via fe80::ba6a:97ff:fec4:31c5, eth1, 00:02:29
R1#

R2#show ipv6 route isis
```


© 2021 IP Infusion Inc. Proprietary

```
IP Route Table for VRF "default"
i      11:1:1:1::/64 [115/0] via ::, Null, 00:02:30
i L2   11:1:1:1:1:1::/96 [115/10] via fe80::ba6a:97ff:fec7:32c5, eth2, 00:04:54
i L2   11:1:1:1:2:1::/96 [115/10] via fe80::ba6a:97ff:fec7:32c5, eth2, 00:04:54
i L2   11:1:1:1:3:1::/96 [115/10] via fe80::ba6a:97ff:fec7:32c5, eth2, 00:04:54
R2#

R3#show ipv6 route isis
IP Route Table for VRF "default"
R3#




R1#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
ia   11:1:1:1::/64 [68]
      via fe80::ba6a:97ff:fec4:31c5, eth1

R1#


R2#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
D    11:1:1:1::/64 [0]
      via ::
L2   11:1:1:1:1:1::/96 [10]
      via fe80::ba6a:97ff:fec7:32c5, eth2
L2   11:1:1:1:2:1::/96 [10]
      via fe80::ba6a:97ff:fec7:32c5, eth2
L2   11:1:1:1:3:1::/96 [10]
      via fe80::ba6a:97ff:fec7:32c5, eth2

R2#


R3#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
```

```
E    11:1:1:1:1:1::/96 [0]
      via ::
E    11:1:1:1:2:1::/96 [0]
      via ::
E    11:1:1:1:3:1::/96 [0]
      via ::

R3#



R1#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000002   0xA557        497               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0001.01
0000.0000.0001.01-00* 0x00000001   0x1FBD        497               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00  0x00000004   0x4DA0        909               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0001.01
  Metric:   58         IPv6-Interarea 11:1:1:1::/64

R1#


R2#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000002   0xA557        496               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0001.01
0000.0000.0001.01-00  0x00000001   0x1FBD        496               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000004   0x4DA0        910               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0001.01
  Metric:   58         IPv6-Interarea 11:1:1:1::/64

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
```


© 2021 IP Infusion Inc. Proprietary

```
0000.0000.0002.00-00* 0x00000002   0xCD2A        506               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0003.01
0000.0000.0003.00-00  0x00000003   0x89E2        765               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0003.01
  Metric:   0          IPv6 11:1:1:1:1:1::/96
  Metric:   0          IPv6 11:1:1:1:2:1::/96
  Metric:   0          IPv6 11:1:1:1:3:1::/96
0000.0000.0003.01-00  0x00000001   0x2DA9        505               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00

R2#
```

Passive Interface

In ISP and large enterprise networks, many of the distribution routers have more than 200 interfaces. Before the Default Passive-Interface feature, there were two possibilities for obtaining routing information from tall of these interfaces:

- Configure a routing protocol on the backbone interfaces and redistribute connected interfaces.
- Configure the routing protocol on all interfaces and manually set most of them as passive, which was time consuming.

The solution to this problem was to configure the routing protocol on all interfaces and manually set the passive interface command on the interfaces where adjacency was not desired. In certain networks, this meant coding 200 or more passive-interface statements. With the Default Passive Interface feature, this problem is solved by allowing all interfaces to be set as passive by default using a single passive-interface default command, then configuring individual interfaces in which adjacencies are desired using the no passive-interface command.

Usage

1. When a specific interface is configured as passive using the passive-interface command:
   - The interface loses its adjacency on that interface, for example, eth1.
   - The interface (eth1) is still advertised by other IS-IS speaking interfaces to their neighbors.
2. When a specific interface is configured as passive using passive-interface command followed by removing the configuration using no passive-interface command:
   - The interface is IS-IS disabled and must be enabled using the ipv6 router isis command (for example, ipv6 router isis 1).
   - The interface (for example, eth1) is not advertised by other IS-IS speaking interfaces to their neighbors.
3. When an interface is configured with the passive interface command:
   - All interfaces lose their adjacency, except the interface with the higher index number. (For example: If eth1, eth2, eth3, and eth4 are the router interfaces, eth4 has the highest index number.)
   - All interfaces are advertised by the active IS-IS speaking interface to its neighbors.

4. When an interface is configured with the no passive interface command:
   - All interfaces are IS-IS disabled, except the interface that was active, and all interfaces must enable IS-IS on these interfaces using the ipv6 router isis command (for example, ipv6 router isis 1).
   - All interfaces are not advertised by the active IS-IS speaking interface to its neighbors.

Topology



Figure 7-134: IS-ISv6 Passive Interface

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#end`	Exit the current mode and enter privilege mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#ipv6 address 1000::2/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable OSPFv3 routing on an interface and assign the Area ID 0.
`(config-if)#ipv6 address 2000::1/64`	Configure IPv6 address on interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.

© 2021 IP Infusion Inc. Proprietary

(config-router)#net 49.0005.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#passive-interface eth1	Configure interface eth1 as a passive-interface.
(config-router)#end	Exit the current mode and enter privilege mode.

R3

#configure terminal	Enter configure mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 router isis ABC	Enable IS-ISv6 routing on an interface for area 49(ABC).
(config-if)#ipv6 address 2000::2/64	Configure IPv6 address on interface.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0005.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#end	Exit the current mode and enter privilege mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 0
Total number of adjacencies: 0
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R1#


R2#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0003 eth2         b86a.97c7.32c5   Up     7         L2   IS-IS
R2#


R3#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
```

```
0000.0000.0002 eth2         b86a.97c4.31c5      Up     24        L2   IS-IS
R3#


R1#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
C    1000::/64 [10]
      via ::, eth1

R1#


R2#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
C    1000::/64 [0]
      via ::, eth1
C    2000::/64 [10]
      via ::, eth2

R2#

R3#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
L2   1000::/64 [10]
      via fe80::ba6a:97ff:fec4:31c5, eth2
C    2000::/64 [10]
      via ::, eth2

R3#


R1#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x0000000E   0x0E19        931               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
```

 © 2021 IP Infusion Inc. Proprietary

```
  IPv6 Address: 1000::1
  Metric:   10         IPv6 1000::/64
0000.0000.0001.01-00* 0x00000009   0xE110        0 (931)           0/0/0
0000.0000.0002.00-00  0x00000011   0xABC7        440               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 1000::2
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IPv6 1000::/64
  Metric:   10         IPv6 2000::/64
0000.0000.0003.00-00  0x00000002   0x9ED3        439               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 2000::2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IPv6 2000::/64
0000.0000.0003.01-00  0x00000001   0x2DA9        436               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00

R1#
R1#

R2#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x0000000D   0x2666        879               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 1000::1
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IPv6 1000::/64
0000.0000.0001.01-00  0x00000009   0x11C1        821               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000012   0x669F        906               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 2000::1
  Metric:   10         IS 0000.0000.0003.01
  Metric:   0          IPv6 1000::/64
  Metric:   10         IPv6 2000::/64
0000.0000.0003.00-00  0x00000002   0x9ED3        439               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 2000::2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IPv6 2000::/64
```

```
0000.0000.0003.01-00  0x00000001   0x2DA9        436               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00

R2#

R3#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x0000000D   0x2666        879               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 1000::1
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IPv6 1000::/64
0000.0000.0001.01-00  0x00000009   0x11C1        821               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00  0x00000012   0x669F        905               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 2000::1
  Metric:   10         IS 0000.0000.0003.01
  Metric:   0          IPv6 1000::/64
  Metric:   10         IPv6 2000::/64
0000.0000.0003.00-00* 0x00000002   0x9ED3        440               0/0/0
  Area Address: 49.0005
  NLPID:        0x8E
  IPv6 Address: 2000::2
  Metric:   10         IS 0000.0000.0003.01
  Metric:   10         IPv6 2000::/64
0000.0000.0003.01-00* 0x00000001   0x2DA9        437               0/0/0
  Metric:   0          IS 0000.0000.0003.00
  Metric:   0          IS 0000.0000.0002.00

R3#
```

Enable BFD over IS-ISv6

This example shows how to configure Bidirectional Forwarding Detection with ISISv6 instance

Topology

© 2021 IP Infusion Inc. Proprietary

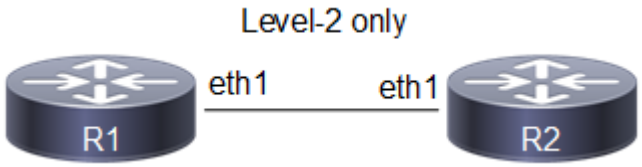


Figure 7-135: Basic BFD over IS-ISv6 Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#bfd all-interfaces`	Enable the Bidirectional Forwarding Detection (BFD) feature on the interfaces enabled with this ISIS instance.
`(config-router)#end`	Exit current mode and enter privilege mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0005.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#bfd all-interfaces`	Enable the Bidirectional Forwarding Detection (BFD) feature on the interfaces enabled with this ISIS instance.
`(config-router)#end`	Exit current mode and enter privilege mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
```

```
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        b86a.97c4.31c5  Up     24        L2   IS-IS
R1#

R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
------------------------------------------------------------------------------
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
256      256        IPv6       Single-Hop  Up        00:04:26  eth1         NA
fe80::ba6a:97ff:fec4:31c5/128
Number of Sessions:    1
R1#
R1#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
------------------------------------------------------------------------------

Session Interface Index : 10018          Interface name :eth1
Session Index : 256
Lower Layer : IPv6                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 256                Local Address : fe80::ba6a:97ff:fecb:3ec5/128
Remote Discriminator : 256               Remote Address : fe80::ba6a:97ff:fec4:31c5/128
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250              Min Rx: 250              Multiplier: 3
Neg Tx: 250              Neg Rx: 250              Neg detect mult: 3
Min echo Tx: 1000        Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : n/a                             Pkt Out : n/a
Pkts Drop : 00000000000000000000         Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000          IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000001231       IPv6 Pkt Out : 00000000000000001233
UP Count : 1                             UPTIME : 00:04:30

Protocol Client Info:
ISIS-> Client ID: 6      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```


© 2021 IP Infusion Inc. Proprietary

```
R1#
```

Originate Default Route to ISISv6 Neighbors

This example shows how to originate default route present to ISISv6 neighbors.

Note: To get a default route in ISIS, we must have it (said default route) in the routing table first.To get a default route in ISIS, we should have it (said default route) in the routing table first otherwise we can use the CLI "default information originate always" which advertises default route.

Topology

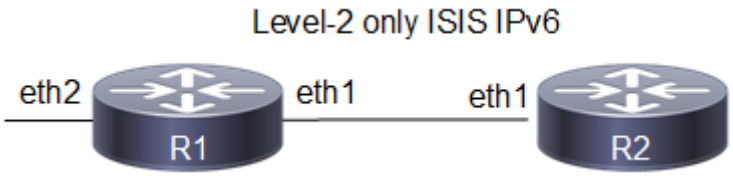


Figure 7-136: Basic IS-ISv6 Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#ipv6 route ::/0 2345::2`	Configure default route.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 address 2345::1/64`	Configure IPv6 address on interface.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (ABC).
`(config-router)#is-type level-2-only`	Configure instance as level-2-only routing.
`(config-router)#net 49.0001.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#address-family ipv6`	Enter ipv6 address family.
`(config-router-af)#default-information originate`	Originate reachability information to Default destination into LSP.
`(config-router-af)#end`	Exit all modes and enter privilege mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 router isis ABC`	Enable IS-ISv6 routing on an interface for area 49(ABC).

(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0005.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#end	Exit current mode and enter privilege mode

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag ABC:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 eth1        b86a.97cb.3ec5      Up     6         L2   IS-IS
R2#

R2#show ipv6 route isis
IP Route Table for VRF "default"
i L2   ::/0 [115/10] via fe80::ba6a:97ff:fecb:3ec5, eth1, 00:09:12
R2#

R2#show ipv6 isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag ABC:  VRF : default
L2   ::/0 [10]
      via fe80::ba6a:97ff:fecb:3ec5, eth1

R2#
R2#show isis database verbose
Tag ABC:  VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000006   0x5FA4        1033              0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
  Metric:   10         IS 0000.0000.0001.01
  Metric:   0          IPv6 ::/0
0000.0000.0001.01-00  0x00000001   0x21B9        628               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS R2.00
R2.00-00            * 0x00000002   0xFBED        633               0/0/0
  Area Address: 49.0001
  NLPID:        0x8E
```


© 2021 IP Infusion Inc. Proprietary

```
Hostname:     R2
Metric:   10          IS 0000.0000.0001.01
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 8 IS-IS Graceful Restart Configuration

The Intermediate System to Intermediate System (IS-IS) routing protocol is a link state intra-domain routing protocol. Normally, when an IS-IS router is restarted, temporary disruption of routing occurs due to events in both the restarting router and the neighbors of the restarting router.

ISIS provides graceful restart, in which the adjacency and routes are maintained in the routing table for the grace period. In this way, the data flow is not affected, and there is no packet loss during the restart phase.

With ISIS GR, the ISIS router should be able to restart gracefully with non-stop forwarding during the recovery. And the Helper ISIS router should be able to help restarting router by maintaining the adjacency.

ISIS Grace Restart Functionality applies to:

- ISIS broadcast network
- ISIS point-to-point network
- IPv4 domain
- IPv6 domain

Topology

In this example, R1 is the L1/L2 router, and R2 is the L1/L2 restart-helper router.

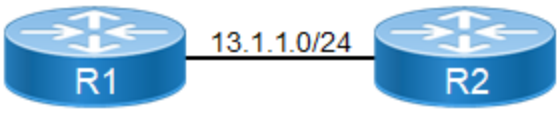


Figure 8-137: IS-IS Graceful Restart

Configuration

The following configuration is given only for R2, assuming that the adjacency with R1 is already up and the route tables with the appropriate routes are already populated.

R2

`#configure terminal`	Enter configure mode.
`(config)#isis restart helper`	Configure this router as a restart helper.
`(config)#isis restart grace-period 100`	Set the grace period to 100 seconds. The restarting router should come up before 100 seconds, otherwise, the adjacency and routes will be deleted.

Note: The IS-IS daemon in the restarting router must be manually restarted using `restart isis graceful` command: it does not restart automatically.

Note: The scope of unplanned GR is that if the ISIS daemon crashes or gets killed with SIGSEGV signal then the routes will be stale marked until the hold time (30 seconds), assuming that ISIS will be restarted within the hold time. Neighbor adjacency cannot be maintained in unplanned GR.

Validation

```
R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     13.1.1.0/24 is directly connected, eth1, 04:08:20
i ia  20.0.0.0/6 [115/11] via 13.1.1.2, eth1, 00:10:44
i L1  33.0.0.0/24 [115/20] via 13.1.1.2, eth1, 00:10:44
C     127.0.0.0/8 is directly connected, lo, 04:10:59
C     192.168.52.0/24 is directly connected, eth0, 04:10:55


R2#show clns neighbors

Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 eth1        5254.0099.1e21      Up     20        L1   IS-IS


R2#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
C    *>  13.1.1.0/24 is directly connected, eth1, 04:10:56
i L1     13.1.1.0/24 [115/10] is directly connected, eth1, 01:58:50
i ia *>  20.0.0.0/6 [115/11] via 13.1.1.2, eth1, 00:13:20
i L1 *>  33.0.0.0/24 [115/20] via 13.1.1.2, eth1, 00:13:20
C    *>  127.0.0.0/8 is directly connected, lo, 04:13:35
C    *>  192.168.52.0/24 is directly connected, eth0, 04:13:31

Gateway of last resort is not set
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 9 BGP

This chapter contains basic Border Gateway Protocol configuration examples.

Enable BGP Routers in the Same Autonomous System

Figure 9-138 shows the minimum configuration required to enable BGP on an interface. R1 and R2 are two routers belonging to the same AS, AS200, connecting to network 10.10.10.0/24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

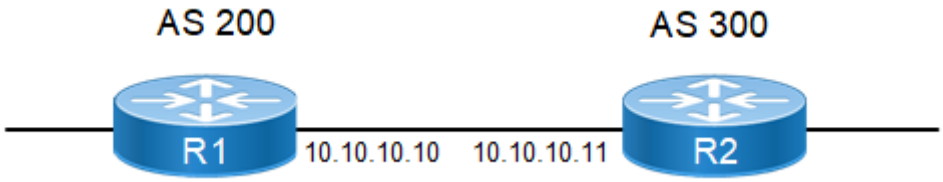


Figure 9-138: Routers in the Same Autonomous System

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R1.
`(config-router)#neighbor 10.10.10.11 remote-as 200`	Define BGP neighbors, and establish a TCP session. `10.10.10.11` is the IP address of the neighbor (R2), and `200` is the neighbor's AS number.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.10.10.11 activate`	Activate the neighbor in the Ipv4 address family.
`(config-router-af)# exit-address-family`	Exit address-family mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of `R2`.
`(config-router)#neighbor 10.10.10.10 remote-as 200`	Define BGP neighbors, and establish a TCP session. `10.10.10.10` is the IP address of the neighbor (`R1`), and `200` is the neighbor's AS number.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode

`#configure terminal`	Enter configure mode.
`(config-router-af)# neighbor 10.10.10.10 activate`	Activate the neighbor in the Ipv4 address family.
`(config-router-af)# exit-address-family`	Exit address-family mode.

Validation

```
#show ip bgp summary
BGP router identifier 192.168.52.2, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.10.10.11              4   200  387        390       1      0      0
00:00:04               0

Total number of neighbors 1

Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 10.10.10.11, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  BGP state = Established, up for 00:01:41
  Last read 00:00:11, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 5 messages, 0 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.10, Local port: 179
Foreign host: 10.10.10.11, Foreign port: 33931
Nexthop: 10.10.10.10
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

Enable BGP Between Different Autonomous Systems

This example shows the minimum configuration required for enabling BGP on an interface, when the routers belong to different autonomous systems. R1 and R2 are two routers in different autonomous system, AS200 and AS300, connecting to network 10.10.10.0/24.

© 2021 IP Infusion Inc. Proprietary

Topology

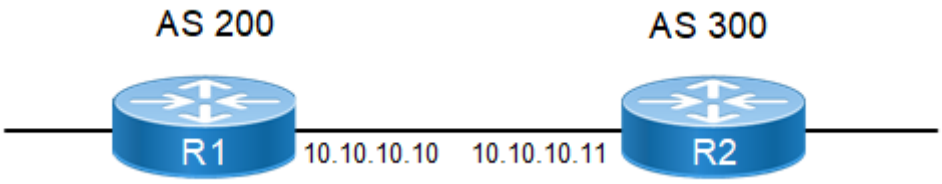


Figure 9-139: Routers in Different Autonomous Systems

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R1.
`(config-router)#neighbor 10.10.10.11 remote-as 300`	Define BGP neighbors, and establish a TCP session. `10.10.10.11` is the IP address of the neighbor (R2), and `300` is the neighbor's AS number.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.10.10.11 activate`	Activate the neighbor in the Ipv4 address family.
`(config-router-af)# exit-address-family`	Exit address-family mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 300`	Define the routing process. The number `300` specifies the AS number of `R2`.
`(config-router)#neighbor 10.10.10.10 remote-as 200`	Define BGP neighbors, and establish a TCP session. `10.10.10.10` is the IP address of the neighbor (R1), and `200` is the neighbor's AS number.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.10.10.10 activate`	Activate the neighbor in the Ipv4 address family.
`(config-router-af)# exit-address-family`	Exit address-family mode.

Validation

```
#show ip bgp neighbors
BGP neighbor is 10.10.10.10, remote AS 200, local AS 300, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  BGP state = Established, up for 00:00:15
  Last read 00:00:15, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 2 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
```

© 2021 IP Infusion Inc. Proprietary

```
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.11, Local port: 56091
Foreign host: 10.10.10.10, Foreign port: 179
Nexthop: 10.10.10.11
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip bgp summary
BGP router identifier 192.168.52.3, local AS number 300
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
Down    State/PfxRcd
10.10.10.10              4    200     3          3       1       0       0
00:00:50              0

Total number of neighbors 1

Total number of Established sessions 1
```

Route-Map

Use route maps to filter incoming updates from a BGP peer. In this example, the prefix-list `ABC` on R1 is configured to deny entry of any routes with the IP address 1.1.1.0/M (M = 26, 27, 28). To test the filter, R2 is configured to generate network addresses 1.1.1.0/27 and 1.1.2.0/24. To verify, use the `show ip bgp` command on R1; it displays R1 receiving updates from only 1.1.2.0/24.

Topology

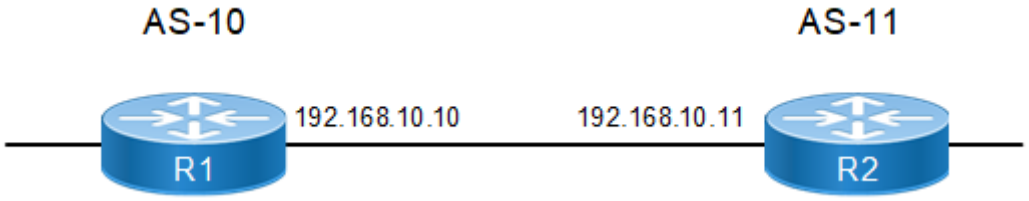


Figure 9-140: Configure Route-Map

© 2021 IP Infusion Inc. Proprietary

R1

`#configure terminal`	Enter configure mode.
`(config)#ip prefix-list ABC`	Create an entry in the prefix-list. The ABC parameter is the name of the map that is created above. 5 specifies the sequence number or position of this specific route map. deny specifies the packets are to be rejected. 26 and 28 are the minimum and maximum prefix lengths to be matched.
`(config-ip-prefix-list)#seq 5 deny 1.1.1.0/24 ge 26 le 28`	5 specifies the sequence number or position of this specific route map. deny specifies the packets are to be rejected. 26 and 28 are the minimum and maximum prefix lengths to be matched.
`(config-ip-prefix-list)#seq 10 permit any`	10 specifies the sequence number or position of this specific route map. The permit parameter any specifies accept all packets of any length.
`(config-ip-prefix-list)#exit`	Exit the prefix-list mode
`(config)#route-map ABC permit 1`	Enter Route-map mode to set the match operation.
`(config-route-map)#match ip address prefix-list ABC`	Set the match criteria. In this case, if the route-map name matches ABC, the packets from the first sequence are denied.
`(config-route-map)#exit`	Exit Route-map mode, and return to Configure mode.
`(config)#router bgp 10`	Define the routing process, and establish a TCP session. The number 10 specifies the AS number of R1.
`(config-router)#neighbor 192.168.10.11 remote-as 11`	Define BGP neighbors, and establish a TCP session. 192.168.10.11 is the IP address of the neighbor (R2), and 11 is the neighbor's AS number.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 192.168.10.11 activate`	Activate the neighbor in the Ipv4 address family.
`(config-router-af)#neighbor 192.168.10.11 route-map ABC in`	Apply a route map to routes. 192.168.10.11 specifies the IP address of BGP neighbor. The ABC parameter is the name of the route map, and in specifies that the access list applies to incoming advertisements.
`(config-router-af)#exit-address-family`	Exit address-family mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 1.1.1.1/27 secondary`	Specify the interface address.
`(config-if)#ip address 1.1.2.1/24 secondary`	Specify the interface address.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 11`	Define the routing process, and establish a TCP session. The number `11` specifies the AS number of R2.
`(config-router)#neighbor 192.168.10.10 remote-as 10`	Define BGP neighbors, and establish a TCP session. `192.168.10.10` is the IP address of the neighbor (R1), and `10` is the neighbor's AS number.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode

`(config-router-af)# neighbor 192.168.10.10 activate`	Activate the neighbor in the Ipv4 address family.
`(config-router-af)#network 1.1.1.0/27`	Specify the network to be advertised by the BGP routing process.
`(config-router-af)#network 1.1.2.0/24`	Specify the network to be advertised by the BGP routing process.
`(config-router-af)#exit-address-family`	Exit router mode.

Validation

```
#show  ip bgp
BGP table version is 2, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   1.1.2.0/24       192.168.10.11         0         100            0       11
i

Total number of prefixes 1
```

Route Reflector

The configurations in this section apply to BGP Route Reflectors (RR).

Reduce the iBGP Mesh Inside an Autonomous System

Use Route Reflectors to reduce the iBGP mesh inside an Autonomous System (AS).

Topology

In this example, R2, R5, and R4 would have to maintain a full mesh among themselves, but by making R5 the Route Reflector, R2 (Client1) has an iBGP session with the RR only, but not with R4 (Client 2). The routes learned from R2 are advertised to the other clients, and to iBGP peers outside the cluster; the iBGP routes learned from iBGP peers outside the cluster are advertised to R2. This reduces the iBGP peer connections in AS1.

© 2021 IP Infusion Inc. Proprietary

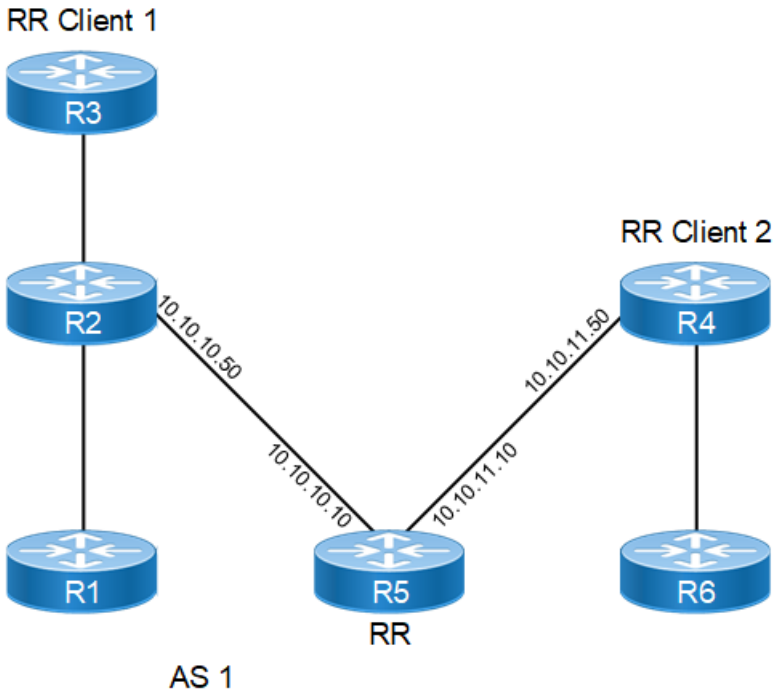


Figure 9-141: BGP Route Reflector

RR (R5)

`#configure terminal`	Enter configure mode.
`(config)#router bgp 1`	Define the routing process. The number 1 identifies the AS number of R5.
`(config-router)#neighbor 10.10.10.50 remote-as 1`	Define the BGP neighbor, and establish a TCP session. 10.10.10.50 is the IP address of one of the neighbors (R2), and 1 is the neighbor's AS number.
`(config-router)#neighbor 10.10.11.50 remote-as 1`	Define the BGP neighbor, and establish a TCP session. 10.10.11.50 is the IP address of one of the neighbors (R4), and 1 is the neighbor's AS number.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.10.10.50 activate`	Activate the neighbor in the Ipv4 address family.
`(config-router-af)#neighbor 10.10.11.50 activate`	Activate the neighbor in the Ipv4 address family.
`(config-router-af)#neighbor 10.10.10.50 route-reflector-client`	Configure R5 as the Route-Reflector (RR) and neighbor R2 as its client.
`(config-router-af)#neighbor 10.10.11.50 route-reflector-client`	Configure R5 as the Route-Reflector (RR) and neighbor R4 as its client.
`(config-router-af)#exit-address-family`	Exit address-family mode.

© 2021 IP Infusion Inc. Proprietary

RR Client 1 (R2)

`(config)#router bgp 1`	Define the routing process. The number `1` specifies the AS number of R2.
`(config-router)#neighbor 10.10.10.10 remote-as 1`	Define the BGP neighbor, and establish a TCP session. `10.10.10.10` is the IP address of the neighbor (R5), and `1` is the neighbor's AS number.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.10.10.10 activate`	Activate the neighbor in the Ipv4 address family.
`(config-router-af)#exit-address-family`	Exit address-family mode.
`(config-router)#exit`	Exit router mode.

RR Client 2 (R4)

`(config)#router bgp 1`	Define the routing process. The number `1` identifies the AS number of `R4`.
`(config-router)#neighbor 10.10.11.10 remote-as 1`	Define BGP neighbor, and establish a TCP session. `10.10.11.10` is the IP address of the neighbor (R5), and `1` is the neighbor's AS number.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.10.11.10 activate`	Activate the neighbor in the Ipv4 address family.
`(config-router-af)#exit-address-family`	Exit address-family mode.
`(config-router)#exit`	Exit router mode.

Validation

R5

```
#show ip bgp neighbors
BGP neighbor is 10.10.10.50, remote AS 1, local AS 1, internal link
  BGP version 4, local router ID 192.160.50.3, remote router ID 10.12.4.152
  BGP state = Established, up for 00:01:04
  Last read 00:01:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
```


© 2021 IP Infusion Inc. Proprietary

```
Local host: 10.10.10.10, Local port: 47983
Foreign host: 10.10.10.50, Foreign port: 179
Nexthop: 10.10.10.10
Nexthop global: fe80::a00:27ff:fe09:fd25
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 10.10.11.50, remote AS 1, local AS 1, internal link
  BGP version 4, remote router ID 10.12.4.197
  local router ID 192.160.50.3
  BGP state = Established, up for 00:01:04
  Last read 00:01:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.11.10, Local port: 39851
Foreign host: 10.10.11.50, Foreign port: 179
Nexthop: 10.10.11.10
Nexthop global: fe80::a00:27ff:fe52:45f6
Nexthop local: ::
BGP connection: non shared network
```

R3

```
#show ip bgp neighbors
BGP neighbor is 10.10.11.10, remote AS 1, local AS 1, internal link
  BGP version 4, local router ID 192.160.50.4, remote router ID 10.12.4.185
  BGP state = Established, up for 00:00:56
  Last read 00:00:56, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
  Sent 3 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
```

```
Local host: 10.10.11.50, Local port: 179
Foreign host: 10.10.11.10, Foreign port: 39851
Nexthop: 10.10.11.50
Nexthop global: fe80::a00:27ff:fe42:fb7a
Nexthop local: ::
BGP connection: non shared network
```

R2

```
#show ip bgp neighbors
BGP neighbor is 10.10.10.10, remote AS 1, local AS 1, internal link
  BGP version 4, local router ID 192.160.50.2, remote router ID 10.12.4.185
  BGP state = Established, up for 00:01:23
  Last read 00:01:23, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.50, Local port: 179
Foreign host: 10.10.10.10, Foreign port: 47983
Nexthop: 10.10.10.50
Nexthop global: fe80::a00:27ff:fe9c:f35d
Nexthop local: ::
BGP connection: non shared network
```

Multiple Route Reflectors

The basic rule of BGP is that a BGP speaker cannot advertise a route to an iBGP neighbor if that route was learned from another iBGP neighbor. Configuring a route reflector provides a means to circumvent this rule. The entire route reflector process is transparent to the clients, and no configuration is necessary on these clients.

Whenever an iBGP-speaking router receives a route update, it forwards the route to the neighbor without changing the nexthop IP address, thus making it an unreachable route, unless verified by an iGP (for example, neighbor x.x.x.x route-reflector-client).

- A route learned from a non-RR client is advertised to RR clients but not to non-RR clients.
- A route learned from a RR client is advertised to both RR clients and non-RR clients. Even the RR client that advertised the route will receive a copy and discards it because it sees itself as the originator.
- A route learned from an EBGP neighbor is advertised to both RR clients and non-RR clients.

© 2021 IP Infusion Inc. Proprietary

Topology

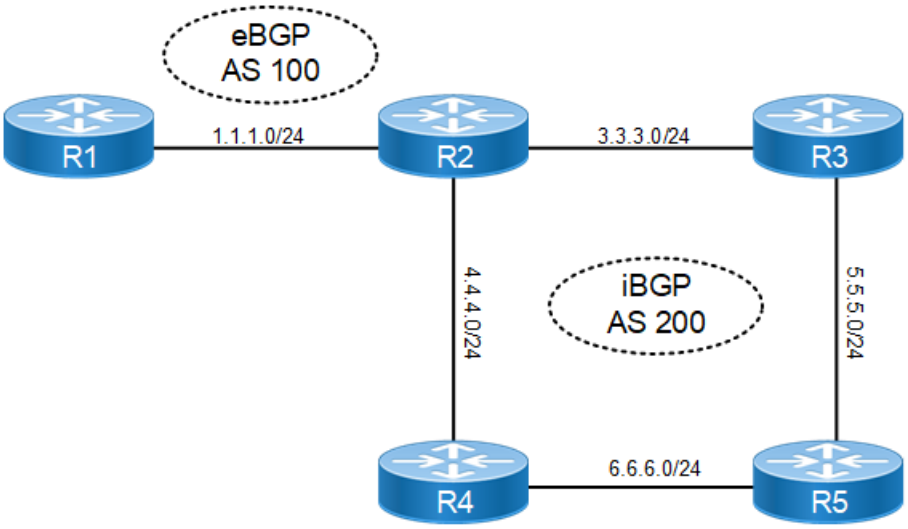


Figure 9-142: eBGP and iBGP Route Reflector Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip addr 1.1.1.1/24`	Specify IP address for the interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 100.100.100.100/32 secondary`	Specify IP address for the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 100`	Define the routing process with AS number `100`.
`(config-router)#neighbor 1.1.1.2 remote-as 200`	Define the eBGP neighbor (R2).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 1.1.1.2 activate`	Activate the neighbor under address family mode
`(config-router-af)#network 100.100.100.100/32`	Advertise a route via eBGP connection to R2.
`(config-router-af)#exit-address-family`	Exit router mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 1.1.1.2/24`	Specify IP address for the interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 3.3.3.2/24`	Specify IP address for the interface.

(config-if)#exit	Exit interface mode
(config)#interface eth3	Enter interface mode
(config-if)#ip address 4.4.4.2/24	Specify IP address for the interface.
(config-if)#exit	Exit interface mode
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 1.1.1.1 remote-as 100	Define the eBGP neighbor (R1).
(config-router)#neighbor 4.4.4.1 remote-as 200	Define the iBGP neighbor (R4).
(config-router)#neighbor 3.3.3.1 remote-as 200	Define the iBGP neighbor (R3).
(config-router)#bgp cluster-id 4	Define a cluster ID (4) when multiple Route Reflectors exist.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 1.1.1.1 activate	Activate the neighbor under address family mode
(config-router-af)# neighbor 4.4.4.1 activate	Activate the neighbor under address family mode
(config-router-af)# neighbor 3.3.3.1 activate	Activate the neighbor under address family mode
(config-router-af)#neighbor 3.3.3.1 route-reflector-client	Configure R2 as the Route-Reflector and neighbor R3 as its client.
(config-router-af)#neighbor 4.4.4.1 route-reflector-client	Configure R2 as the Route-Reflector and neighbor R4 as its client.
(config-router-af)#exit-address-family	Exit address-family mode.

R3

#configure terminal	Enter configure mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 3.3.3.1/24	Assign an IP address
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip addr 5.5.5.1/24	Assign an IP address
(config-if)#exit	Exit interface mode
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 3.3.3.2 remote-as 200	Define the iBGP neighbor (R2).
(config-router)#neighbor 5.5.5.2 remote-as 200	Define the iBGP neighbor (R5).
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 3.3.3.2 activate	Activate the neighbor under address family mode
(config-router-af)# neighbor 5.5.5.2 activate	Activate the neighbor under address family mode

© 2021 IP Infusion Inc. Proprietary

(config-router-af)#neighbor 5.5.5.2 route-reflector-client	Configure R3 as the Route-Reflector and neighbor R5 as its client.
(config-router-af)#exit-address-family	Exit address-family mode.

R4

#configure terminal	Enter configure mode
(config)#interface eth2	Enter interface mode
(config-if)#ip address 6.6.6.1/24	Specify an IP address for the interface.
(config-if)#exit	Exit interface mode
(config)#interface eth4	Enter interface mode
(config-if)#ip address 4.4.4.1/24	Specify an IP address for the interface.
(config-if)#exit	Exit interface mode
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 4.4.4.2 remote-as 200	Define the iBGP neighbor (R2).
(config-router)#neighbor 6.6.6.2 remote-as 200	Define the iBGP neighbor (R5).
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 4.4.4.2 activate	Activate the neighbor under address family mode
(config-router-af)# neighbor 6.6.6.2 activate	Activate the neighbor under address family mode
(config-router-af)#exit-address-family	Exit address-family mode.
(config-router)#exit	Exit router mode.

R5

#configure terminal	Enter configure mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 5.5.5.2/24	Specify an IP address for the interface.
(config-if)#exit	Exit interface mode
(config-if)#interface eth2	Enter interface mode
(config-if)#ip address 6.6.6.2/24	Specify an IP address for the interface.
(config-if)#exit	Exit interface mode
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 5.5.5.1 remote-as 200	Define the iBGP neighbor (R3).
(config-router)#neighbor 6.6.6.1 remote-as 200	Define the iBGP neighbor (R4).
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 5.5.5.1 activate	Activate the neighbor under address family mode
(config-router-af)# neighbor 6.6.6.1 activate	Activate the neighbor under address family mode
(config-router-af)#exit-address-family	Exit address-family mode.

Validation

R2

```
#show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 200, external link
  BGP version 4, local router ID 10.12.4.196, remote router ID 192.160.50.2
  BGP state = Established, up for 00:14:41
  Last read 00:00:11, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 32 messages, 0 notifications, 0 in queue
  Sent 31 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.2, Local port: 50649
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 1.1.1.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 3.3.3.1, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.3, remote router ID 192.160.50.4
  BGP state = Established, up for 00:04:17
  Last read 00:00:17, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 10 messages, 0 notifications, 0 in queue
  Sent 13 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 3, Offset 0, Mask 0x8
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 3.3.3.2, Local port: 179
Foreign host: 3.3.3.1, Foreign port: 32973
Nexthop: 3.3.3.2
Nexthop global: ::
Nexthop local: ::
```


© 2021 IP Infusion Inc. Proprietary

```
BGP connection: non shared network

BGP neighbor is 4.4.4.1, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.3, remote router ID 192.160.50.6
  BGP state = Established, up for 00:00:16
  Last read 00:00:16, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 4.4.4.2, Local port: 179
Foreign host: 4.4.4.1, Foreign port: 60398
Nexthop: 4.4.4.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     1.1.1.0/24 is directly connected, eth1, 00:16:10
C     3.3.3.0/24 is directly connected, eth2, 00:15:59
C     4.4.4.0/24 is directly connected, eth3, 00:15:49
B     100.100.100.100/32 [20/0] via 1.1.1.1, eth1, 00:14:53
C     127.0.0.0/8 is directly connected, lo, 00:32:26
C     192.160.50.0/24 is directly connected, eth0, 00:32:22

Gateway of last resort is not set


#show ip bgp
BGP table version is 2, local router ID is 192.160.50.3
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop            Metric    LocPrf       Weight Path
*>   100.100.100.100/32
                      1.1.1.1               0         100            0       100
i

Total number of prefixes 1
Total number of neighbors 3
```

R1

```
#show bgp neighbors
BGP neighbor is 1.1.1.2, remote AS 200, local AS 100, external link
  BGP version 4, local router ID 10.12.4.142, remote router ID 10.12.4.196
  BGP state = Established, up for 00:16:11
  Last read 00:00:11, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 34 messages, 0 notifications, 0 in queue
  Sent 36 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.1, Local port: 179
Foreign host: 1.1.1.2, Foreign port: 50649
Nexthop: 1.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network


#show ip bgp summary
BGP router identifier 192.160.50.2, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
1.1.1.2                  4   200   34         36       1      0      0
00:16:18              0

Total number of neighbors 1

Total number of Established sessions 1
#
```

R3

```
#show ip bgp
BGP table version is 1, local router ID is 192.160.50.4
```


© 2021 IP Infusion Inc. Proprietary

```
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
* i  100.100.100.100/32
                      1.1.1.1              0         100            0       100
i

Total number of prefixes 1
#

#show ip bgp neighbors
BGP neighbor is 3.3.3.2, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.4, remote router ID 192.160.50.3
  BGP state = Established, up for 00:06:15
  Last read 00:00:15, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 15 messages, 0 notifications, 0 in queue
  Sent 14 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 3.3.3.1, Local port: 32973
Foreign host: 3.3.3.2, Foreign port: 179
Nexthop: 3.3.3.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 5.5.5.2, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.4, remote router ID 192.160.50.5
  BGP state = Established, up for 00:03:35
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 9 messages, 0 notifications, 0 in queue
  Sent 10 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
```

```
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 5.5.5.1, Local port: 179
Foreign host: 5.5.5.2, Foreign port: 39271
Nexthop: 5.5.5.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#

#show ip bgp summary
BGP router identifier 192.160.50.4, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
3.3.3.2                  4   200   15         14       1      0      0
00:06:26               1
5.5.5.2                  4   200    9         10       1      0      0
00:03:46               0

Total number of neighbors 2
```

R4

```
#show ip bgp
BGP table version is 1, local router ID is 192.160.50.6
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
* i  100.100.100.100/32
                      1.1.1.1              0         100           0       100
i

Total number of prefixes 1
#

#sh ip bgp neighbors
BGP neighbor is 4.4.4.2, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.6, remote router ID 192.160.50.3
  BGP state = Established, up for 00:03:58
  Last read 00:00:28, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 10 messages, 0 notifications, 0 in queue
  Sent 9 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
```


© 2021 IP Infusion Inc. Proprietary

```
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 4.4.4.1, Local port: 60398
Foreign host: 4.4.4.2, Foreign port: 179
Nexthop: 4.4.4.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 6.6.6.2, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.6, remote router ID 192.160.50.5
  BGP state = Established, up for 00:03:52
  Last read 00:00:22, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 9 messages, 0 notifications, 0 in queue
  Sent 9 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 6.6.6.1, Local port: 48257
Foreign host: 6.6.6.2, Foreign port: 179
Nexthop: 6.6.6.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#


#show ip bgp summary
BGP router identifier 192.160.50.6, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
4.4.4.2                  4   200   11         10       1      0      0
00:04:09               1
6.6.6.2                  4   200   10         10       1      0      0
00:04:03               0

Total number of neighbors 2
```

```
Total number of Established sessions 2
```

R5

```
#show ip bgp neighbors
BGP neighbor is 5.5.5.1, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.5, remote router ID 192.160.50.4
  BGP state = Established, up for 00:09:04
  Last read 00:00:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 20 messages, 0 notifications, 0 in queue
  Sent 20 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 5.5.5.2, Local port: 39271
Foreign host: 5.5.5.1, Foreign port: 179
Nexthop: 5.5.5.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 6.6.6.1, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.160.50.5, remote router ID 192.160.50.6
  BGP state = Established, up for 00:07:36
  Last read 00:00:06, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 17 messages, 0 notifications, 0 in queue
  Sent 18 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 6.6.6.2, Local port: 179
Foreign host: 6.6.6.1, Foreign port: 48257
Nexthop: 6.6.6.2
Nexthop global: ::
Nexthop local: ::
```

 © 2021 IP Infusion Inc. Proprietary

```
BGP connection: non shared network
#

#sh ip bgp summary
BGP router identifier 192.160.50.5, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                  V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
Down    State/PfxRcd
5.5.5.1                   4    200    20          20        1       0       0
00:09:20                0
6.6.6.1                   4    200    17          18        1       0       0
00:07:52                0

Total number of neighbors 2

Total number of Established sessions 2
#
```

BGP Confederations

In BGP, nodes running iBGP protocols must be interconnected forming a full mesh. Confederation solves the iBGP full-mesh network complexity and inefficiency by splitting a large autonomous system domain into smaller autonomous system domains, called member autonomous systems. Member autonomous systems can form eBGP connections among themselves, to prevent full-mesh connections among each iBGP-running node.

The `bgp confederation identifier` command tells the router that it is a member of a confederation and the confederation ID. The `bgp confederation peers` command lists the member AS to which the router is connected.

In the following example, R1, R2, and R3 are members of the same confederation with different AS numbers.

Topology

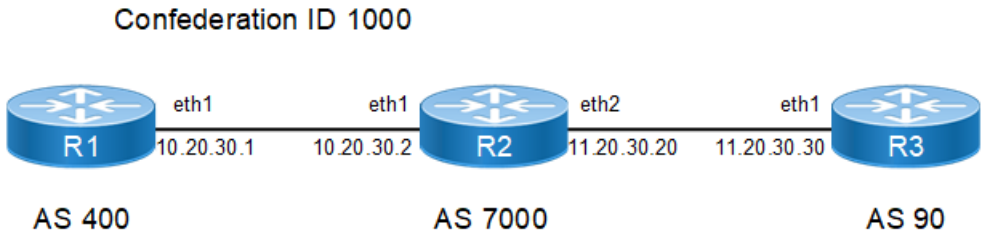


Figure 9-143: BGP Confederation

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID, the externally visible autonomous system number that identifies the BGP confederation as a whole.

`#configure terminal`	Enter configure mode.
`(config-router)#bgp confederation peers 7000`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.2 remote-as 7000`	Specify the neighbor's IP address (`10.20.30.2`) and the ASN value of the neighbor (`7000`).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.20.30.2 activate`	Activate the neighbor under address family mode
`(config-router-af)#exit-address-family`	Exit address-family mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 7000`	Assign the ASN value (`7000`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 400 90`	Specify the neighbor ASN values for confederation membership.
`(config-router)#neighbor 10.20.30.1 remote-as 400`	Specify the neighbor's IP address (`10.20.30.1`) and the ASN value of the neighbor (`400`).
`(config-router)#neighbor 11.20.30.30 remote-as 90`	Specify the neighbor's IP address (`11.20.30.30`) and the ASN value of the neighbor (`90`).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.20.30.1 activate`	Activate the neighbor under address family mode
`(config-router-af)# neighbor 11.20.30.30 activate`	Activate the neighbor under address family mode
`(config-router-af)#exit-address-family`	Exit address-family mode.

R3

`#configure terminal`	Enter configure mode.
`(config-router)#router bgp 90`	Assign the ASN value (`90`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 7000`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 11.20.30.20 remote-as 7000`	Specify the neighbor's IP address (`11.20.30.20`) and the ASN value of the neighbor (`7000`).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 11.20.30.20 activate`	Exit address-family mode.
`(config-router-af)#exit-address-family`	Exit address-family mode.

© 2021 IP Infusion Inc. Proprietary

Validation

R2

```
#sh ip bgp summary
BGP router identifier 192.168.52.3, local AS number 7000
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.1               4   400    5          5       1      0      0
00:01:36               0
11.20.30.30              4    90    2          3       1      0      0
00:00:24               0

Total number of neighbors 2

Total number of Established sessions 2

#show ip bgp neighbors
BGP neighbor is 10.20.30.1, remote AS 400, local AS 7000, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  Neighbor under common administration
  BGP state = Established, up for 00:01:25
  Last read 00:01:25, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.20.30.2, Local port: 35108
Foreign host: 10.20.30.1, Foreign port: 179
Nexthop: 10.20.30.2
Nexthop global: fe80::a00:27ff:fe21:7ed2
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.20.30.30, remote AS 90, local AS 7000, external link
  BGP version 4, remote router ID 192.168.56.103
  Neighbor under common administration
  BGP state = Established, up for 00:00:13
  Last read 00:00:13, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
```

```
  Received 2 messages, 0 notifications, 0 in queue
  Sent 3 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.20, Local port: 179
Foreign host: 11.20.30.30, Foreign port: 33465
Nexthop: 11.20.30.20
Nexthop global: fe80::a00:27ff:fed0:57d1
Nexthop local: ::
BGP connection: non shared network
```

R1

```
#show ip bgp neighbors
BGP neighbor is 10.20.30.2, remote AS 7000, local AS 400, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  Neighbor under common administration
  BGP state = Established, up for 00:01:51
  Last read 00:01:51, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 5 messages, 0 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.20.30.1, Local port: 179
Foreign host: 10.20.30.2, Foreign port: 35108
Nexthop: 10.20.30.1
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
BGP connection: non shared network


#sh ip bgp summary
BGP router identifier 192.168.52.3, local AS number 400
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries
```


© 2021 IP Infusion Inc. Proprietary

```
Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.2               4  7000    5          6       3      0      0
00:01:57              0

Total number of neighbors 1

Total number of Established sessions 1
```

R3

```
#sh ip bgp neighbors
BGP neighbor is 11.20.30.20, remote AS 7000, local AS 90, external link
  BGP version 4, local router ID 192.168.52.5, remote router ID 192.168.52.3
  Neighbor under common administration
  BGP state = Established, up for 00:00:04
  Last read 00:00:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 2 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.30, Local port: 33465
Foreign host: 11.20.30.20, Foreign port: 179
Nexthop: 11.20.30.30
Nexthop global: fe80::a00:27ff:fe24:5dc9
Nexthop local: ::
BGP connection: non shared network

#sh ip bgp summary
BGP router identifier 192.168.56.103, local AS number 90
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
11.20.30.20              4  7000    3          3       1      0      0
00:00:55              0

Total number of neighbors 1

Total number of Established sessions 1
```

Multiple Autonomous Systems

In the following example, R1 and R2 are members of the same confederation with the same AS numbers, and R3 is a member of the same confederation with a different AS number.

Topology

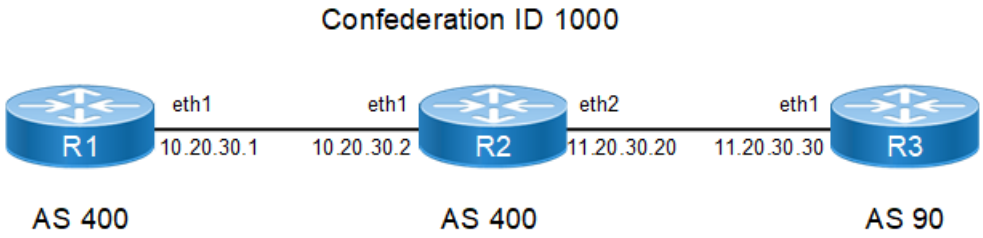


Figure 9-144: BGP Confederation with Multiple AS

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#neighbor 10.20.30.2 remote-as 400`	Specify the neighbor's IP address (`10.20.30.2`) and the ASN value of the neighbor (`400`).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.20.30.2 activate`	Activate the neighbor under address family mode
`(config-router-af)#exit-address-family`	Exit address-family mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 90`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.1 remote-as 400`	Specify the neighbor's IP address (`10.20.30.1`) and the ASN value of the neighbor (`400`).
`(config-router)#neighbor 11.20.30.30 remote-as 90`	Specify the neighbor's IP address (`11.20.30.30`) and the ASN value of the neighbor (`90`).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.20.30.1 activate`	Activate the neighbor under address family mode
`(config-router-af)# neighbor 11.20.30.30 activate`	Activate the neighbor under address family mode
`(config-router-af)#exit-address-family`	Exit address-family mode.

© 2021 IP Infusion Inc. Proprietary

R3

`#configure terminal`	Enter configure mode.
`(config)#router bgp 90`	Assign the ASN value (`90`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 400`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 11.20.30.20 remote-as 400`	Specify the neighbor's IP address (`11.20.30.20`) and the ASN value of the neighbor (`400`).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 11.20.30.20 activate`	Activate the neighbor under address family mode
`(config-router-af)#exit-address-family`	Exit address-family mode.

Validation

R2

```
#show ip bgp summary
BGP router identifier 192.168.52.3, local AS number 400
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.1               4   400   16         16       1      0      0
00:07:27              0
11.20.30.30              4    90   32         42       1      0      0
00:00:27              0

Total number of neighbors 2

Total number of Established sessions 2
#show ip bgp neighbors
BGP neighbor is 10.20.30.1, remote AS 400, local AS 400, internal link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  BGP state = Established, up for 00:08:10
  Last read 00:08:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 18 messages, 0 notifications, 0 in queue
  Sent 18 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
```

```
 Connections established 1; dropped 0
Local host: 10.20.30.2, Local port: 35214
Foreign host: 10.20.30.1, Foreign port: 179
Nexthop: 10.20.30.2
Nexthop global: fe80::a00:27ff:fe21:7ed2
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.20.30.30, remote AS 90, local AS 400, external link
  BGP version 4, remote router ID 192.168.56.103
  Neighbor under common administration
  BGP state = Established, up for 00:01:10
  Last read 00:01:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 20 messages, 14 notifications, 0 in queue
  Sent 42 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.20, Local port: 179
Foreign host: 11.20.30.30, Foreign port: 33623
Nexthop: 11.20.30.20
Nexthop global: fe80::a00:27ff:fed0:57d1
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:01:36, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

R1

```
#show ip bgp neighbors
BGP neighbor is 10.20.30.2, remote AS 400, local AS 400, internal link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  BGP state = Established, up for 00:08:41
  Last read 00:08:41, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 34 messages, 0 notifications, 0 in queue
  Sent 35 messages, 3 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 16, neighbor version 16
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
```

 © 2021 IP Infusion Inc. Proprietary

```
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 10.20.30.1, Local port: 179
Foreign host: 10.20.30.2, Foreign port: 35214
Nexthop: 10.20.30.1
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:09:03, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)

#show ip bgp summary
BGP router identifier 192.168.52.2, local AS number 400
BGP table version is 16
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.2               4   400   34         38      16      0      0
00:08:44              0

Total number of neighbors 1

Total number of Established sessions 1
```

R3

```
#show ip bgp summary
BGP router identifier 192.168.52.5, local AS number 90
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
11.20.30.20              4   400    2          2       1      0      0
00:00:15              0

Total number of neighbors 1

Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 11.20.30.20, remote AS 400, local AS 90, external link
  BGP version 4, local router ID 192.168.52.5, remote router ID 192.168.52.3
  Neighbor under common administration
  BGP state = Established, up for 00:02:24
  Last read 00:02:24, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 6 messages, 0 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
```

```
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.30, Local port: 33623
Foreign host: 11.20.30.20, Foreign port: 179
Nexthop: 11.20.30.30
Nexthop global: fe80::a00:27ff:fe24:5dc9
Nexthop local: ::
BGP connection: non shared network
```

Outside Autonomous System

In the following example, R1 and R2 are members of the same confederation with different AS numbers, and R3 is a member outside the confederation.

Topology

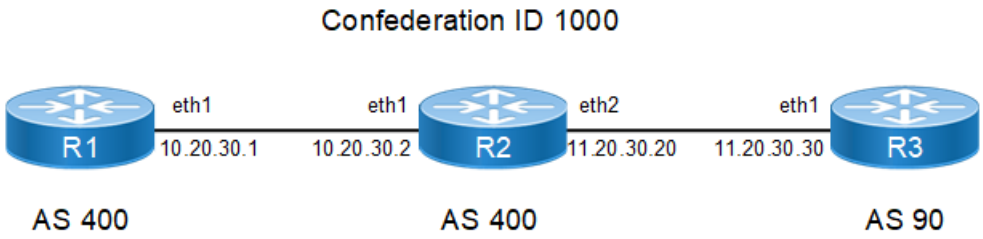


Figure 9-145: Single Confederation with Outside AS

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 7000`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.2 remote-as 7000`	Specify the neighbor's IP address (`10.20.30.2`) and the ASN value of the neighbor (`7000`).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.20.30.2 activate`	Activate the neighbor under address family mode
`(config-router-af)#exit-address-family`	Exit address-family mode.

© 2021 IP Infusion Inc. Proprietary

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 7000`	Assign the ASN value (`7000`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 400`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.1 remote-as 400`	Specify the neighbor's IP address (`10.20.30.1`) and the ASN value of the neighbor (`400`).
`(config-router)#neighbor 11.20.30.30 remote-as 90`	Specify the neighbor's IP address (`11.20.30.30`) and the ASN value of the neighbor (`90`).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.20.30.1 activate`	Activate the neighbor under address family mode
`(config-router-af)# neighbor 11.20.30.30 activate`	Activate the neighbor under address family mode
`(config-router-af)#exit-address-family`	Exit address-family mode.

R3

`#configure terminal`	Enter configure mode.
`(config)#router bgp 90`	Assign the ASN value (`90`) to the router.
`(config-router)#neighbor 11.20.30.20 remote-as 1000`	Specify the neighbor's IP address (`11.20.30.20`) and the BGP confederation ID (`1000`).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 11.20.30.20 activate`	Activate the neighbor under address family mode
`(config-router-af)#exit-address-family`	Exit address-family mode.

Validation

R3

```
#show ip bgp neighbors
BGP neighbor is 11.20.30.20, remote AS 1000, local AS 90, external link
  BGP version 4, local router ID 192.168.52.5, remote router ID 192.168.52.3
  BGP state = Established, up for 00:01:10
  Last read 00:01:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 112 messages, 1 notifications, 0 in queue
  Sent 142 messages, 88 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
```

```
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 11.20.30.30, Local port: 33951
Foreign host: 11.20.30.20, Foreign port: 179
Nexthop: 11.20.30.30
Nexthop global: fe80::a00:27ff:fe24:5dc9
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:01:26, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)

#sh ip bgp summary
BGP router identifier 192.168.52.5, local AS number 90
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
11.20.30.20              4  1000  113        230       1      0      0
00:01:13              0

Total number of neighbors 1

Total number of Established sessions 1
```

R2

```
#show ip bgp summary
BGP router identifier 192.168.52.3, local AS number 7000
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
10.20.30.1               4   400   22         22       1      0      0
00:10:04              0
11.20.30.30              4    90  179        202       1      0      0
00:00:42              0

Total number of neighbors 2

Total number of Established sessions 2

#show ip bgp neighbors
BGP neighbor is 10.20.30.1, remote AS 400, local AS 7000, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.3
  Neighbor under common administration
  BGP state = Established, up for 00:11:06
  Last read 00:11:06, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
```


© 2021 IP Infusion Inc. Proprietary

```
  Received 24 messages, 0 notifications, 0 in queue
  Sent 24 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.20.30.2, Local port: 35444
Foreign host: 10.20.30.1, Foreign port: 179
Nexthop: 10.20.30.2
Nexthop global: fe80::a00:27ff:fe21:7ed2
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.20.30.30, remote AS 90, local AS 1000, external link
  BGP version 4, remote router ID 192.168.56.103
  BGP state = Established, up for 00:01:44
  Last read 00:01:44, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 93 messages, 88 notifications, 0 in queue
  Sent 204 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.20, Local port: 179
Foreign host: 11.20.30.30, Foreign port: 33951
Nexthop: 11.20.30.20
Nexthop global: fe80::a00:27ff:fed0:57d1
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:02:00, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

R1

```
#sh ip bgp summary
BGP router identifier 192.168.52.2, local AS number 400
BGP table version is 34
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
```

```
10.20.30.2                4  7000   77          91       34       0       0
00:10:18                0

Total number of neighbors 1

Total number of Established sessions 1
#sh ip bgp neighbors
BGP neighbor is 10.20.30.2, remote AS 7000, local AS 400, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  Neighbor under common administration
  BGP state = Established, up for 00:11:40
  Last read 00:11:40, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 80 messages, 0 notifications, 0 in queue
  Sent 82 messages, 12 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 35, neighbor version 35
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 3; dropped 2
Local host: 10.20.30.1, Local port: 179
Foreign host: 10.20.30.2, Foreign port: 35444
Nexthop: 10.20.30.1
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:12:47, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

Dynamic BGP Peering

BGP Dynamic Neighbors is a quick way of setting up BGP on device like a Hub router where user is expecting numerous BGP neighbors. Before dynamic neighbors, user had to provide a large amount of configuration to work with all these neighbors. This new feature dramatically reduces the amount and complexity of CLI configuration on the router and save CPU and memory usage.

BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. Each range can be configured as a subnet IP address. BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups.

After a subnet range is configured for a BGP peer group and a TCP session is initiated by another router for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. After the initial configuration of subnet ranges and activation of the peer group, dynamic BGP neighbor creation does not require any further CLI configuration on the initial router. Other routers can establish a BGP session with the initial router, but the initial router need not establish a BGP session to other routers if the IP address of the remote peer used for the BGP session is not within the configured range.

© 2021 IP Infusion Inc. Proprietary

A dynamic BGP neighbor will inherit any configuration for the peer group. In larger BGP networks, implementing BGP dynamic neighbors can reduce the amount and complexity of CLI configuration and save CPU and memory usage. Both IPv4 and IPV6 peering is supported.

IPv4 IBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11.11.11.0/24 and 11.11.12.0/24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

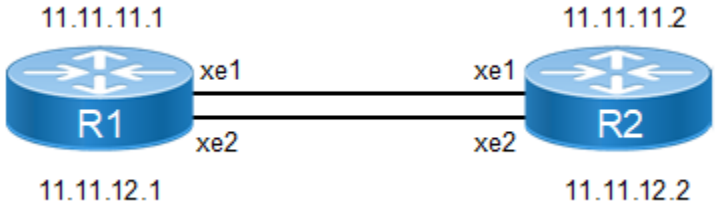


Figure 9-146: IPv4 IBGP Peering

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 33.33.33.33/32 secondary`	Assign a secondary IP address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)#ip address 11.11.11.1/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)#ip add 11.11.12.1/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 1.1.1.1`	Assign a BGP router ID.
`(config-router)#neighbor IPV4_IBGP_PEER peer- group range 11.11.0.0/16`	Create a dynamic peer-group, IPV4_IBGP_PEER with a dynamic range 11.11.0.0/16
`(config-router)#neighbor IPV4_IBGP_PEER remote-as 100`	Assign a remote AS for the peer-group, IPV4_IBGP_PEER.
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor IPV4_IBGP_PEER activate`	Activate peer-group in the address family
`(config-router-af)#network 33.33.33.33/32`	Advertise the loopback network into BGP.
`(config-router-af)#end`	Exit from Router BGP mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 22.22.22.22/32 secondary`	Assign a secondary IP address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)#ip address 11.11.11.2/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)#ip add 11.11.12.2/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 2.2.2.2`	Assign a BGP router ID.
`(config-router)#neighbor 11.11.11.1 remote-as 100`	Create a static BGP neighbor 11.11.11.1 in remote AS 100.
`(config-router)#neighbor 11.11.12.1 remote-as 100`	Create a static BGP neighbor 11.11.12.1 in remote AS 100.
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 11.11.12.1 activate`	Activate the neighbor under address family mode
`(config-router-af)# neighbor 11.11.12.1 activate`	Activate the neighbor under address family mode
`(config-router-af)# network 22.22.22.22/32`	Advertise the loopback network into BGP.
`(config-router-af)#exit-address-family`	Exit address-family mode.

Validation

R1

```
#show ip bgp summary

BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11.11.11.2              4   100   42         43       2      0      0
00:20:25              1
*11.11.12.2              4   100   42         43       2      0      0
00:20:25              1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV4_IBGP_PEER
  listen range:  11.11.0.0/16
```


© 2021 IP Infusion Inc. Proprietary

```
  Total number of dynamically created neighbors/limit: 2/(200)

Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
1

Total number of neighbors 2
Total number of Established sessions 2


#show ip bgp neighbors

BGP neighbor is 11.11.11.2, remote AS 100, local AS 100, internal link
 Member of peer-group IPV4_IBGP_PEER for session parameters
  BGP version 4, local router ID 1.1.1.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:21:56
  Last read 00:00:27, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 46 messages, 0 notifications, 0 in queue
  Sent 46 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 0, Offset 0, Mask 0x1
  IPV4_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.11.1, Local port: 40361
Foreign host: 11.11.11.2, Foreign port: 179
Nexthop: 11.11.11.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.11.12.2, remote AS 100, local AS 100, internal link
 Member of peer-group IPV4_IBGP_PEER for session parameters
  BGP version 4, local router ID 1.1.1.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:21:56
  Last read 00:00:27, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 46 messages, 0 notifications, 0 in queue
  Sent 46 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  IPV4_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
```

```
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.12.1, Local port: 33478
Foreign host: 11.11.12.2, Foreign port: 179
Nexthop: 11.11.12.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show running-config bgp
router bgp 100
bgp router-id 1.1.1.1 network 33.33.33.33/32
neighbor IPV4_IBGP_PEER peer-group range 11.11.0.0/16 neighbor IPV4_IBGP_PEER
remote-as 100
!
address-family ipv4 unicast
 neighbor IPV4_IBGP_PEER activate
 exit-address-family

#show ip bgp
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

NetworkNext HopMetricLocPrfWeight Path
*>i22.22.22.22/3211.11.11.201000i
* i11.11.12.201000i
*>33.33.33.33/320.0.0.0010032768i

Total number of prefixes 2
```

R2

```
#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
11.11.11.1               4   100   55         56       3      0      0
00:26:21              1
11.11.12.1               4   100   55         56       3      0      0
00:26:21              1

Total number of neighbors 2
Total number of Established sessions 2


#show bgp neighbors
BGP neighbor is 11.11.11.1, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
```


© 2021 IP Infusion Inc. Proprietary

```
  BGP state = Established, up for 00:26:43
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 56 messages, 0 notifications, 0 in queue
  Sent 57 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.11.2, Local port: 179
Foreign host: 11.11.11.1, Foreign port: 40361
Nexthop: 11.11.11.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.11.12.1, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 00:26:43
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 56 messages, 0 notifications, 0 in queue
  Sent 57 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.12.2, Local port: 179
Foreign host: 11.11.12.1, Foreign port: 33478
Nexthop: 11.11.12.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip bgp
BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop            Metric     LocPrf       Weight Path
*>   22.22.22.22/32   0.0.0.0              0          100           32768    i
*>i  33.33.33.33/32   11.11.11.1           0          100           0        i
* i                   11.11.12.1           0          100           0        i

Total number of prefixes 2
```

IPv4 IBGP VRF Configuration

Below figure displays the minimum configuration required to enable BGP on an interface with vrf enabled on the device and interface being part of vrf. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11.11.11.0/24 and 11.11.12.0/24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

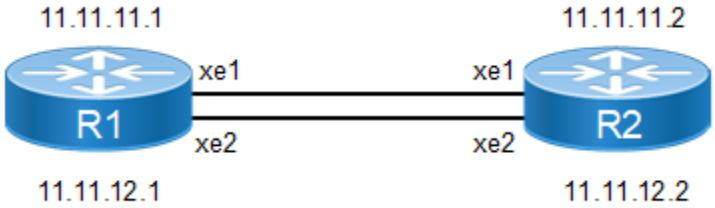


Figure 9-147: IPv4 VRF IBGP Peering

R1

`#Configure terminal`	Enter Configuration mode.
`(config)#ip vrf vrfA`	Create a VRF, vrfA on the router.
`(config-vrf)#rd 1:1`	Assign a route distinguisher to VRF.
`(config-if)#exit`	Exit VRF mode and return to Configure mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)# ip vrf forwarding vrfA`	Assign IP address to VRF.
`(config-if)#ip address 11.11.11.1/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)# ip vrf forwarding vrfA`	Assign IP address to VRF.
`(config-if)#ip add 11.11.12.1/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 1.1.1.1`	Assign a BGP router ID.
`(config-router)#address-family ipv4 vrf vrfA`	Enter IPv4 VRF Address Family.
`(config-router-af)#neighbor IPV4_IBGP_PEER peer-group range 11.11.0.0/16`	Create a dynamic peer-group, IPV4_IBGP_PEER with a dynamic range 11.11.0.0/16.
`(config-router-af)#neighbor IPV4_IBGP_PEER remote-as 100`	Assign a remote AS for the peer-group, IPV4_IBGP_PEER.

© 2021 IP Infusion Inc. Proprietary

(config-router-af)# neighbor IPV4_IBGP_PEER activate	Activate peer-group in the address family
(config-router-af)#network 33.33.33.33/32	Advertise the loopback network into BGP
(config-router-af)#end	Exit from Router BGP mode.

R2

#configure terminal	Enter configure mode.
(config)#ip vrf vrfA	Create a VRF, vrfA on router.
(config-vrf)#rd 2:1	Assign a route distinguisher to VRF.
(config-if)#exit	Exit VRF mode and return to Configure mode.
(config)#interface xe1	Enter interface mode for xe1.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.
(config-if)#ip address 11.11.11.2/24	Assign IP address to the interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode for xe2.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.
(config-if)#ip add 11.11.12.2/24	Assign IP address to the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#bgp router-id 2.2.2.2	Assign a BGP router ID.
(config-router)#address-family ipv4 vrf vrfA	Enter IPv4 VRF Address Family.
(config-router-af)#neighbor 11.11.11.1 remote-as 100	Create a static BGP neighbor 11.11.11.1 in remote AS 100.
(config-router-af)# neighbor 11.11.11.1 activate	Activate neighbor in the address family
(config-router-af)#neighbor 11.11.12.1 remote-as 100	Create a static BGP neighbor 11.11.12.1 in remote AS 100
(config-router-af)# neighbor 11.11.12.1 activate	Activate neighbor in the address family
(config-router-af)#network 22.22.22.22/32	Advertise the loopback network into BGP.
(config-router-af)#end	Exit from Router BGP mode.

Validation

R1

```
#show running-config bgp
!
router bgp 100
 bgp router-id 1.1.1.1
 !
 address-family ipv4 vrf vrfA
 neighbor IPV4_VRF_IBGP_PEER peer-group range 11.11.0.0/16
 neighbor IPV4_VRF_IBGP_PEER remote-as 100
 neighbor IPV4_VRF_IBGP_PEER activate
```

```
 network 33.33.33.33/32
 exit-address-family
!

#show ip bgp summary vrf vrfA
BGP router identifier 11.11.11.1, local AS number 100
BGP VRF vrfA Route Distinguisher: 1:1
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11.11.11.2              4   100    3          3       1      0      0
00:01:00               0
*11.11.12.2              4   100    3          3       1      0      0
00:00:55               0
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV4_IBGP_PEER
  listen range:  11.11.0.0/16
  Total number of dynamically created neighbors/limit: 2/(200)

Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
1

Total number of neighbors 2

Total number of Established sessions 2


#show bgp neighbors
BGP neighbor is 11.11.11.2, vrf vrfA, remote AS 100, local AS 100, internal
link
 Member of peer-group IPV4_IBGP_PEER for session parameters
  BGP version 4, local router ID 11.11.11.1, remote router ID 11.11.11.2
  BGP state = Established, up for 00:07:26
  Last read 00:00:26, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 16 messages, 0 notifications, 0 in queue
  Sent 16 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  IPV4_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.11.1, Local port: 36365
Foreign host: 11.11.11.2, Foreign port: 179
Nexthop: 11.11.11.1
```


© 2021 IP Infusion Inc. Proprietary

```
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.11.12.2, vrf vrfA, remote AS 100, local AS 100, internal
link
 Member of peer-group IPV4_IBGP_PEER for session parameters
  BGP version 4, local router ID 11.11.11.1, remote router ID 11.11.11.2
  BGP state = Established, up for 00:07:21
  Last read 00:00:21, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 16 messages, 0 notifications, 0 in queue
  Sent 16 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  IPV4_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.12.1, Local port: 38144
Foreign host: 11.11.12.2, Foreign port: 179
Nexthop: 11.11.12.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

IPv4 EBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1, R2 and R3 are three routers belonging to the different AS, AS100 AS200 and AS300, connecting to network 11.11.11.0/24 and 11.11.12.0/24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology



Figure 9-148: IPv4 EBGP Peering

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 33.33.33.33/32 secondary`	Assign a secondary IP address.

(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode for xe1.
(config-if)#ip address 11.11.11.1/24	Assign IP address to the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#bgp router-id 1.1.1.1	Assign a BGP router ID.
(config-router)#neighbor 11.11.11.2 remote-as 200	Create a static neighbor 11.11.11.2 with remote AS 200.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode.
(config-router-af)# neighbor 11.11.11.2 activate	Activate the neighbor under address family mode
(config-router-af)#exit-address-family	Exit address-family mode.

R2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode for loopback.
(config-if)#ip address 22.22.22.22/32 secondary	Assign a secondary IP address.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode for xe1.
(config-if)#ip address 11.11.11.2/24	Assign IP address to the interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode for xe2.
(config-if)#ip add 11.11.12.2/24	Assign IP address to the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 200	Enter Router BGP mode.
(config-router)#bgp router-id 2.2.2.2	Assign a BGP router ID.
(config-router)#neighbor IPV4_EBGP_PEER peer-group range 11.11.0.0/16	Create a dynamic peer-group, IPV4_EBGP_PEER.
(config-router)#neighbor IPV4_EBGP_PEER remote-as 100	Assign remote AS with the peer-group IPV4_EBGP_PEER.
(config-router)#neighbor IPV4_EBGP_PEER optional-as 300	Assign optional AS with the peer-group IPV4_EBGP_PEER
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor IPV4_EBGP_PEER activate	Activate the peer-group in address family
(config-router-af)#network 22.22.22.22/32	Advertise the loopback network into BGP.
(config-router-af)#end	Exit from address family mode.

R3

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode for loopback.

© 2021 IP Infusion Inc. Proprietary

(config-if)#ip address 44.44.44.44/32 secondary	Assign a secondary IP address.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode for xe2.
(config-if)#ip add 11.11.12.3/24	Assign IP address to the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 300	Enter Router BGP mode.
(config-router)#bgp router-id 3.3.3.3	Assign a BGP router ID.
(config-router)#neighbor 11.11.12.2 remote-as 200	Create a static BGP neighbor 11.11.12.2 with remote AS 200.
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 11.11.12.2 activate	Activate the neighbor under address family mode
(config-router-af)#network 44.44.44.44/32	Advertise the loopback network into BGP.
(config-router-af)#exit-address-family	Exit address-family mode.

Validation

R2

```
#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 200
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries
Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11.11.11.1              4   100   29         29       3      0      0
00:13:10              1
*11.11.12.3              4   300   27         27       3      0      0
00:12:20              1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV4_EBGP_PEER
  listen range:  11.11.0.0/16
  Total number of dynamically created neighbors/limit: 2/(200)
Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
1
Total number of neighbors 2
Total number of Established sessions 2

#show running-config bgp
!
router bgp 200
 bgp router-id 2.2.2.2
 network 22.22.22.22/32
 neighbor IPV4_EBGP_PEER peer-group range 11.11.0.0/16
 neighbor IPV4_EBGP_PEER remote-as 100
 neighbor IPV4_EBGP_PEER optional-as 300
!
 address-family ipv4 unicast
```

```
 neighbor IPV4_EBGP_PEER activate
 network 33.33.33.33/32
 exit-address-family
!


#show bgp neighbors
BGP neighbor is 11.11.11.1, remote AS 100, local AS 200, external link
 Member of peer-group IPV4_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 00:17:15
  Last read 00:00:15, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 37 messages, 0 notifications, 0 in queue
  Sent 38 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  IPV4_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  2 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.11.2, Local port: 42252
Foreign host: 11.11.11.1, Foreign port: 179
Nexthop: 11.11.11.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.11.12.3, remote AS 300, local AS 200, external link
 Member of peer-group IPV4_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID 3.3.3.3
  BGP state = Established, up for 00:13:17
  Last read 00:00:17, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 29 messages, 0 notifications, 0 in queue
  Sent 30 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 2, Offset 0, Mask 0x4
  IPV4_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  2 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.12.2, Local port: 59839
```


© 2021 IP Infusion Inc. Proprietary

```
Foreign host: 11.11.12.3, Foreign port: 179
Nexthop: 11.11.12.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

IPv6 IBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11:11:11::1/64 and 11:11:12::1/64. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

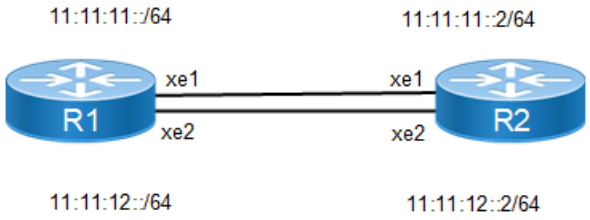


Figure 9-149: IPv6 IBGP Peering

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ipv6 address 33::1/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)#ipv6 address 11:11:11::1/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)#ipv6 address 11:11:12::1/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 1.1.1.1`	Assign a BGP router ID.
`(config-router)#neighbor IPV6_IBGP_PEER peer-group range 11:11::/16`	Create a dynamic peer-group, IPV6_IBGP_PEER with a dynamic range 11:11::/16
`(config-router)#neighbor IPV6_IBGP_PEER remote-as 100`	Configure a remote AS with the peer group, IPV6_IBGP_PEER.
`(config-router)#neighbor IPV6_IBGP_PEER limit 1`	Set peer group neighbors limit to 1. Only one BGP session will be up.
`(config-router)#address-family ipv6 unicast`	Enter the IPv6 Unicast Address Family.
`(config-router-af)#neighbor IPV6_IBGP_PEER activate`	Activate the peer group, IPV6_IBGP_PEER in the IPv6 address family.

`#configure terminal`	Enter configure mode.
`(config-router-af)#network 33::1/128`	Advertise the loopback network into the BGP IPv6 address family.
`(config-router-af)#end`	Exit from address family mode.

R2

`#Configure terminal`	Enter Configuration mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ipv6 address 22::2/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)#ipv6 address 11:11:11::2/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)#ipv6 address 11:11:12::2/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 2.2.2.2`	Assign a BGP router ID.
`(config-router)#neighbor 11:11:11::1 remote-as 100`	Configure BGP neighbor by specifying the neighbor IP address.
`(config-router)#neighbor 11:11:12::1 remote-as 100`	Configure BGP neighbor by specifying the neighbor IP address.
`(config-router)#address-family ipv4 unicast`	Enter the Ipv4 Unicast Address Family.
`(config-router-af)# neighbor 11:11:11::1 activate`	Activate the neighbor under address family mode
`(config-router-af)# neighbor 11:11:12::1 activate`	Activate the neighbor under address family mode
`(config-router-af)# exit-address-family`	Exit address-family mode.
`(config-router)#address-family ipv6 unicast`	Enter the IPv6 Unicast Address Family.
`(config-router-af)#network 22::2/128`	Advertise the loopback network into BGP.
`(config-router-af)#neighbor 11:11:12::1 activate`	Activate the neighbor in the IPv6 address family.
`(config-router-af)#neighbor 11:11:11::1 activate`	Activate the neighbor in the IPv6 address family.
`(config-router-af)#end`	Exit from address family mode.

Validation

R1

```
#show ipv6 bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
```


© 2021 IP Infusion Inc. Proprietary

```
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11:11:11::2             4   100    6          6       2      0      0
00:01:41               1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV6_IBGP_PEER
  listen range:  11::/16
  Total number of dynamically created neighbors/limit: 1/(1)

Total number of dynamically created neighbors: 1
Total number of activated dynamic peer-groups for IPv6 Unicast address-family:
1

Total number of neighbors 1

Total number of Established sessions 1

#show ip bgp peer-group IPV6_IBGP_PEER

BGP dynamic peer-group is IPV6_IBGP_PEER, IBGP, remote AS 100
  BGP dynamic peer-group IPV6_IBGP_PEER listen range group members:
  11::/16
  BGP version 4
Minimum time between advertisement runs is 5 seconds
For address family: IPv4 Unicast
  Peer-group member:
  *11:11:11::2
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes, 0 announced prefixes
For address family: IPv6 Unicast
  Peer-group member:
  *11:11:11::2
  Index 0, Offset 0, Mask 0x0
  1 accepted prefixes, 1 announced prefixes


#show bgp ipv6
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  22::2/128        11:11:11::2(fe80::5054:ff:fe95:85ec)
                                          0         100           0        i
*>   33::1/128        ::                   0         100           32768    i

Total number of prefixes 2

#show running-config bgp
!
router bgp 100
 bgp router-id 1.1.1.1
```

```
 neighbor IPV6_IBGP_PEER peer-group range 11::/16
 neighbor IPV6_IBGP_PEER remote-as 100
 neighbor IPV6_IBGP_PEER limit 1
 !
 address-family ipv6 unicast
 network 33::1/128
 neighbor IPV6_IBGP_PEER activate
 exit-address-family


#show bgp neighbors
BGP neighbor is 11:11:11::2, remote AS 100, local AS 100, internal link
 Member of peer-group IPV6_IBGP_PEER for session parameters
  BGP version 4, local router ID 1.1.1.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:04:17
  Last read 00:00:18, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  IPV6_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: IPv6 Unicast
  BGP table version 2, neighbor version 2
  Index 0, Offset 0, Mask 0x0
  IPV6_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 11:11:11::1, Local port: 42410
Foreign host: 11:11:11::2, Foreign port: 179
Nexthop: 1.1.1.1
Nexthop global: 11:11:11::1
Nexthop local: fe80::5054:ff:fe51:f74
BGP connection: shared network
```

IPV6 IBGP VRF Configuration

Below figure displays the minimum configuration required to enable BGP on an interface with VRF enabled on the device and interface being part of VRF. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11:11:11::1 and 11:11:12::1. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

 © 2021 IP Infusion Inc. Proprietary

Topology

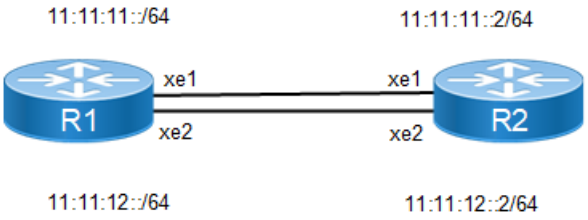


Figure 9-150: IPv6 VRF IBGP peering

R1

`#Configure terminal`	Enter Configuration mode.
`(config)#ip vrf vrfA`	Configure a VRF, vrfA.
`(config-vrf)#rd 1:1`	Configure a route distinguisher to VRF.
`(config-vrf)#router-id 7.7.7.7`	Configure a router ID.
`(config-vrf)#exit`	Exit from VRF mode and return to Configuration mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)# ip vrf forwarding vrfA`	Assign IP address to VRF.
`(config-if)#ipv6 address 11:11:11::1/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)# ip vrf forwarding vrfA`	Assign IP address to VRF.
`(config-if)#ipv6 address 11:11:12::1/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#address-family ipv6 vrf vrfA`	Enter IPv6 VRF Address Family.
`(config-router-af)#neighbor IPV6_VRF_IBGP_PEER peer-group range 11:11::1/16`	Configure a dynamic peer group, IPV6_IBGP_PEER with a dynamic range value.
`(config-router-af)#neighbor IPV6_VRF_IBGP_PEER remote-as 100`	Configure a remote AS with the peer group, IPV6_IBGP_PEER.
`(config-router-af)# neighbor IPV6_VRF_IBGP_PEER activate`	Activate neighbor in the address family
`(config-router-af)#end`	Exit from address family mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrfA`	Configure a VRF, vrfA.
`(config-vrf)#rd 2:1`	Configure a route distinguisher to VRF.
`(config-vrf)#router-id 1.1.1.1`	Configure a router ID.
`(config-vrf)#exit`	Exit from VRF mode and return to Configuration mode.
`(config)#interface xe1`	Enter interface mode for xe1.

© 2021 IP Infusion Inc. Proprietary

`#configure terminal`	Enter configure mode.
`(config-if)# ip vrf forwarding vrfA`	Assign IP address to VRF.
`(config-if)#ipv6 address 11:11:11::2/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)# ip vrf forwarding vrfA`	Assign IP address to vrf.
`(config-if)#ipv6 address 11:11:12::2/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode
`(config-router)#address-family ipv6 vrf vrfA`	Enter IPv6 VRF Address Family.
`(config-router-af)#neighbor 11:11:12::1 remote-as 100`	Configure BGP neighbor by specifying the neighbor IP address.
`(config-router-af)#neighbor 11:11:11::1 remote-as 100`	Configure BGP neighbor by specifying the neighbor IP address.
`(config-router-af)#end`	Exit from address family mode..

Validation

R1

```
#show ipv6 bgp summary vrf vrfA
BGP router identifier 7.7.7.7, local AS number 100
BGP VRF vrfA Route Distinguisher: 1:1
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11:11:11::2             4   100    6          6       1      0      0
00:00:17              0
*11:11:12::2             4   100    7         10       1      0      0
00:00:15              0
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV6_VRF_IBGP_PEER
  listen range:  11::/16
  Total number of dynamically created neighbors/limit: 2/(200)

Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv6 Unicast address-family:
1

Total number of neighbors 2

Total number of Established sessions 2


#show running-config bgp
!
router bgp 100
```


© 2021 IP Infusion Inc. Proprietary

```
 !
 address-family ipv6 vrf vrfA
 neighbor IPV6_VRF_IBGP_PEER peer-group range 11::/16
 neighbor IPV6_VRF_IBGP_PEER remote-as 100
 neighbor IPV6_VRF_IBGP_PEER activate
 exit-address-family
!

#show ip bgp peer-group vrf vrfA

BGP dynamic peer-group is IPV6_VRF_IBGP_PEER, IBGP, remote AS 100
  BGP dynamic peer-group IPV6_VRF_IBGP_PEER listen range group members:
  11::/16
  BGP version 4
Minimum time between advertisement runs is 5 seconds
For address family: IPv6 Unicast
  Peer-group member:
  *11:11:12::2
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes, 0 announced prefixes
  Peer-group member:
  *11:11:11::2
  Index 2, Offset 0, Mask 0x4
  0 accepted prefixes, 0 announced prefixes

#show running-config bgp
!
router bgp 100
 !
 address-family ipv6 vrf vrfA
 neighbor IPV6_VRF_IBGP_PEER peer-group range 11::/16
 neighbor IPV6_VRF_IBGP_PEER remote-as 100
 neighbor IPV6_VRF_IBGP_PEER activate
 exit-address-family
!
#show bgp ipv6 neighbors
BGP neighbor is 11:11:11::2, vrf vrfA, remote AS 100, local AS 100, internal
link
 Member of peer-group IPV6_VRF_IBGP_PEER for session parameters
  BGP version 4, local router ID 7.7.7.7, remote router ID 1.1.1.1
  BGP state = Established, up for 00:02:13
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv6 Unicast: advertised and received
  Received 8 messages, 2 notifications, 0 in queue
  Sent 10 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  IPV6_VRF_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
```

```
 Connections established 1; dropped 0
Local host: 11:11:11::1, Local port: 179
Foreign host: 11:11:11::2, Foreign port: 48206
Nexthop: 7.7.7.7
Nexthop global: 11:11:11::1
Nexthop local: fe80::5054:ff:fe51:f74
BGP connection: shared network
Last Reset: 00:02:18, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad BGP Identifier.)

BGP neighbor is 11:11:12::2, vrf vrfA, remote AS 100, local AS 100, internal
link
 Member of peer-group IPV6_VRF_IBGP_PEER for session parameters
  BGP version 4, local router ID 7.7.7.7, remote router ID 1.1.1.1
  BGP state = Established, up for 00:02:11
  Last read 00:00:12, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv6 Unicast: advertised and received
  Received 8 messages, 3 notifications, 0 in queue
  Sent 13 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  IPV6_VRF_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11:11:12::1, Local port: 179
Foreign host: 11:11:12::2, Foreign port: 49010
Nexthop: 7.7.7.7
Nexthop global: 11:11:12::1
Nexthop local: fe80::5054:ff:fe8b:8f5c
BGP connection: shared network
Last Reset: 00:02:16, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad BGP Identifier.)
```

IPv6 EBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1, R2 and R3 are three routers belonging to the different AS, AS100 AS200 and AS300, connecting to network 11:11:11::/64 and 11:11:12::/64. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology



Figure 9-151: IPv6 EBGP peering

© 2021 IP Infusion Inc. Proprietary

R1

`#configure terminal`	Enter Configuration mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ipv6 address 33::1/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1.
`(config-if)#ipv6 address 11:11:11::1/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 1.1.1.1`	Assign a BGP router ID.
`(config-router)#neighbor 11:11:11::2 remote-as 200`	Configure BGP neighbor by specifying the neighbor IP address.
`(config-router)#address-family ipv6 unicast`	Enter the IPv6 Unicast Address Family.
`(config-router-af)#neighbor 11:11:11::2 activate`	Activate the neighbor in the address family.
`(config-router-af)#network 33::1/128`	Advertise the loopback network into BGP.
`(config-router-af)#end`	Exit from Router BGP mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ipv6 address 22::1/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter interface mode for xe1
`(config-if)#ipv6 address 11:11:11::2/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2.
`(config-if)#ipv6 address 11:11:12::2/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Enter Router BGP mode.
`(config-router)#bgp router-id 2.2.2.2`	Assign a BGP router ID.
`(config-router)#neighbor IPV6_EBGP_PEER peer-group range 11::1/16`	Configure a dynamic peer group, IPV6_EBGP_PEER.
`(config-router)#neighbor IPV6_EBGP_PEER remote-as 100`	Configure remote AS with peer group, IPV6_EBGP_PEER.
`(config-router)#neighbor IPV6_EBGP_PEER optional-as 300`	Configure optional AS with peer group, IPV6_EBGP_PEER.
`(config-router)#address-family ipv6 unicast`	Enter IPv6 Unicast Address Family.
`(config-router-af)#neighbor IPV6_EBGP_PEER activate`	Activate peer group in the address family.
`(config-router-af)#network 22::1/128`	Advertise the loopback network into BGP.
`(config-router-af)#end`	Exit from Router BGP mode.

R3

`#Configure terminal`	Enter Configuration mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ipv6 address 44::1/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode for xe2
`(config-if)#ipv6 address 11:11:12::3/64`	Assign an IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 300`	Enter Router BGP mode.
`(config-router)#bgp router-id 3.3.3.3`	Assign a BGP router ID.
`(config-router)#neighbor 11:11:12::2 remote-as 200`	Configure the BGP neighbor by specifying the neighbor IP address.
`(config-router)#address-family ipv6 unicast`	Enter the IPv6 Unicast Address Family.
`(config-router-af)#neighbor 11:11:12::2 activate`	Activate the neighbor in address family.
`(config-router-af)#network 44::1/128`	Advertise the loopback network into BGP.
`(config-router-af)#end`	Exit from Router BGP mode.

Validation

R2

```
#show ipv6 bgp sum
BGP router identifier 2.2.2.2, local AS number 200
BGP table version is 5
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11:11:11::1             4   100    9          11       5      0      0
00:01:28              1
*11:11:12::3             4   300    6           6       5      0      0
00:01:14              1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV6_EBGP_PEER
  listen range:  11::/16
  Total number of dynamically created neighbors/limit: 2/(200)
Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv6 Unicast address-family:
1
Total number of neighbors 2
Total number of Established sessions 2


#show running-config bgp
!
```


© 2021 IP Infusion Inc. Proprietary

```
router bgp 200
 bgp router-id 2.2.2.2
 neighbor IPV6_EBGP_PEER peer-group range 11::/16
 neighbor IPV6_EBGP_PEER remote-as 100
 neighbor IPV6_EBGP_PEER optional-as 300
 !
 address-family ipv6 unicast
 network 22::1/128
 neighbor IPV6_EBGP_PEER activate
 exit-address-family
!

#show bgp ipv6 neighbors
BGP neighbor is 11:11:11::1, remote AS 100, local AS 200, external link
 Member of peer-group IPV6_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 00:02:15
  Last read 00:00:16, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 12 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  IPV6_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: IPv6 Unicast
  BGP table version 5, neighbor version 5
  Index 0, Offset 0, Mask 0x0
  IPV6_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  2 announced prefixes

 Connections established 2; dropped 1
Local host: 11:11:11::2, Local port: 53043
Foreign host: 11:11:11::1, Foreign port: 179
Nexthop: 2.2.2.2
Nexthop global: 11:11:11::2
Nexthop local: fe80::5054:ff:fe95:85ec
BGP connection: shared network
Last Reset: 00:02:20, due to BGP Notification sent
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 11:11:12::3, remote AS 300, local AS 200, external link
 Member of peer-group IPV6_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID 3.3.3.3
  BGP state = Established, up for 00:02:01
  Last read 00:00:02, hold time is 90, keepalive interval is 30 seconds
```

```
 Neighbor capabilities:
   Route refresh: advertised and received (old and new)
   Address family IPv4 Unicast: advertised and received
   Address family IPv6 Unicast: advertised and received
 Received 8 messages, 0 notifications, 0 in queue
 Sent 8 messages, 0 notifications, 0 in queue
 Route refresh request: received 0, sent 0
 Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
 BGP table version 1, neighbor version 1
 Index 0, Offset 0, Mask 0x1
 IPV6_EBGP_PEER peer-group member
 Community attribute sent to this neighbor (both)
 0 accepted prefixes
 0 announced prefixes

For address family: IPv6 Unicast
 BGP table version 5, neighbor version 5
 Index 0, Offset 0, Mask 0x0
 IPV6_EBGP_PEER peer-group member
 Community attribute sent to this neighbor (both)
 1 accepted prefixes
 2 announced prefixes

 Connections established 1; dropped 0
Local host: 11:11:12::2, Local port: 47743
Foreign host: 11:11:12::3, Foreign port: 179
Nexthop: 2.2.2.2
Nexthop global: 11:11:12::2
Nexthop local: fe80::5054:ff:fee5:b088
BGP connection: shared network
```

VPNV4 Configuration

Below mentioned topology displays bgp vpnv4 configuration on PE nodes, R1 and R3. IBGP peering will be formed on the loopback interface of R1 and R3; also IGP is running between all the routers.

Topology



Figure 9-152: IPv4 IBGP VPNv4 Configuration

R1

`#Configure terminal`	Enter Configuration mode.
`(config)#ip vrf vrf1`	Create a VRF, vrf1.
`(config-vrf)#rd 100:1`	Configure a route distinguisher value.
`(config-vrf)#route-target export 100:1`	Configure a route target export value to VRF.
`(config-vrf)#route-target import 200:1`	Configure a route target import value to VRF.

© 2021 IP Infusion Inc. Proprietary

(config-vrf)#exit	Exit from VRF configuration mode.
(config)#router ldp	Enter Router LDP mode.
(config-router)#router-id 3.3.3.3	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode.
(config)#interface xe5	Enter Interface configuration mode.
(config-if)#ip vrf forwarding vrf1	Configure the interface to a VRF.
(config-if)#ip address 1.1.1.1/24	Assign an IP address to the interface.
(config-if)#exit	Exit from Interface configuration mode.
(config-if)#interface xe1	Enter another interface.
(config-if)#ip address 11.11.11.1/24	Assign an IP address to the interface.
(config-if)#label-switching	Enable label switching on interface.
(config-if)#enable-ldp ipv4	Enable IPv4 LDP configuration on interface.
(config-if)#exit	Exit from Interface configuration mode.
(config-if)#interface lo	Enter the loopback interface.
(config-if)#ip address 20.20.20.20/32 secondary	Assign a secondary IP address to the interface.
(config-if)#exit	Exit from Interface Configuration mode.
(config)#router ospf 100	Enter Router OSPF mode.
(config-router)#network 11.11.11.0/24 area 0	Configure the interface on which OSPF runs, and associate the area ID.
(config-router)#network 20.20.20.20/32 area 0	Configure the interface on which OSPF runs, and associate the area ID.
(config-router)#exit	Exit from Router OSPF mode.
(config)#router ospf 200 vrf1	Create an OSPF process on VRF.
(config-router)#network 1.1.1.1/24 area 0	Configure the interface on which OSPF runs, and associate the area ID.
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode.
(config-router-af)#redistribute bgp	Redistribute BGP into OSPF.
(config-router-af)#exit-address-family	Exit from `address-family` mode.
(config-router)#exit	Exit from Router OSPF mode.
(config)#router bgp 100	Create a BGP process.
(config-router)#neighbor lo_peer peer-group range 30.30.30.30/32	Configure a dynamic peer group with the range command.
(config-router)#neighbor lo_peer remote-as 100	Configure remote AS to the peer group.
(config-router)#neighbor lo_peer update-source lo	Configure BGP neighbors to update the source routes.
(config-router)#address-family vpnv4 unicast	Enter the VPNv4 Address Family.
(config-router-af)#neighbor lo_peer activate	Activate the peer group in VPNv4 address family.
(config-router-af)#exit-address-family	Exit from VPNv4 address family.
(config-router)#address-family ipv4 vrf vrf1	Enter IPv4 VRF address family.
(config-router-af)#redistribute ospf 200	Redistribute OSPF into the IPv4 VRF address family.
(config-router-af)#end	Exit from the Router BGP mode.

R2

`#Configure terminal`	Enter Configuration mode.
`(config)#router ldp`	Enter Router LDP mode.
`(config-router)#router-id 4.4.4.4`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode.
`(config-if)#interface xe2`	Enter Interface Configuration mode.
`(config-if)#ip address 12.12.12.2/24`	Assign an IP address to the interface.
`(config-if)#label-switching`	Enable label switching on the interface.
`(config-if)#enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from Interface configuration mode.
`(config-if)#interface xe1`	Enter another Interface.
`(config-if)#ip address 11.11.11.2/24`	Assign an IP address to the interface.
`(config-if)#label-switching`	Enable label switching on the interface.
`(config-if)#enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from Interface mode.
`(config)#router ospf 100`	Create an OSPF process.
`(config-router)#network 11.11.11.0/24 area 0`	Define the interface on which OSPF runs, and associate the area ID
`(config-router)#network 12.12.12.0/24 area 0`	Define the interface on which OSPF runs, and associate the area ID
`(config-router)#end`	Exit from Router BGP mode.

R3

`#Configure terminal`	Enter Configuration mode.
`(config)#router ldp`	Enter Router LDP mode.
`(config-router)#router-id 5.5.5.5`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode.
`(config)#ip vrf vrf2`	Create a VRF, vrf2.
`(config-vrf)#rd 200:1`	Configure a route distinguisher value.
`(config-vrf)#route-target export 200:1`	Configure a route target export value to VRF.
`(config-vrf)#route-target import 100:1`	Configure a route target import value to VRF.
`(config-vrf)#exit`	Exit from VRF configuration mode.
`(config)#interface xe1`	Enter Interface configuration mode.
`(config-if)#ip vrf forwarding vrf2`	Configure an interface to a VRF.
`(config-if)#ip address 2.2.2.3/24`	Assign an IP address to the interface.
`(config-if)#exit`	Exit from Interface configuration mode.
`(config-if)#interface xe2`	Enter another interface.
`(config-if)#ip address 12.12.12.3/24`	Assign an IP address to the interface.
`(config-if)#label-switching`	Enable label switching on interface.
`(config-if)#enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit from Interface configuration mode.
(config-if)#interface lo	Enter loopback interface.
(config-if)#ip address 30.30.30.30/32 se	Assign a secondary IP address to the interface.
(config-if)#exit	Exit from Interface mode.
(config)#router ospf 100	Enter Router OSPF mode.
(config-router)#network 12.12.12.0/24 area 0	Define the interface on which OSPF runs, and associate the area ID
(config-router)#network 30.30.30.30/32 area 0	Define the interface on which OSPF runs, and associate the area ID
(config-router)#exit	Exit from Router OSPF mode.
(config)#router ospf 200 vrf2	Create an OSPF process on VRF.
(config-router)#network 2.2.2.3/24 area 0	Define the interface on which OSPF runs, and associate the area ID.
(config-router)#redistribute bgp	Redistribute BGP into OSPF.
(config-router)#exit	Exit from Router OSPF mode.
(config)#router bgp 100	Create a BGP process.
(config-router)#neighbor 20.20.20.20 remote-as 100	Configure BGP neighbor by specifying a neighbor IP address.
(config-router)#neighbor 20.20.20.20 update-slo	Define the BGP neighbors to update the source routes.
(config-router)#address-family vpnv4 unicast	Enter VPNv4 Address Family.
(config-router-af)#neighbor 20.20.20.20 activate	Activate the neighbor in VPNv4 address family.
(config-router-af)#exit-address-family	Exit from VPNv4 address family.
(config-router)#address-family ipv4 vrf vrf2	Enter IPv4 VRF address family.
(config-router-af)#redistribute ospf 200	Redistribute OSPF into the IPv4 address family.
(config-router-af)#end	Exit from Router BGP mode.

Validation

R1

```
#show running-config router bgp
router bgp 100
 neighbor lo_peer peer-group range 30.30.30.30/32
 neighbor lo_peer remote-as 100
 neighbor lo_peer update-source lo
 !
 address-family vpnv4 unicast
 neighbor lo_peer activate
 exit-address-family
 !
 address-family ipv4 vrf vrf1
 redistribute ospf 200
 exit-address-family
!

#show ip bgp vpnv4 all summary
BGP router identifier 192.168.52.3, local AS number 100
```

```
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*30.30.30.30             4   100    4          4       2      0      0
00:00:37               1
* Dynamically created based on a listen range command

BGP dynamic peer-group: lo_peer
  listen range:  30.30.30.30/32
  Total number of dynamically created neighbors/limit: 1/(200)

Total number of dynamically created neighbors: 1
Total number of activated dynamic peer-groups for VPNv4 Unicast address-
family: 1

Total number of neighbors 1

Total number of Established sessions 1


#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 100:1 (Default for VRF vrf1)
*>   1.1.1.0/24       0.0.0.0              1         100           32768    ?
*>i  2.2.2.0/24       30.30.30.30          1         100           0        ?
 Announced routes count = 1
 Accepted routes count = 1
Route Distinguisher: 200:1
*>i  2.2.2.0/24       30.30.30.30          1         100           0        ?
 Announced routes count = 0
 Accepted routes count = 1


#show ip bgp vpnv4 all 1.1.1.0
Route Distinguisher: 100:1
  Local
    20.20.20.20 (metric 12) from 20.20.20.20 (192.178.50.2)
      Origin incomplete, metric 1, localpref 100, label    24960, valid,
internal, best
      Extended Community: RT:100:1 0:0  OSPF-Route-type:0.0.0.0 :3:0

      Last update: Tue Apr 23 10:29:10 2019

Route Distinguisher: 200:1 (Default for VRF vrf2)
  Local
    20.20.20.20 from 20.20.20.20 (192.178.50.2)
      Origin incomplete, metric 1, localpref 100, label    24960, valid,
internal, best
      Extended Community: RT:100:1 0:0  OSPF-Route-type:0.0.0.0 :3:0
```


© 2021 IP Infusion Inc. Proprietary

```
          Last update: Tue Apr 23 10:29:10 2019


    #show ip bgp peer-group

    BGP dynamic peer-group is lo_peer, IBGP, remote AS 100
      BGP dynamic peer-group lo_peer listen range group members:
      30.30.30.30/32
      BGP version 4
    Minimum time between advertisement runs is 5 seconds
    For address family: IPv4 Unicast
      Peer-group member:
      *30.30.30.30
      Index 1, Offset 0, Mask 0x2
      0 accepted prefixes, 0 announced prefixes
    For address family: VPNv4 Unicast
      Peer-group member:
      *30.30.30.30
      Index 0, Offset 0, Mask 0x0
      1 accepted prefixes, 1 announced prefixes
```

R2

```
R2#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 100:1 (Default for VRF vrf1)
*>   1.1.1.0/24       0.0.0.0              1         100           32768    ?
*>i  2.2.2.0/24       30.30.30.30          1         100           0        ?
 Announced routes count = 1
 Accepted routes count = 1
Route Distinguisher: 200:1
*>i  2.2.2.0/24       30.30.30.30          1         100           0        ?
 Announced routes count = 0
 Accepted routes count = 1
R2#
```

R3

```
R3#show ip bgp vpnv4 all 1.1.1.0
Route Distinguisher: 100:1
  Local
    20.20.20.20 (metric 12) from 20.20.20.20 (192.178.50.2)
      Origin incomplete, metric 1, localpref 100, label    24960, valid, internal, best
      Extended Community: RT:100:1 0:0  OSPF-Route-type:0.0.0.0 :3:0

      Last update: Tue Apr 23 10:29:10 2019

Route Distinguisher: 200:1 (Default for VRF vrf2)
  Local
```

```
    20.20.20.20 from 20.20.20.20 (192.178.50.2)
      Origin incomplete, metric 1, localpref 100, label    24960, valid, internal, best
      Extended Community: RT:100:1 0:0  OSPF-Route-type:0.0.0.0 :3:0

      Last update: Tue Apr 23 10:29:10 2019

R3#
```

Enable eBGP Multihop

This example shows the minimum configuration required for enabling eBGP multihop on peers speaking BGP. eBGP multihop is used for routers that are not directly connected to each other. Typically, eBGP peers are directly connected, but if there is a requirement that necessitates this scenario, this configuration can be used.

Note: The IP addresses used in the configuration should be accessible through an IGP or static routing.

Topology

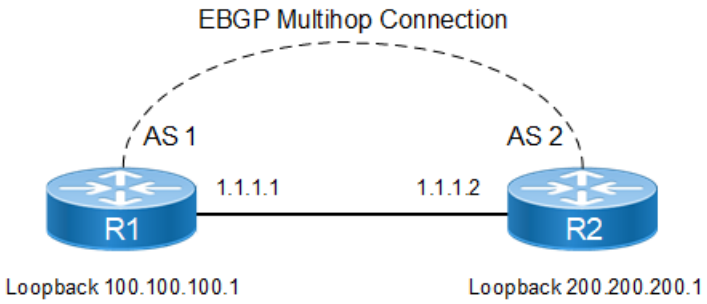


Figure 9-153: eBGP Multihop Connection

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 100.100.100.1/24 secondary`	Specify IP address to the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#ip route 200.200.200.0/24 1.1.1.2`	Specify route IP address.
`(config)#router bgp 1`	Define the routing process. The number `1` specifies the AS number of `R1`.
`(config-router)#neighbor 200.200.200.1 remote-as 2`	Define BGP neighbors, and establish a TCP session. 200.200.200.1 is the IP address of the neighbor (R2), and 2 is the neighbor's AS number.
`(config-router)#neighbor 200.200.200.1 update-source lo`	Define BGP neighbors, to update the source routes.
`(config-router)#neighbor 200.200.200.1 ebgp-multihop`	Define the neighbor `200.200.200.1` for eBGP multihops.
`(config-router)#address-family ipv4 unicast`	Enter the Ipv4 Unicast Address Family.

© 2021 IP Infusion Inc. Proprietary

(config-router-af)# neighbor 200.200.200.1 activate	Activate the neighbor under address family mode
(config-router-af)# exit-address-family	Exit address-family mode.

R2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter loopback interface mode.
(config-if)#ip address 200.200.200.1/24 secondary	Specify IP address to the interface.
(config-if)#exit	Exit loopback interface mode.
(config)#ip route 100.100.100.0/24 1.1.1.1	Specify route IP address.
(config)#router bgp 2	Define the routing process. The number 2 specifies the AS number of R1.
(config-router)#neighbor 100.100.100.1 remote-as 1	Define BGP neighbors, and establish a TCP session. 100.100.100.1 is the IP address of the neighbor (R2), and 1 is the neighbor's AS number.
(config-router)#neighbor 100.100.100.1 update-source lo	Define BGP neighbors, to update the source routes.
(config-router)#neighbor 100.100.100.1 ebgp-multihop	Define the neighbor 100.100.100.1 for eBGP multihops.
(config-router)#address-family ipv4 unicast	Config redistribute under address-family
(config-router-af)# neighbor 100.100.100.1 activate	Activate the neighbor under address family mode
(config-router-af)#redistribute static	Redistribute static route
(config-router-af)#exit-address-family	Exit address-family mode

Validation

R1

```
#show ip bgp neighbors
BGP neighbor is 200.200.200.1, remote AS 2, local AS 1, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  BGP state = Established, up for 00:00:22
  Last read 00:00:22, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 3 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
```

```
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
  External BGP neighbor may be up to 255 hops away.
Local host: 100.100.100.1, Local port: 179
Foreign host: 200.200.200.1, Foreign port: 59458
Nexthop: 100.100.100.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network


#show ip bgp
BGP table version is 4, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   100.100.100.0/24 200.200.200.1        0         100           0       2 ?

Total number of prefixes 1


#show ip bgp neighbors
BGP neighbor is 200.200.200.1, remote AS 2, local AS 1, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  BGP state = Established, up for 00:00:26
  Last read 00:00:26, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 5 messages, 0 notifications, 0 in queue
  Sent 6 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
  External BGP neighbor may be up to 255 hops away.
Local host: 100.100.100.1, Local port: 57260
Foreign host: 200.200.200.1, Foreign port: 179
Nexthop: 100.100.100.1
```


© 2021 IP Infusion Inc. Proprietary

```
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:31, due to BGP Notification sent
Notification Error Message: (Cease/Administratively Reset.)
```

R2

```
#sh ip bgp neighbors
BGP neighbor is 100.100.100.1, remote AS 1, local AS 2, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  BGP state = Established, up for 00:00:35
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 6 messages, 1 notifications, 0 in queue
  Sent 7 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
  External BGP neighbor may be up to 255 hops away.
Local host: 200.200.200.1, Local port: 179
Foreign host: 100.100.100.1, Foreign port: 57260
Nexthop: 200.200.200.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:40, due to BGP Notification received
Notification Error Message: (Cease/Administratively Reset.)

#show ip bgp
BGP table version is 4, local router ID is 192.168.52.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   100.100.100.0/24 1.1.1.1              0         100           32768    ?

Total number of prefixes 1
```

Enable Peer Groups

A BGP speaker might have the same update policies for a set of its peers. This is very useful if you have to change the update policies for all of the peers: Changing individual routers for separate policies can be very time-consuming, thus, peer groups play an important role in creating and assigning policies to a group of routers.

The peer group can be created dynamically or statically.

For dynamic peer groups all configuration can be done at group level only.

The static peer group configuration falls into two categories:

- Attributes that can be configured only at group level. Attempt to configure at member peer level will return error.
- Attributes that allow member peer level configuration. The member peer configuration has precedence.

Category A: Neighbor configuration allowed only at peer-group level

The outbound update impacting configurations of peer group will replace peer member configurations of same attributes when a peer becomes member of peer group. Outbound attribute modifications to group members are not allowed.

Following are the commands which are allowed at peer-group level.

- neighbor WORD activate - neighbor activate
- neighbor WORD as-origination-interval <1-65535> - neighbor as-origination-interval
- neighbor WORD attribute-unchanged ({as-path|next-hop|med}|) - neighbor attribute-unchanged
- neighbor WORD fall-over bfd - neighbor fall-over bfd
- neighbor WORD fall-over bfd multihop - neighbor enforce-multihop
- neighbor WORD next-hop-self - neighbor next-hop-self
- neighbor WORD remove-private-AS - neighbor remove-private-AS
- neighbor WORD route-reflector-client - neighbor route-reflector-client
- neighbor WORD route-server-client - neighbor route-server-client
- neighbor WORD send-community - neighbor send-community
- neighbor WORD distribute-list WORD out - neighbor distribute-list
- neighbor WORD dont-capability-negotiate - neighbor dont-capability-negotiate
- neighbor WORD capability orf prefix-list (both|receive|send) - neighbor capability orf prefix-list
- neighbor WORD filter-list WORD out - neighbor filter-list
- neighbor WORD prefix-list WORD out - neighbor prefix-list
- neighbor WORD route-map WORD out - neighbor restart-time
- neighbor WORD advertisement-interval <1-65535> - neighbor advertisement-interval
- neighbor WORD disallow-infinite-holdtime - neighbor disallow-infinite-holdtime
- neighbor WORD local-as <1-4294967295> - neighbor local-as

Category: Neighbor configuration allowed at peer-group member level; precedence based

For the below configuration, member level configurations will take precedence over peer group configuration.

Following are the commands which are allowed at member level also.

- neighbor WORD authentication-key WORD - neighbor authentication-key

© 2021 IP Infusion Inc. Proprietary

- neighbor WORD remote-as <1-4294967295> - neighbor remote-as
- neighbor WORD allowas-in <1-10> - neighbor allowas-in
- neighbor WORD description WORD - neighbor description
- neighbor WORD distribute-list WORD In - neighbor distribute-list
- neighbor WORD ebgp-multihop - neighbor ebgp-multihop
- neighbor WORD ebgp-multihop <1-255> - neighbor ebgp-multihop
- neighbor WORD maximum-prefix <1-4294967295> - neighbor maximum-prefix
- neighbor WORD update-source WORD - neighbor update-source
- neighbor WORD weight <0-65535> - neighbor weight
- neighbor WORD soft-reconfiguration inbound - neighbor soft-reconfiguration inbound
- neighbor WORD shutdown - neighbor shutdown
- neighbor WORD strict-capability-match - neighbor strict-capability-match
- neighbor WORD route-map WORD in - neighbor restart-time
- neighbor WORD prefix-list WORD in - neighbor prefix-list
- neighbor WORD passive - neighbor passive
- neighbor WORD override-capability - neighbor override-capability
- neighbor WORD filter-list WORD in - neighbor filter-list
- neighbor WORD enforce-multihop - neighbor enforce-multihop
- neighbor WORD collide-established - neighbor collide-established

BGP Peer Groups for Address-Family IPv4 Unicast

In the following scenario, R1, R2, and R3 belong to the same peer group ABC. R1, R2 and R3 are in AS 200 and R1 is the route reflector.R4 and R1 are eBGP peers. R4 is in AS 100.

Topology

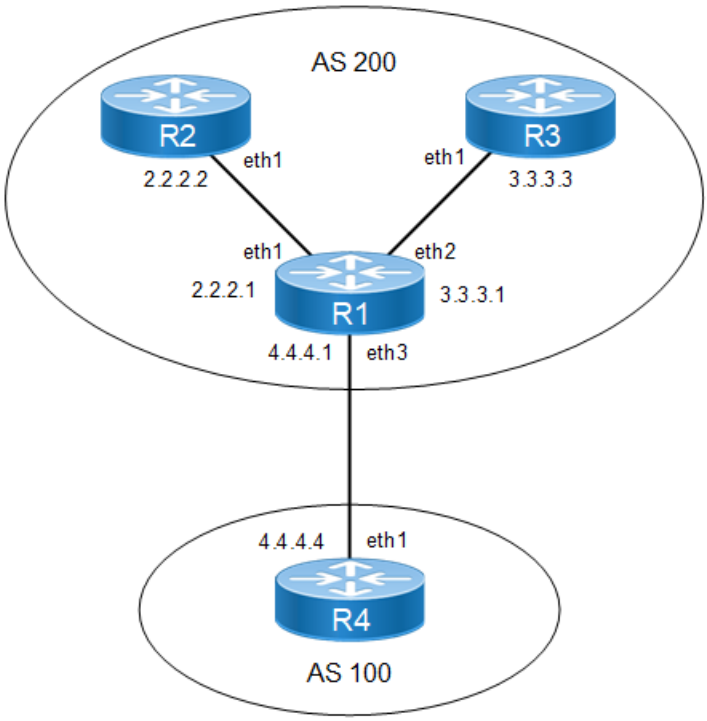


Figure 9-154: BGP Peer Groups with IPv4 Unicast Members

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number 200 specifies the AS number of R2.
`OcNOS(config-router)#neighbor ABC peer-group`	Configuring ABC peer-group
`(config-router)#neighbor ABC remote-as 200`	Assign options to the peer group named ABC.
`(config-router)#neighbor 2.2.2.2 peer-group ABC`	Define neighbor 2.2.2.2 (R2) as a peer group member.
`(config-router)#neighbor 3.3.3.3 peer-group ABC`	Define neighbor 3.3.3.3 (R3) as a peer group member.
`(config-router)#neighbor 4.4.4.4 remote-as 100`	Define neighbor 4.4.4.4 (R4) is the IP address of R4 and 100 is the AS number.
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor ABC activate`	Activate neighbor under address family mode
`(config-router-af)# neighbor 4.4.4.4 activate`	Activate neighbor under address family mode
`(config-router-af)# neighbor ABC route-reflector-client`	Configure the peer-group ABC to be route-reflector-client
`(config-router-af)#network 1.1.1.1/32`	Advertise the network 1.1.1.1/32
`(config-router-af)#network 11.11.11.11/32`	Advertise the network 11.11.11.11/32

© 2021 IP Infusion Inc. Proprietary

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number 200 specifies the AS number of R2.
`(config-router)#neighbor 2.2.2.1 remote-as 200`	Create a TCP connection with neighbor 2.2.2.1 of AS 200.
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 2.2.2.1 activate`	Activate neighbor under address family mode
`OcNOS(config-router-af)#exit-address-family`	Exit address family mode

R3

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Define the routing process. The number 200 specifies the AS number of R3.
`(config-router)#neighbor 3.3.3.1 remote-as 200`	Create a TCP connection with neighbor 3.3.3.1 of AS 200.
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 3.3.3.1 activate`	Activate neighbor under address family mode
`OcNOS(config-router-af)#exit-address-family`	Exit address family mode

R4

`#configure terminal`	Enter configure mode.
`(config)#router bgp 100`	Define the routing process. The number 100 specifies the AS number of R4.
`(config-router)#neighbor 4.4.4.1 remote-as 200`	Create a TCP connection with neighbor 4.4.4.1 of AS 200.
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 4.4.4.1 activate`	Activate neighbor under address family mode
`(config-router-af)#exit-address-family`	Exit address family mode

Validation

R1

```
R1#show ip bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 192.168.52.2, remote router ID 10.12.7.155
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
```

```
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes
 Connections established 1; dropped 0
Local host: 2.2.2.1, Local port: 33865
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: 1111::1
Nexthop local: fe80::a00:27ff:fecc:47a6
BGP connection: non shared network

BGP neighbor is 3.3.3.3, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 192.168.52.2, remote router ID 10.12.7.153
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes
 Connections established 1; dropped 0
Local host: 3.3.3.1, Local port: 44280
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 3.3.3.1
Nexthop global: fe80::a00:27ff:fe85:25d4
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 4.4.4.4, remote AS 100, local AS 200, external link
  BGP version 4, remote router ID 10.12.7.120
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
```


© 2021 IP Infusion Inc. Proprietary

```
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 3, Offset 0, Mask 0x8
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes
 Connections established 1; dropped 0
Local host: 4.4.4.1, Local port: 55493
Foreign host: 4.4.4.4, Foreign port: 179 Nexthop: 4.4.4.1
Nexthop global: fe80::a00:27ff:fe7e:674a
Nexthop local: ::
BGP connection: non shared network

R1#show ip bgp summary
BGP router identifier 192.168.52.2, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
2.2.2.2                  4   200   12         12       1      0      0
00:05:02               0
3.3.3.3                  4   200   12         12       1      0      0
00:05:02               0
4.4.4.4                  4   100   12         12       1      0      0
00:05:02               0
Total number of neighbors 3
Total number of Established sessions 3
```

R2

```
R2#show ip bgp
BGP table version is 4, local router ID is 10.12.65.123
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  1.1.1.1/32       2.2.2.1               0         100           0        i
*>i  11.11.11.11/32   2.2.2.1               0         100           0        i

Total number of prefixes 2
R2#
```

R3

```
R3#show ip bgp
BGP table version is 8, local router ID is 10.12.65.121
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
```

```
*>i  1.1.1.1/32       3.3.3.1              0         100           0        i
*>i  11.11.11.11/32   3.3.3.1              0         100           0        i

Total number of prefixes 2
R3#
```

Peer-group can have either iBGP or eBGP peers but not both.

Validation

The configuration above fails with an appropriate error:

```
R1(config)#router bgp 200
R1(config-router)#neighbor 4.4.4.4 peer-group ABC
%% Peer with AS 100 cannot be in this peer-group, members must be all internal
or all external
R1(config-router)#
```

Peer group members inherit the properties of Outbound Policies configured for Peer-group.

R1

`#configure terminal`	Enter configure mode.
`(config)# ip access-list permit-1`	Configure access-list to permit 1.1.1.1/32
`(config-ip-acl)# permit any 1.1.1.1/32 any`	Configure a permit statement in the acl to permit 1.1.1.1/32
`(config-ip-acl)#exit`	Exit ip access-list mode
`(config)# route-map permit-only-1`	Configure route-map
`(config-route-map)# match ip address permit-1`	Configure a match statement in the route-map to match the access-list permit-1
`(config-route-map)#set local-preference 250`	Set local preference as 250
`(config-route-map)#exit`	Exit route-map mode
`(config)#router bgp 200`	Define the routing process. The number 200 specifies the AS number of R1.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor ABC route-map permit-only-1  out`	Configure the peer-group ABC with route-map in the outbound direction
`(config-router-af)#exit`	Exit router BGP mode
`(config-router)#exit`	Exit router mode.
`(config# exit`	Exit configure terminal mode
`#clear ip bgp peer-group ABC soft out`	Do outbound soft reset for the peer-group ABC for the policy to take affect for the peer-group members

Validation

R1

```
R1#show bgp neighbors 2.2.2.2
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.123
```


© 2021 IP Infusion Inc. Proprietary

```
  BGP state = Established, up for 00:07:01
  Last read 00:00:15, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 20 messages, 0 notifications, 0 in queue
  Sent 28 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  Outbound path policy configured
  Route map for outgoing advertisements is *permit-only-1
  0 accepted prefixes
  1 announced prefixes

 Connections established 2; dropped 1
Local host: 2.2.2.1, Local port: 179
Foreign host: 2.2.2.2, Foreign port: 42657
Nexthop: 2.2.2.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:08:39, due to Hold Timer Expired (Notification sent)
Notification Error Message: (Hold Timer Expired/No sub-error code)

R1#show bgp neighbors 3.3.3.3
BGP neighbor is 3.3.3.3, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.121
  BGP state = Established, up for 00:11:46
  Last read 00:00:18, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 29 messages, 0 notifications, 0 in queue
  Sent 32 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  Outbound path policy configured
  Route map for outgoing advertisements is *permit-only-1
  0 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 3.3.3.1, Local port: 179
Foreign host: 3.3.3.3, Foreign port: 48008
```

```
Nexthop: 3.3.3.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

R2

```
R2#show ip bgp
BGP table version is 3, local router ID is 10.12.65.123
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  1.1.1.1/32       2.2.2.1               0         250           0        i

Total number of prefixes 1
```

R3

```
R3#show ip bgp
BGP table version is 7, local router ID is 10.12.65.121
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  1.1.1.1/32       3.3.3.1               0         250           0        i

Total number of prefixes 1
```

Peer-group-members cannot be configured with Outbound Policies.

Validation

The above configuration fails with an appropriate error:

```
R1(config)#router bgp 200
R1(config)#address-family ipv4 unicast
R1(config-router-af)#neighbor 2.2.2.2 route-map permit-only-11 out
%% Invalid command for a peer-group member
```

Peer-group-members inherit the properties of Inbound Policies configured for Peer-group.

R2

`#configure terminal`	Enter configure mode.
`(config)# interface lo`	Enter interface mode for Loopback interface
`(config-if)#ip address 100.1.1.1/24 secondary`	Configure IP address for Loopback interaface
`(config-if)#interface eth3`	Enter interface mode for interface eth3
`(config-if)#ip address 22.1.1.1/24`	Configure IP address for interface eth3
`(config-if)#exit`	Exit interface mode

© 2021 IP Infusion Inc. Proprietary

(config)#router bgp 200	Enter router bgp mode
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#network 22.1.1.0/24	Advertise the network of eth3 in BGP
(config-router-af)#network 100.1.1.0/24	Advertise the network of Loopback in BGP
(config-router-af)#exit-address-family	Exit router bgp mode

R3

#configure terminal	Enter configure mode.
(config)# interface lo	Enter interface mode for Loopback interface
(config-if)#ip address 100.1.1.2/24 secondary	Configure IP address for Loopback interaface
(config-if)#interface eth3	Enter interface mode for interface eth3
(config-if)#ip address 22.1.1.2/24	Configure IP address for interface eth3
(config-if)#exit	Exit interface mode
(config)#router bgp 200	Enter router bgp mode
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#network 22.1.1.0/24	Advertise the network of eth3 in BGP
(config-router-af)#network 100.1.1.0/24	Advertise the network of Loopback in BGP
(config-router-af)#exit	Exit router bgp mode

R1

#configure terminal	Enter configure mode.
(config)#ip access-list permit-22	Configure access-list to permit 22.1.1.0/24
(config-ip-acl)# permit any 22.1.1.0/24 any	Configure a permit statement to permit 22.1.1.0/24
(config-ip-acl)#exit	Exit ip access-list mode
(config)#route-map permit-only-22	Configure route-map
(config-route-map)#match ip address permit-22	Configure match statement in route-map to match the access-list permit-22
(config-route-map)#exit	Exit route-map mode
(config)#router bgp 200	Enter BGP router mode
(config)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor ABC activate	Activate peer-group in the address family
(config-router-af)#neighbor ABC route-map permit-only-22 in	Configure the peer-group ABC with route-map in the inbound direction
(config-router)#exit	Exit router bgp mode
(config)# exit	Exit configure terminal mode
#clear ip bgp peer-group ABC soft in	Do inbound soft reset for the peer-group ABC for the policy to take affect for the peer-group members

© 2021 IP Infusion Inc. Proprietary

Validation

R1

```
R1#show ip bgp

BGP table version is 7, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, a add-path, g group-best, *
valid, > best, i - internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network             Next Hop             Metric        LocPrf
Weight  Path
*>   1.1.1.1/32          0.0.0.0              0             100          32768
i
*>   11.11.11.11/32      0.0.0.0              0             100          32768
i
*>i  22.1.1.0/24         2.2.2.2              0             100          0
i
* i                      3.3.3.3              0             100          0
i

Total number of prefixes 3
```

Peer group members can be configured with Inbound Policies

R1

`#configure terminal`	Enter configure mode.
`(config)#ip access-list permit-100`	Configure access-list to permit 100.1.1.0/24
`(config-ip-acl)# permit any 100.1.1.0/24 any`	Configure a permit statement to permit 100.1.1.0/24
`(config-ip-acl)#exit`	Exit ip access-list mode
`(config)#route-map permit-only-100`	Configure route-map
`(config-route-map)#match ip address permit-100`	Configure match statement in route-map to match the access-list permit-100
`(config-route-map)#exit`	Exit route-map mode
`(config)#router bgp 200`	Enter BGP router mode
`(config)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 2.2.2.2 activate`	Activate neighbor in the address family
`(config-router-af)#neighbor 2.2.2.2 route-map permit-only-100 in`	Configure the peer-group-member R2(2.2.2.2) with route-map in the inbound direction
`(config-router-af)#exit`	Exit address-family mode
`(config-router)#exit`	Exit router bgp mode
`(config)# exit`	Exit configure terminal mode
`#clear ip bgp peer-group ABC soft in`	Do inbound soft reset for the peer-group ABC for the policy to take affect for the peer-group members

© 2021 IP Infusion Inc. Proprietary

Validation

R1

```
R1#show ip bgp
BGP table version is 4, local router ID is 10.12.65.126
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   1.1.1.1/32       0.0.0.0               0         100           32768    i
*>   11.11.11.11/32   0.0.0.0               0         100           32768    i
*>i  22.1.1.0/24      3.3.3.3               0         100           0        i
*>i  100.1.1.0/24     2.2.2.2               0         100           0        i

Total number of prefixes 4
R1#
```

Route Redistribution in BGP

If there are routers that run both OSPF and BGP, certain OSPF routes might have to be sent to other eBGP peers. This can be achieved using the redistribution feature. Consider the following topology, in which R1 and R2 are eBGP peers, and R2 and R3 are OSPF peers. R2 is redistributing OSPF routes into BGP. The OSPF routes are sent to the R1 BGP routing table. This configuration assumes that all OSPF and eBGP sessions are up and running, and that only the redistribution must be configured.

Topology

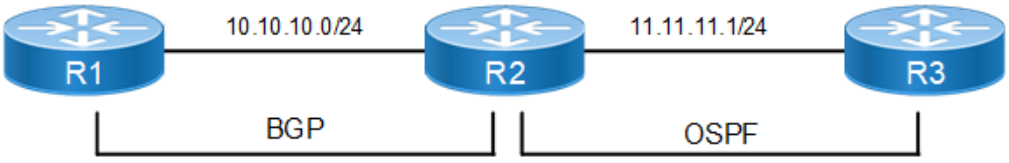


Figure 9-155: Redistribute with OSPF

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 100`	Define the routing process. The number `100` specifies the AS number of R2.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#redistribute ospf`	Redistribute OSPF routes in the R2 routing table into the R1 BGP routing table.
`(config-router-af)# exit-address-family`	Exit address-family mode.

Validation

```
#show ip bgp
```

```
BGP table version is 3, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric     LocPrf       Weight Path
*>   3.3.3.3/32       10.10.10.2            11        100            0       100
?
*>   11.11.11.0/24    10.10.10.2            1         100            0       100
?

Total number of prefixes 2
```

Add Multiple Instances of the Same Autonomous System

BGP supports adding the same AS number multiple times to influence the route selection process. This can be done using route maps, as described below.

Under normal circumstances, any route advertised by R1 is sent to R4 via two different routes, and then R4 selects the path from R2. This decision can be influenced by adding multiple instances of AS number 200 at R2.

Topology

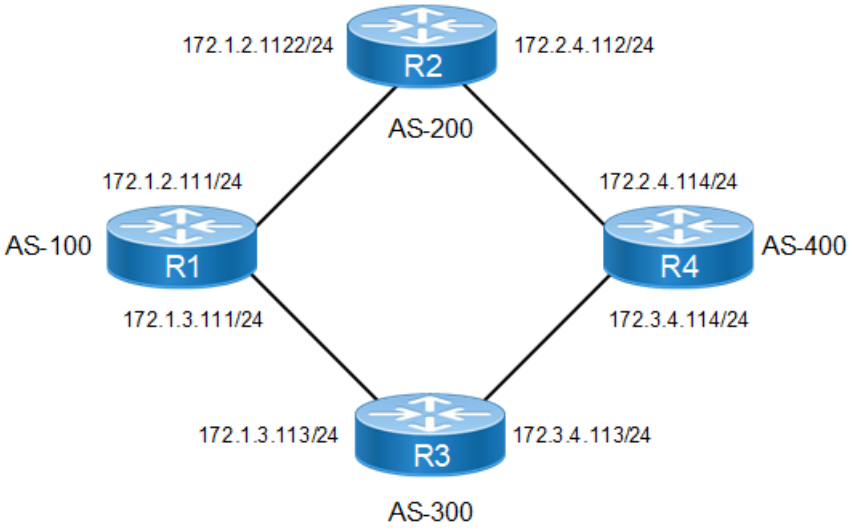


Figure 9-156: Multiple Instances of Same AS

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 44.44.44.1/24 secondary`	Specify the IP address for the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 100`	Define the routing process with AS number 100.
`(config-router)#neighbor 172.1.2.112 remote-`	

© 2021 IP Infusion Inc. Proprietary

as 200	Define neighbor R2. 172.1.2.112 is the IP address of R2, and 200 is the AS number.
(config-router)#neighbor 172.1.3.113 remote-	
as 300	Define neighbor R3. 172.1.3.113 is the IP address of R2, and 300 is the AS number.
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 172.1.2.112 activate	Activate neighbor under address family mode
(config-router-af)# neighbor 172.1.2.113 activate	Activate neighbor under address family mode
(config-router-af)#network 44.44.44.0/24	Advertise network 44.44.44.0/24 through BGP. This route reaches R4 via R2 and R3.

R2

#configure terminal	Enter configure mode.
(config)#route-map mul_inst permit 10	Define the route-map multiple instance with permit definition sequence number 10.
(config-route-map)#set as-path prepend 200 200	Prepend AS number 200 two times to the AS_PATH attribute in the BGP Update message.
(config-route-map)#exit	Exit Route-map mode, and return to Configure mode.
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 172.1.2.111 remote-as 100	Define neighbor R1. 172.1.2.111 is the IP address of R1, and 100 is the AS number.
(config-router)#neighbor 172.2.4.114 remote-as 400	Define neighbor R4. 172.2.4.114 is the IP address of R2, and 400 is the AS number.
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 172.2.4.114 activate	Activate neighbor under address family mode
(config-router-af)# neighbor 172.1.2.111 activate	Activate neighbor under address family mode
(config-router-af)#neighbor 172.2.4.114 route-map mul_inst out	Apply route-map multi_inst to all outbound routes to R4

R3

#configure terminal	Enter configure mode.
(config)#router bgp 300	Define the routing process with AS number 300.
(config-router)#neighbor 172.1.3.111 remote-as 100	Define neighbor R1. 172.1.3.111 is the IP address of R1, and 100 is the AS number.
(config-router)#neighbor 172.3.4.114 remote-as 400	Define neighbor R4. 172.3.4.114 is the IP address of R4, and 400 is the AS number.
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 172.3.4.114 activate	Activate neighbor under address family mode
(config-router-af)# neighbor 172.1.3.111 activate	Activate neighbor under address family mode

R4

`#configure terminal`	Enter configure mode.
`(config)#router bgp 400`	Define the routing process with AS number 400.
`(config-router)#neighbor 172.2.4.112 remote-as 200`	Define neighbor R2. 172.2.4.112 is the IP address of R2, and 200 is the AS number.
`(config-router)#neighbor 172.3.4.113 remote-as 300`	Define neighbor R3. 172.3.4.113 is the IP address of R3, and 300 is the AS number.
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 172.2.4.112 activate`	Activate neighbor under address family mode
`(config-router-af)# neighbor 172.3.4.113 activate`	Activate neighbor under address family mode

Validation

```
#show ip bgp
BGP table version is 1, local router ID is 44.44.44.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*> 44.44.44.0/24 0.0.0.0 0 100 32768 i

Total number of prefixes 1
```

Remove the Multi-Exit Disc Attribute from Update Messages

You can remove the Multi-Exit Disc (MED) attribute values from received update messages.

Topology



Figure 9-157: Remove MED Attribute

R1

`#configure terminal`	Enter configure mode.
`(config)#route-map med permit 1`	Define the route-map MED with permit definition sequence number 1.
`(config-route-map)#set metric 400`	Set the metric value.
`(config-route-map)#exit`	Exit Route-map mode, and return to Configure mode.
`(config)#router bgp 100`	Define the routing process with AS number 100.

© 2021 IP Infusion Inc. Proprietary

(config-router)#neighbor 1.1.1.2 remote-as 200	Define neighbor R2. 1.1.1.2 is the IP address of R2, and 200 is the AS number.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 1.1.1.2 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode
(config-router)#exit	Exit router BGP mode
(config)#interface xe2	Enter interface mode
(config-if)#ip ad 10.10.10.1/24	Assign IP address
(config-if)#no shutdown	Make interface administratively up
(config-if)#exit	Exit interface mode
(config)#ip route 100.0.0.0/8 10.10.10.2	Configure the static route with the nexthop address.

R3

#configure terminal	Enter configure mode.
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 2.2.2.1 remote-as 200	Define neighbor R2. 2.2.2.1 is the IP address of R2, and 200 is the AS number.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 2.2.2.1 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode

Removing Sent and Received MED values

The following describes how to remove the received and sent MED values, respectively.

R2 - Remove Received MED Value

#configure terminal	Enter configure mode.
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 1.1.1.1 remote-as 100	Define neighbor R1. 1.1.1.1 is the IP address of R1, and 100 is the AS number.
(config-router)#neighbor 2.2.2.2 remote-as 200	Define neighbor R3. 2.2.2.2 is the IP address of R3, and 200 is the AS number.
(config-router)#bgp bestpath med remove-recv- med	Enable the remove received MED value option.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 1.1.1.1 activate	Activate neighbor under address family mode
(config-router-af)# neighbor 2.2.2.2 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode

R1 - Add Static Route

(config)#router bgp 100	Enter to router bgp mode
(config)#address-family ipv4 unicast	Config redistribute under address-family
(config-router-af)#redistribute static	Redistribute the static routes

R2 - Remove Send MED Value

#configure terminal	Enter configure mode.
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 1.1.1.1 remote-as 100	Define neighbor R1. 1.1.1.1 is the IP address of R1, and 100 is the AS number.
(config-router)#neighbor 2.2.2.2 remote-as 200	Define neighbor R3. 2.2.2.2 is the IP address of R3, and 200 is the AS number.
(config-router)#bgp bestpath med remove-send- med	Enable the remove sent MED value option.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 1.1.1.1 activate	Activate neighbor under address family mode
(config-router-af)# neighbor 2.2.2.2 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode

Validation

```
R2#show ip bgp
BGP table version is 2, local router ID is 192.168.52.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   100.0.0.0        1.1.1.1          removed     100           0       100 ?

Total number of prefixes 1


R3#show ip bgp
BGP table version is 1, local router ID is 192.168.52.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
* i  100.0.0.0        1.1.1.1              400       100           0       100 ?

Total number of prefixes 1
```


© 2021 IP Infusion Inc. Proprietary

BGP Four-Byte Autonomous System

Extended AS numbers can be mapped to 2-byte AS numbers if the value is less than, or equal to, 65535. If the AS number is higher than 65535, it cannot be mapped to a 2-byte AS number. Therefore, if a BGP speaker is configured with a non-mappable AS number, it must enable the BGP extended ASN capability in OcNOS.

Note: Autonomous System number 23456 is a reserved IANA number for AS transition; thus, it is recommended that no system be configured with 23456 as its AS number.

The extended ASN capability is disabled by default. However, when it is enabled, it is able to interoperate with a 2-byte AS-numbered speaker, in compliance with RFC 4893.

If a 4-byte AS number is configured in the provider's network using BGP MPLS VPN or standard IPv4/IPv6 BGP, it is recommended that the PE routers be 4-byte AS-enabled before connecting to 4-byte AS-enabled customer networks. For implications related to AS number transition issues, refer to RFC 4893.

You can also set up 4-byte AS-specific extended communities and route distinguishers (RDs) with limited capabilities. However, it is recommended that 2-byte AS-specific RDs and extended communities be used for regular deployment.

BGP encodes an ASN into four octets, so that more autonomous systems can be supported. Extended ASN capability is advertised in the Open message capabilities when the 4-octet ASN capability is enabled. When the 4-octet ASN capability is enabled, the valid ASN value range is <1-4294967295>, with the exception discussed in the first Note, above.

Note: Four-octet capability is disabled by default.

4-Octet ASN Capability Enabled on R1 and R2

In this example, 4-Octet ASN capability is enabled on BGP speakers R1 and R2.

Topology



Figure 9-158: 4-Octet ASN on Both Routers

R1

`#configure terminal`	Enter configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 400000`	Assign the ASN value (400000) to the router.
`(config-router)#neighbor 10.20.30.2 remote-as 7000`	Specify the neighbor's IP address (10.20.30.2) and the ASN value of the neighbor (7000).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode

`(config-router-af)# neighbor 10.20.30.2 activate`	Activate neighbor under address family mode
`(config-router-af)# exit-address-family`	Exit address family mode

R2

`#configure terminal`	Enter configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 7000`	Assign the ASN value (7000) to the router.
`(config-router)#neighbor 10.20.30.1 remote-as 400000`	Specify the neighbor's IP address (10.20.30.1) and the ASN value of the neighbor (400000).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.20.30.1 activate`	Activate neighbor under address family mode
`(config-router-af)# exit-address-family`	Exit address family mode

4-Octet ASN Capability Enabled on R1 and Disabled on R2

In the following two examples, 4-Octet ASN capability is enabled on BGP speaker R1 and disabled on R2.

Topology

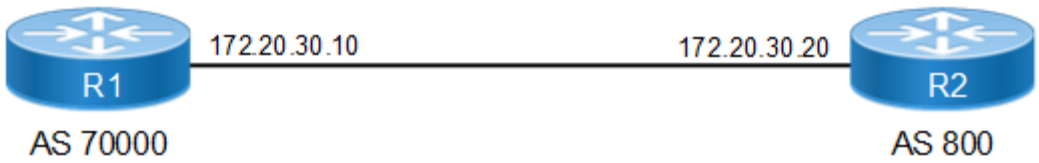


Figure 9-159: 4-Octet ASN on One Router

R1

`#configure terminal`	Enter configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 70000`	Assign the ASN value (70000) to the router.
`(config-router)#neighbor 172.20.30.20 remote-as 800`	Specify the neighbor's IP address (172.20.30.20) and the ASN value of the neighbor (800).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 172.20.30.20 activate`	Activate neighbor under address family mode
`(config-router-af)# exit-address-family`	Exit address family mode

R2

`#configure terminal`	Enter configure mode.
`(config)#no bgp extended-asn-cap`	Disable 4-octet ASN capability.

© 2021 IP Infusion Inc. Proprietary

(config)#router bgp 800	Assign the ASN value (800) to the router.
(config-router)#neighbor 172.20.30.10 remote-as 70000	Specify the neighbor's IP address (172.20.30.10) and the ASN value of the neighbor (70000).
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 172.20.30.10 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode

Topology

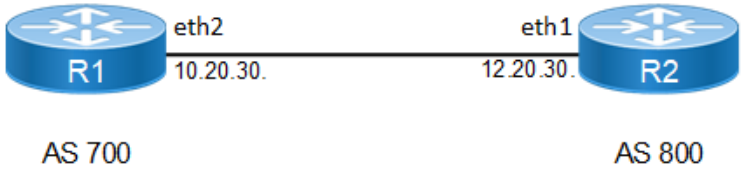


Figure 9-160: 4-Octet ASN

R1

#configure terminal	Enter configure mode.
(config)#bgp extended-asn-cap	Enable 4-octet ASN capability.
(config)#router bgp 700	Assign the ASN value (700) to the router.
(config-router)#neighbor 172.20.30.20 remote-as 800	Specify the neighbor's IP address (172.20.30.20) and the ASN value of the neighbor (800).
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 172.20.30.20 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode

R2

#configure terminal	Enter configure mode.
(config)#no bgp extended-asn-cap	Disable 4-octet ASN capability.
(config)#router bgp 800	Assign the ASN value (800) to the router.
(config-router)#neighbor 172.20.30.10 remote-as 700	Specify the neighbor's IP address (172.20.30.10) and the ASN value of the neighbor (700).
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 172.20.30.10 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode

Validation

```
#show ip bgp summary
BGP router identifier 192.168.52.2, local AS number 400000
BGP table version is 1
```

© 2021 IP Infusion Inc. Proprietary

```
    0 BGP AS-PATH entries
    0 BGP community entries

    Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
    Down   State/PfxRcd
    10.20.30.2               4  7000    2          3       1      0      0
    00:00:08              0

    Total number of neighbors 1

    Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 10.20.30.1, remote AS 400000, local AS 7000, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  BGP state = Established, up for 00:02:20
  Last read 00:00:20, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 6 messages, 0 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.20.30.2, Local port: 49434
Foreign host: 10.20.30.1, Foreign port: 179
Nexthop: 10.20.30.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

BGP Extended Community Attribute

The Extended Community Attribute provides a mechanism for labeling information carried in BGP.

Extended Community with a 2-Byte ASN

In the following example, CE1, PE1, PE2, and CE2 are 2-byte-ASN capable, and do not support 4-byte-ASN capability.

© 2021 IP Infusion Inc. Proprietary

Topology

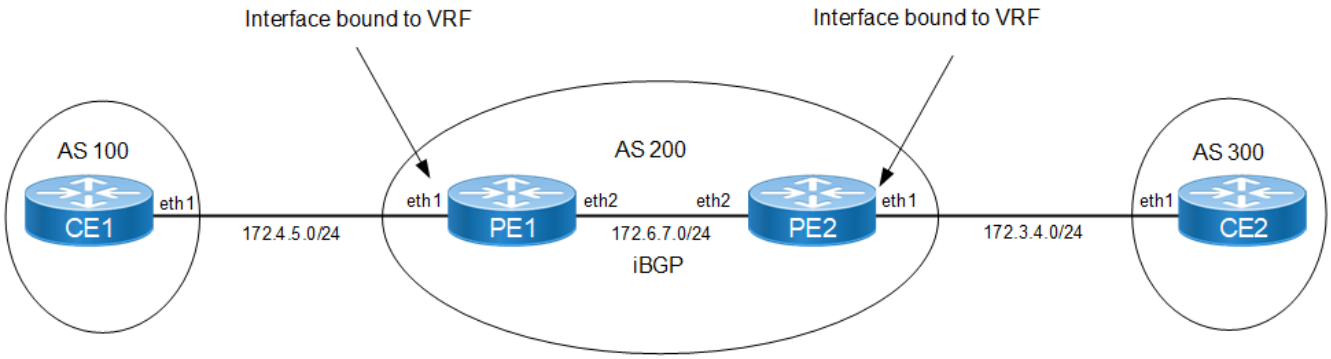


Figure 9-161: Extended Communities — 2-Byte ASN

CE1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 172.4.5.115/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 172.4.5.116 remote-as 200`	Specify the neighbor's IP address (172.4.5.116) and the ASN value of the neighbor (200).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 172.4.5.116 activate`	Activate neighbor under address family mode
`(config-router-af)# exit-address-family`	Exit address family mode

CE2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 172.3.4.114/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 300`	Assign the ASN value (300) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 172.3.4.117 remote-as 200`	Specify the neighbor's IP address (172.3.4.117) and the ASN value of the neighbor (200).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 172.3.4.117 activate`	Activate neighbor under address family mode
`(config-router-af)# exit-address-family`	Exit address family mode

© 2021 IP Infusion Inc. Proprietary

PE1

`#configure terminal`	Enter configure mode.
`(config)#ip vrf VRF1`	Specify the name of the VRF (`VRF1`) to be created.
`(config-vrf)#rd 100:10`	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
`(config-vrf)#route-target both 100:10`	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
`(config-vrf)#exit`	Exit VRF mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip vrf forwarding VRF1`	Bind the interface (eth1) to the VRF (`VRF1`).
`(config-if)#ip address 172.4.5.116/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#ip route vrf VRF1 75.1.1.0/24 eth1`	Create a VRF static route.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 172.6.7.116/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#neighbor 172.6.7.117 remote-as 200`	Specify the neighbor's (PE2) IP address (`172.6.7.117`) and the ASN value of the neighbor (`200`). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
`(config-router)#address-family vpnv4 unicast`	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
`(config-router-af)#neighbor 172.6.7.117 activate`	Activate the neighbor in address-family
`(config-router-af)#exit`	Exit Address-Family-VPNv4 mode.
`(config-router)#address-family ipv4 vrf VRF1`	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
`(config-router-af)#neighbor 172.4.5.115 remote-as 100`	Specify the neighbor's (CE1) IP address and ASN value.
`(config-router-af)#neighbor 172.4.5.115 activate`	Activate the neighbor in address-family
`(config-router-af)#neighbor 172.4.5.115 send-community both`	Enable extended community attribute for the neighbor.
`(config-router-af)#redistribute static`	Configure static redistribution.
`(config-router-af)#end`	Exit Address-Family mode

PE2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf VRF1`	Specify the name of the VRF (VRF1) tobe created.
`(config-vrf)#rd 100:10`	Assign a route distinguisher (RD) for the VRF.

© 2021 IP Infusion Inc. Proprietary

(config-vrf)#route-target both 100:10	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip vrf forwarding VRF1	Bind the interface (eth1) to the VRF (VRF1).
(config-if)#ip address 172.3.4.117/24	Configure the IP address on this interface
(config-if)#exit	Exit interface mode.
(config)#ip route vrf VRF1 100.1.1.0/24 eth1	Create a VRF static route.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 172.6.7.117/24	Configure the IP address on this interface
(config-if)#exit	Exit interface mode.
(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#neighbor 172.6.7.116 remote-as 200	Specify the neighbor's (PE1) IP address (172.6.7.116) and the ASN value of the neighbor (200). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
(config-router)#address-family vpnv4 unicast	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 172.6.7.116 activate	Enable the exchange of routing information with a peer router.
(config-router-af)#exit	Exit Address-Family-VPNv4 mode.
(config-router)#address-family ipv4 vrf VRF1	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
(config-router-af)#neighbor 172.3.4.114	
remote-as 300	Specify the neighbor's (CE2) IP address and ASN value.
(config-router-af)# neighbor 17.3.4.114 activate	Activate the neighbor in address family mode
(config-router-af)#neighbor 172.3.4.114 send- community both	Enable extended community attribute for the neighbor.
(config-router-af)#redistribute static	Configure static redistribution.
(config-router-af)#end	Exit Address-Family mode

Validation

CE1

```
#show running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management


!
ip domain-lookup feature telnet feature ssh
snmp-server enable snmp
```

```
snmp-server view all .1 included feature ntp
ntp enable
username ocnos role network-admin password encrypted $1$AUeGhbf0$HCHhxemCQ39LPYOjC.Kb7/
feature rsyslog
!
interface lo
ip address 127.0.0.1/8 ipv6 address ::1/128 mtu 65536
!
interface eth0
ip address 192.168.52.2/24
!
interface eth1
ip address 172.4.5.115/24
!
interface eth2 shutdown
!
interface eth3 shutdown
!
interface eth4 shutdown
!
interface eth5 shutdown
!
router bgp 100
neighbor 172.4.5.116 remote-as 200
!
 address-family ipv4 unicast
 neighbor 172.4.5.116 activate
 exit-address-family
!
line con 0 login
line vty 0 39 login
!
end

#
#show ip bgp
BGP table version is 8, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete



   NetworkNext HopMetricLocPrfWeightPath
*> 75.1.1.0/24172.4.5.11601000200?
*> 100.1.1.0/24172.4.5.11601000200?

Total number of prefixes 2 #
#show ip bgp neighbors
BGP neighbor is 172.4.5.116, remote AS 200, local AS 100, external link
```

 © 2021 IP Infusion Inc. Proprietary

```
BGP version 4, local router ID 192.168.52.2, remote router ID 172.4.5.116 BGP state =
Established, up for 00:04:22
Last read 00:00:22, hold time is 90, keepalive interval is 30 seconds Neighbor
capabilities:
Route refresh: advertised and received (old and new) Address family IPv4 Unicast:
advertised and received
Received 131 messages, 1 notifications, 0 in queue
Sent 129 messages, 0 notifications, 0 in queue Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 30 seconds For address family: IPv4 Unicast
BGP table version 8, neighbor version 8 Index 1, Offset 0, Mask 0x2
Community attribute sent to this neighbor (both)
2 accepted prefixes
0 announced prefixes

Connections established 2; dropped 1
Local host: 172.4.5.115, Local port: 179
Foreign host: 172.4.5.116, Foreign port: 37982
Nexthop: 172.4.5.115 Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:04:54, due to BGP Notification received Notification Error Message:
(Cease/Peer Unconfigured.)



#show ip bgp vrf all
BGP table version is 8, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   NetworkNext HopMetricLocPrfWeightPath
*> 75.1.1.0/24172.4.5.11601000200 ?
*> 100.1.1.0/24172.4.5.11601000200 ?

Total number of prefixes 2 #



#show ip bgp summary vrf all
BGP router identifier 192.168.52.2, local AS number 100 BGP table version is 8
1 BGP AS-PATH entries
0 BGP community entries

NeighborVASMsgRcvMsgSen TblVerInQOutQUp/DownState/ PfxRcd
172.4.5.116420016816580 0   00:22:04
2

Total number of neighbors 1

Total number of Established sessions 1
```

PE1

```
#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 100:10 (Default for VRF VRF1)
*>   75.1.1.0/24      0.0.0.0             0         100           32768    ?
*>i  100.1.1.0/24     172.6.7.117          0         100           0        ?
 Announced routes count = 1
 Accepted routes count = 1
Route Distinguisher: 100:10
*>i  100.1.1.0/24     172.6.7.117          0         100           0        ?
 Announced routes count = 0
 Accepted routes count = 1


#show ip bgp vrf all
BGP table version is 2, local router ID is 172.4.5.116
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path

BGP Route Table for VRF VRF1
*>   75.1.1.0/24      0.0.0.0             0         100           32768    ?
*>i  100.1.1.0/24     172.6.7.117          0         100           0        ?

Total number of prefixes 2


#show ip bgp summary vrf all
BGP router identifier 172.4.5.116, local AS number 200
BGP VRF VRF1 Route Distinguisher: 100:10
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.4.5.115             4   100   55        60      2      0      0  00:26:54
0

Total number of neighbors 1

Total number of Established sessions 1
BGP router identifier 192.168.52.3, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
```


© 2021 IP Infusion Inc. Proprietary

```
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.6.7.117             4   200   80       101      1      0      0  00:37:47
0

Total number of neighbors 1

Total number of Established sessions 1


#show ip bgp neighbors
BGP neighbor is 172.6.7.117, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.5
  BGP state = Established, up for 00:38:33
  Last read 00:00:03, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Received 82 messages, 0 notifications, 0 in queue
  Sent 103 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: VPNv4 Unicast
  BGP table version 4, neighbor version 4
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 172.6.7.116, Local port: 179
Foreign host: 172.6.7.117, Foreign port: 57743
Nexthop: 172.6.7.116
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 172.4.5.115, vrf VRF1, remote AS 100, local AS 200, external link
  BGP version 4, local router ID 172.4.5.116, remote router ID 192.168.52.2
  BGP state = Established, up for 00:27:40
  Last read 00:00:10, hold time is 90, keepalive interval is 30 seconds
```

```
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 57 messages, 0 notifications, 0 in queue
  Sent 62 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 Connections established 1; dropped 0
Local host: 172.4.5.116, Local port: 37982
Foreign host: 172.4.5.115, Foreign port: 179
Nexthop: 172.4.5.116
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip bgp vrf all
BGP table version is 2, local router ID is 172.4.5.116
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path

BGP Route Table for VRF VRF1
*>   75.1.1.0/24      0.0.0.0             0         100           32768    ?
*>i  100.1.1.0/24     172.6.7.117          0         100           0        ?

Total number of prefixes 2
```

PE2

```
#show ip bgp vrf all
BGP table version is 1, local router ID is 172.3.4.117
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path

BGP Route Table for VRF VRF1
*>i  75.1.1.0/24      172.6.7.116          0         100           0        ?
*>   100.1.1.0/24     0.0.0.0             0         100           32768    ?
```


© 2021 IP Infusion Inc. Proprietary

```
Total number of prefixes 2


#show ip bgp summary vrf all
BGP router identifier 172.3.4.117, local AS number 200
BGP VRF VRF1 Route Distinguisher: 100:10
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.3.4.114             4   300   82        85      1      0      0  00:40:05
0

Total number of neighbors 1

Total number of Established sessions 1
BGP router identifier 192.168.52.5, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.6.7.116             4   200  113       113      1      0      0  00:54:07
0

Total number of neighbors 1

Total number of Established sessions 1#


#show ip bgp neighbors
BGP neighbor is 172.6.7.116, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 192.168.52.5, remote router ID 192.168.52.3
  BGP state = Established, up for 00:56:09
  Last read 00:00:09, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Received 117 messages, 0 notifications, 0 in queue
  Sent 117 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
```

```
  0 accepted prefixes
  0 announced prefixes

 For address family: VPNv4 Unicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 172.6.7.117, Local port: 57743
Foreign host: 172.6.7.116, Foreign port: 179
Nexthop: 172.6.7.117
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 172.3.4.114, vrf VRF1, remote AS 300, local AS 200, external link
  BGP version 4, local router ID 172.3.4.117, remote router ID 192.168.52.4
  BGP state = Established, up for 00:42:07
  Last read 00:00:07, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 86 messages, 0 notifications, 0 in queue
  Sent 89 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 Connections established 1; dropped 0
Local host: 172.3.4.117, Local port: 54753
Foreign host: 172.3.4.114, Foreign port: 179
Nexthop: 172.3.4.117
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

CE2

```
    #show ip bgp vpnv4 all
    #show ip bgp
    BGP table version is 3, local router ID is 192.168.52.4
    Status codes: s suppressed, d damped, h history, * valid, > best, i -
    internal,
                  l - labeled, S Stale
```


© 2021 IP Infusion Inc. Proprietary

```
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   75.1.1.0/24      172.3.4.117           0         100           0       200
?
*>   100.1.1.0/24     172.3.4.117           0         100           0       200
?

Total number of prefixes 2
#
#
#show ip bgp vrf all
BGP table version is 3, local router ID is 192.168.52.4
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   75.1.1.0/24      172.3.4.117           0         100           0       200
?
*>   100.1.1.0/24     172.3.4.117           0         100           0       200
?

Total number of prefixes 2
#
#
#show ip bgp summary vrf all
BGP router identifier 192.168.52.4, local AS number 300
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
172.3.4.117              4   200  382        414       3      0      0
00:42:54              2

Total number of neighbors 1

Total number of Established sessions 1
#
#
#show ip bgp neighbors
BGP neighbor is 172.3.4.117, remote AS 200, local AS 300, external link
  BGP version 4, local router ID 192.168.52.4, remote router ID 172.3.4.117
  BGP state = Established, up for 00:43:04
  Last read 00:00:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 236 messages, 147 notifications, 0 in queue
  Sent 415 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
```

```
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 172.3.4.114, Local port: 179
Foreign host: 172.3.4.117, Foreign port: 54753
Nexthop: 172.3.4.114
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:43:32, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad Peer AS.)

#
```


© 2021 IP Infusion Inc. Proprietary

Extended Community with a 4-Byte ASN

In the following example, CE1, PE1, PE2, and CE2 support 4-byte ASN capability.

Note: PE1 and PE2 should both either be 4-byte-ASN capable or 2-byte-ASN capable. Support for the combination of one 4-byte-ASN capable PE with one 2-byte-ASN-capable PE is currently unavailable.

Topology

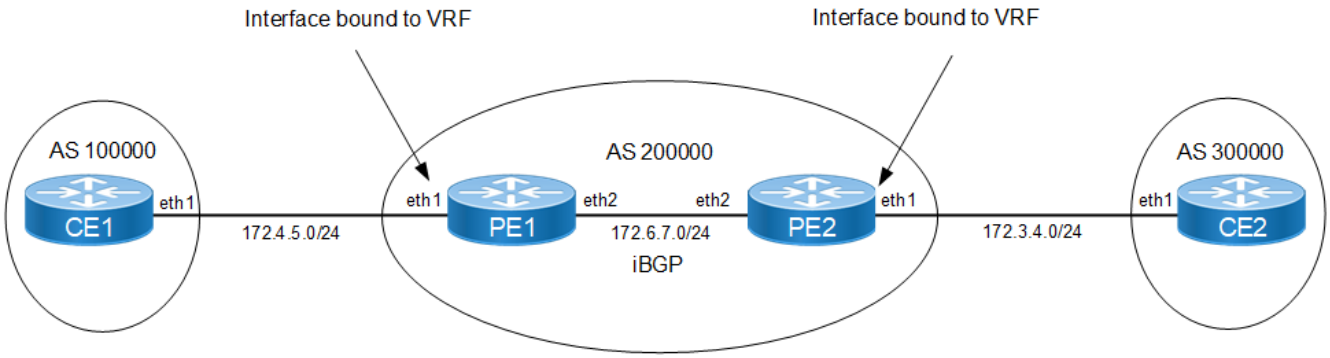


Figure 9-162: Extended Communities — 4-Byte ASN

CE1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 172.4.5.115/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 100000`	Assign the ASN value (100000) to the router. The ASN range is <1-4294967295>.
`(config-router)#neighbor 172.4.5.116 remote-as 200000`	Specify the neighbor's IP address (172.4.5.116) and the ASN value of the neighbor (200000).
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 172.4.5.116 activate`	Activate neighbor under address family mode
`(config-router-af)# exit-address-family`	Exit address family mode

PE1

`#configure terminal`	Enter configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability. Dynamic change from 2- byte to 4-byte capability, or vice versa, is not allowed, unless the VRF is removed.
`(config)#ip vrf VRF1`	Specify the name of the VRF (VRF1) to be created.
`(config-vrf)#rd 1.1.1.1:200`	Assign a 4-byte route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in A.B.C.D:NN format.

`(config-vrf)#route-target both 1.1.1.1:200`	Specify the 4-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
`(config-vrf)#exit`	Exit VRF mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip vrf forwarding VRF1`	Bind the interface (eth1) to the VRF (VRF1).
`(config-if)#ip address 172.4.5.116/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#ip route vrf VRF1 50.1.1.0/24 eth1`	Create a VRF static route.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 172.6.7.116/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200000`	Assign the ASN value (200000) to the router.
`(config-router)#neighbor 172.6.7.117 remote-as 200000`	Specify the neighbor's (PE2) IP address (172.6.7.117) and the ASN value of the neighbor (200000). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
`(config-router)#address-family vpnv4 unicast`	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
`(config-router-af)#neighbor 172.6.7.117 activate`	Enable the exchange of routing information with a peer router.
`(config-router-af)#exit`	Exit Address-Family-VPNv4 mode.
`(config-router)#address-family ipv4 vrf VRF1`	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
`(config-router-af)#neighbor 172.4.5.115`	
`remote-as 100000`	Specify the neighbor's (CE1) IP address and ASN value.
`(config-router-af)# neighbor 172.4.5.115 activate`	Activate neighbor in address family mode
`(config-router-af)#neighbor 172.4.5.115 send- community both`	Enable extended community attribute for the neighbor.
`(config-router-af)#redistribute static`	Configure static redistribution.
`(config-router-af)#end`	Exit Address-Family mode

PE2

`#configure terminal`	Enter configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability. Dynamic change from 2- byte to 4-byte capability, or vice versa, is not allowed, unless the VRF is removed.
`(config)#ip vrf VRF1`	Specify the name of the VRF (VRF1) to be created.
`(config-vrf)#rd 1.1.1.1:200`	Assign a 4-byte route distinguisher (RD) for the VRF.
`(config-vrf)#route-target both 1.1.1.1:200`	Specify the 4-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
`(config-vrf)#exit`	Exit VRF mode, and return to Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip vrf forwarding VRF1`	Bind the interface (eth1) to the VRF (VRF1).
`(config-if)#ip address 172.3.4.117/24`	Configure the IP address on this interface

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit interface mode.
(config)#ip route vrf VRF1 200.1.1.0/24 eth1	Create a VRF static route.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 172.6.7.117/24	Configure the IP address on this interface
(config-if)#exit	Exit interface mode.
(config)#router bgp 200000	Assign the ASN value (200000) to the router.
(config-router)#neighbor 172.6.7.116 remote-as 200000	Specify the neighbor's (PE2) IP address (172.6.7.116) and the ASN value of the neighbor (200000). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
(config-router)#address-family vpnv4 unicast	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 172.6.7.116 activate	Enable the exchange of routing information with a peer router.
(config-router-af)#exit	Exit Address-Family-VPNv4 mode.
(config-router)#address-family ipv4 vrf VRF1	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
(config-router-af)#neighbor 172.3.4.114	
remote-as 300000	Specify the neighbor's (CE1) IP address and ASN value.
(config-router-af)# neighbor 172.3.4.114 activate	Activate neighbor under address family mode
(config-router-af)#neighbor 172.3.4.114 send- community both	Enable extended community attribute for the neighbor.
(config-router-af)#redistribute static	Configure static redistribution.
(config-router-af)#end	Exit Address-Family mode

CE2

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 172.3.4.114/24	Configure the IP address on this interface
(config-if)#exit	Exit interface mode.
(config)#bgp extended-asn-cap	Enable 4-octet ASN capability.
(config)#router bgp 300000	Assign the ASN value (300000) to the router.
(config-router)#neighbor 172.3.4.117 remote-as 200000	Specify the neighbor's IP address (172.3.4.117) and the ASN value of the neighbor (200000).
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 172.3.4.117 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode

Validation

CE1

```
#show ip bgp neighbors
BGP neighbor is 172.4.5.116, remote AS 200000, local AS 100000, external link
```

```
  BGP version 4, local router ID 192.168.52.2, remote router ID 172.4.5.116
  BGP state = Established, up for 00:20:35
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 45 messages, 0 notifications, 0 in queue
  Sent 47 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 172.4.5.115, Local port: 179
Foreign host: 172.4.5.116, Foreign port: 58251
Nexthop: 172.4.5.115
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip bgp vrf all
BGP table version is 3, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   50.1.1.0/24      172.4.5.116           0         100           0       200000 ?
*>   200.1.1.0        172.4.5.116           0         100           0       200000 ?

Total number of prefixes 2


#show ip bgp summary vrf all
BGP router identifier 192.168.52.2, local AS number 100000
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.4.5.116            4 200000   46        48      3     0     0  00:21:12
2

Total number of neighbors 1
```

 © 2021 IP Infusion Inc. Proprietary

```
Total number of Established sessions 1
```

PE1

```
#show ip bgp neighbors
BGP neighbor is 172.4.5.116, remote AS 200000, local AS 100000, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 172.4.5.116
  BGP state = Established, up for 00:20:35
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 45 messages, 0 notifications, 0 in queue
  Sent 47 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 172.4.5.115, Local port: 179
Foreign host: 172.4.5.116, Foreign port: 58251
Nexthop: 172.4.5.115
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network


#show ip bgp vrf all
BGP table version is 3, local router ID is 192.168.52.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   50.1.1.0/24      172.4.5.116           0         100           0       200000 ?
*>   200.1.1.0        172.4.5.116           0         100           0       200000 ?

Total number of prefixes 2

#show ip bgp summary vrf all
BGP router identifier 192.168.52.2, local AS number 100000
BGP table version is 3
1 BGP AS-PATH entries
```

```
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.4.5.116              4 200000   46        48      3     0     0  00:21:12
2

Total number of neighbors 1

Total number of Established sessions 1


#clear bgp *
2019 Mar 22 06:16:56.414 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]: Neighbour
[172.4.5.116] Session down due to peer clear
```

PE2

```
#show ip bgp neighbors
BGP neighbor is 172.4.5.116, remote AS 200000, local AS 100000, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 172.4.5.116
  BGP state = Established, up for 00:20:35
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 45 messages, 0 notifications, 0 in queue
  Sent 47 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 172.4.5.115, Local port: 179
Foreign host: 172.4.5.116, Foreign port: 58251
Nexthop: 172.4.5.115
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network


#show ip bgp vrf all
BGP table version is 1, local router ID is 172.3.4.117
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```


© 2021 IP Infusion Inc. Proprietary

```
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path

BGP Route Table for VRF VRF1
*>i  50.1.1.0/24      172.6.7.116          0         100           0        ?
*>   200.1.1.0        0.0.0.0              0         100           32768    ?

Total number of prefixes 2


#show ip bgp summary vrf all
BGP router identifier 192.168.52.2, local AS number 100000
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.4.5.116            4 200000   46        48      3     0     0  00:21:12
2

Total number of neighbors 1

Total number of Established sessions 1


#clear bgp *
2019 Mar 22 06:16:56.414 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]: Neighbour
[172.4.5.116] Session down due to peer clear
```

CE2

```
#show ip bgp vrf all
BGP table version is 4, local router ID is 192.168.52.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   50.1.1.0/24      172.3.4.117          0         100           0       200000 ?
*>   200.1.1.0        172.3.4.117          0         100           0       200000 ?

Total number of prefixes 2


#show ip bgp summary vrf all
BGP router identifier 192.168.52.4, local AS number 300000
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
172.3.4.117              4 200000   33        30      4     0     0  00:04:34
2

Total number of neighbors 1

Total number of Established sessions 1


#show ip bgp neighbors
BGP neighbor is 172.3.4.117, remote AS 200000, local AS 300000, external link
  BGP version 4, local router ID 192.168.52.4, remote router ID 172.3.4.117
  BGP state = Established, up for 00:04:40
  Last read 00:00:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 33 messages, 0 notifications, 0 in queue
  Sent 29 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 4, neighbor version 4
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 172.3.4.114, Local port: 179
Foreign host: 172.3.4.117, Foreign port: 49361
Nexthop: 172.3.4.114
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:04:40, due to BGP Notification sent
Notification Error Message: (Cease/Administratively Reset.)
```

Nexthop Tracking

Nexthop tracking is used to notify the BGP process asynchronously whenever there is any change in the IGP routes. It reduces the convergence time of BGP routes when IGP routes are changed.

© 2021 IP Infusion Inc. Proprietary

Topology

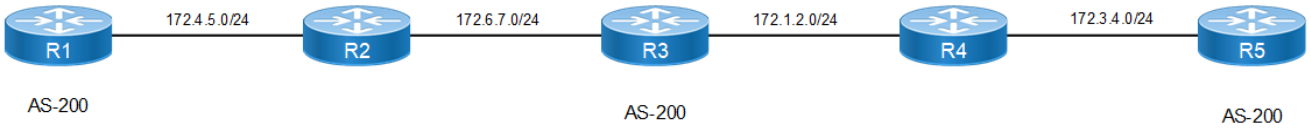


Figure 9-163: BGP Nexthop Tracking

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 100.100.100.100/32 secondary`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 200.200.200.200 remote-as 200`	Specify the neighbor's IP address (200.200.200.200) and the ASN value of the neighbor (200).
`(config-router)#neighbor 200.200.200.200 update-source lo`	Specify the routing update source.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 200.200.200.200 activate`	Activate neighbor under address family mode
`(config-router-af)# exit-address-family`	Exit address family mode
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 1`	Configure the OSPF process (1).
`(config-router)#network 172.4.5.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#redistribute connected`	Redistribute the connected routes.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure the OSPF process (1).
`(config-router)#network 172.4.5.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#network 172.6.7.0/24 area 0`	Advertise the network in Area 0.

R3

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if) #ip address 150.150.150.150/32 secondary`	Configure the IP address on this interface.
`(config-if)#ip address 200.200.200.200/32 secondary`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#neighbor 100.100.100.100 remote-as 200	Specify the neighbor's IP address (100.100.100.100) and the ASN value of the neighbor (200).
(config-router)#neighbor 100.100.100.100 update-source 200.200.200.200	Specify the routing update source.
(config-router)#neighbor 220.220.220.220 remote-as 200	Specify the neighbor's IP address (220.220.220.220) and the ASN value of the neighbor (200).
(config-router)#neighbor 220.220.220.220 update-source 150.150.150.150	Specify the routing update source.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 100.100.100.100 activate	Activate neighbor under address family mode
(config-router-af)# neighbor 220.220.220.220 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.6.7.0/24 area 0	Advertise the network in Area 0.
(config-router)#network 172.1.2.0/24 area 0	Advertise the network in Area 0.
(config-router)#redistribute connected	Redistribute the connected routes.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#bgp nexthop-trigger enable	Enable Nexthop tracking.
(config)#bgp nexthop-trigger delay 20	Configure the nexthop trigger-delay time interval.

R4

#configure terminal	Enter configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.1.2.0/24 area 0	Advertise the network in Area 0.
(config-router)#network 172.3.4.0/24 area 0	Advertise the network in Area 0.

R5

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the loopback interface, and enter Interface mode.
(config-if)#ip address 220.220.220.220/32 secondary	Configure the IP address on this interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#neighbor 150.150.150.150 remote-as 200	Specify the neighbor's IP address (150.150.150.150) and the ASN value of the neighbor (200).
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 150.150.150.150 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode

© 2021 IP Infusion Inc. Proprietary

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 220.220.220.220/32 secondary`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config-router)#neighbor 150.150.150.150 update-source lo`	Specify the routing update source.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 1`	Configure the OSPF process (1).
`(config-router)#network 172.3.4.0/24 area 0`	Advertise the network in Area 0.
`(config-router)#redistribute connected`	Redistribute the connected routes.

Validation

show ip bgp summary, show ip bgp neighbors, show bgp nexthop-tracking, show ip bgp scan

Nexthop Tracking Delay Timer

The delay interval between routing table walks can be configured for nexthop delay tracking. This time determines how long BGP waits before it starts walking the full BGP routing table after receiving notification from NSM about a next-hop change.

Topology

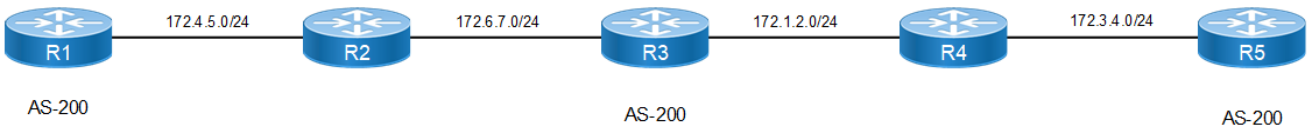


Figure 9-164: Topology for Nexthop Tracking Delay Timer

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 150.150.150.150/32 secondary`	Configure the IP address on this interface.
`(config-if)#ip address 100.100.100.100/32 secondary`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 200.200.200.200 remote-as 200`	Specify the neighbor's IP address (200.200.200.200) and the ASN value of the neighbor (200).
`(config-router)#neighbor 200.200.200.200 update-source lo`	Specify the routing update source.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode

(config-router-af)# neighbor 200.200.200.200 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode
#configure terminal	Enter configure mode.
(config)#interface lo	Specify the loopback interface, and enter Interface mode.
(config-if)#ip address 150.150.150.150/32 secondary	Configure the IP address on this interface.
(config-if)#ip address 100.100.100.100/32 secondary	Configure the IP address on this interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.4.5.0/24 area 0	Advertise the network in Area 0.
(config-router)#redistribute connected	Redistribute the connected routes.

R2

#configure terminal	Enter configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.4.5.0/24 area 0	Advertise the network in Area 0.
(config-router)#network 172.6.7.0/24 area 0	Advertise the network in Area 0.

R3

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the loopback interface, and enter Interface mode.
(config-if)#ip address 200.200.200.200/32	Configure the IP address on this interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#neighbor 100.100.100.100 remote-as 200	Specify the neighbor's IP address (100.100.100.100) and the ASN value of the neighbor (200).
(config-router)#neighbor 100.100.100.100 update-source 200.200.200.200	Specify the routing update source.
(config-router)#neighbor 220.220.220.220 remote-as 200	Specify the neighbor's IP address (220.220.220.220) and the ASN value of the neighbor (200).
(config-router)#neighbor 220.220.220.220 update-source 150.150.150.150	Specify the routing update source.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 100.100.100.100 activate	Activate neighbor under address family mode
(config-router-af)# neighbor 220.220.220.220 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.6.7.0/24 area 0	Advertise the network in Area 0.

© 2021 IP Infusion Inc. Proprietary

(config-router)#network 172.1.2.0/24 area 0	Advertise the network in Area 0.
(config-router)#redistribute connected	Redistribute the connected routes.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#bgp nexthop-trigger enable	Enable nexthop tracking.
(config)#bgp nexthop-trigger delay 20	Configure the nexthop trigger-delay time interval.

R4

#configure terminal	Enter configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.1.2.0/24 area 0	Advertise the network in Area 0.
(config-router)#network 172.3.4.0/24 area 0	Advertise the network in Area 0.

R5

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the loopback interface, and enter Interface mode.
(config-if)#ip address 220.220.220.220/32	Configure the IP address on this interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#neighbor 150.150.150.150 remote-as 200	Specify the neighbor's IP address (150.150.150.150) and the ASN value of the neighbor (200).
(config-router)#neighbor 150.150.150.150 update-source lo	Specify the routing update source.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 150.150.150.150 activate	Activate neighbor under address family mode
(config-router-af)# exit-address-family	Exit address family mode
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.3.4.0/24 area 0	Advertise the network in Area 0.
(config-router)#redistribute connected	Redistribute the connected routes.

Validation

R1

```
#show ip bgp summary
BGP router identifier 10.12.20.71, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
200.200.200.200          4   200   15         16       1      0      0
00:06:37              0
```

```
Total number of neighbors 1

Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 200.200.200.200, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 10.12.20.71, remote router ID 200.200.200.200
  BGP state = Established, up for 00:06:40
  Last read 00:06:40, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 15 messages, 0 notifications, 0 in queue
  Sent 16 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 100.100.100.100, Local port: 37676
Foreign host: 200.200.200.200, Foreign port: 179
Nexthop: 100.100.100.100
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show bgp nexthop-tracking
Configured NHT: DISABLED
NHT Delay time-interval : 5
BGP VRF: (Default) VRF_ID 0
BGP Instance: (Default), AS: 200, router-id 10.12.20.71

#show ip bgp scan
BGP VRF: (Default) VRF_ID 0
BGP scan interval is 60
scan remain-time: 38
Current BGP nexthop cache:
```

R3

```
#show ip bgp summary
BGP router identifier 200.200.200.200, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
100.100.100.100          4   200   17         19       1      0      0
00:07:41              0
```


© 2021 IP Infusion Inc. Proprietary

```
220.220.220.220          4   200   95        101       1      0      0
00:07:12              0

Total number of neighbors 2

Total number of Established sessions 2

#show ip bgp neighbors
BGP neighbor is 100.100.100.100, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 200.200.200.200, remote router ID 10.12.20.71
  BGP state = Established, up for 00:07:46
  Last read 00:07:46, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 17 messages, 0 notifications, 0 in queue
  Sent 19 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is 200.200.200.200
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 200.200.200.200, Local port: 179
Foreign host: 100.100.100.100, Foreign port: 37676
Nexthop: 200.200.200.200
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 220.220.220.220, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 220.220.220.220
  local router ID 200.200.200.200
  BGP state = Established, up for 00:07:17
  Last read 00:07:17, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 94 messages, 1 notifications, 0 in queue
  Sent 97 messages, 4 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is 150.150.150.150
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 6; dropped 5
Local host: 150.150.150.150, Local port: 39831
```

```
Foreign host: 220.220.220.220, Foreign port: 179
Nexthop: 150.150.150.150
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:07:22, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

#show bgp nexthop-tracking
Configured NHT: ENABLED
NHT Delay time-interval : 20
BGP VRF: (Default) VRF_ID 0
BGP Instance: (Default), AS: 200, router-id 200.200.200.200
NHT is Enabled
Recvd Msg count from RIB: 0
NHT delay-timer remaining seconds: 0
BGP nexthop(s):
Total number of IPV4 nexthops : 0
Total number of IPV6 nexthops : 0

#show ip bgp scan
BGP VRF: (Default) VRF_ID 0
BGP scan interval is 60
scan remain-time: 11
Current BGP nexthop cache:
```

R5

```
#show ip bgp summary
BGP router identifier 220.220.220.220, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
150.150.150.150          4   200   99        101       1      0      0
00:08:26              0

Total number of neighbors 1

Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 150.150.150.150, remote AS 200, local AS 200, internal link
  BGP version 4, local router ID 220.220.220.220, remote router ID
200.200.200.200
  BGP state = Established, up for 00:08:29
  Last read 00:08:29, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 96 messages, 3 notifications, 0 in queue
  Sent 99 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
```

 © 2021 IP Infusion Inc. Proprietary

```
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 6; dropped 5
Local host: 220.220.220.220, Local port: 179
Foreign host: 150.150.150.150, Foreign port: 39831
Nexthop: 220.220.220.220
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:08:34, due to BGP Notification sent
Notification Error Message: (Cease/Other Configuration Change.)

#show bgp nexthop-tracking
Configured NHT: DISABLED
NHT Delay time-interval : 5
BGP VRF: (Default) VRF_ID 0
BGP Instance: (Default), AS: 200, router-id 220.220.220.220

#show ip bgp scan
BGP VRF: (Default) VRF_ID 0
BGP scan interval is 60
scan remain-time: 22
Current BGP nexthop cache:
```

BGP Distance

Administrative distance in BGP can be configured for a specific address family.

Topology

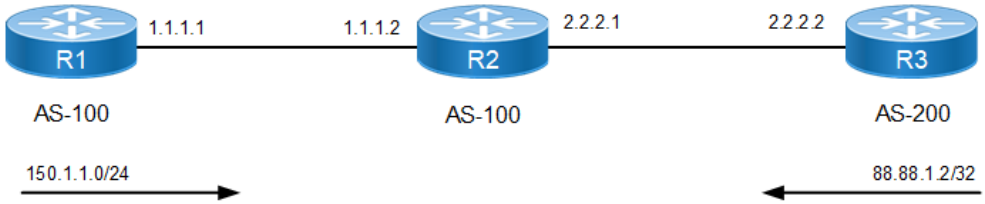


Figure 9-165: Administrative Distance for IPv4 BGP

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 150.1.1.1/24 secondary`	Specify IP address for the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the router.

(config-router)#neighbor 1.1.1.2 remote-as 100	Specify the neighbor's IP address and ASN value.
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#neighbor 1.1.1.2 activate	Activate the neighbor in address family mode
(config-router-af)#network 150.1.1.0/24	Specify the network to be advertised by the BGP routing process.
(config-router-af)#exit-address-family	Exit address-family ipv4 unicast mode

R2

#configure terminal	Enter configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the router.
(config-router)#neighbor 2.2.2.2 remote-as 200	Specify the neighbor's IP address and ASN value.
(config-router)#neighbor 1.1.1.1 remote-as 100	Specify the neighbor's IP address and the ASN value of another neighbor.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#distance bgp 12 13 120	Configure the administrative distance for external, internal, and local routes received.
(config-router-af)#aggregate-address 150.1.0.0/16 summary-only	Configure a non-AS-set aggregate route on R2. The local distance is applied to this route.
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor in address family mode
(config-router-af)#neighbor 2.2.2.2 activate	Activate the neighbor in address family mode
(config-router-af)#exit-address-family	Exit address-family ipv4 unicast mode

R3

#configure terminal	Enter configure mode.
(config)#interface lo	Enter loopback interface mode.
(config-if)#ip address 88.88.1.2/32 secondary	Specify IP address for the interface.
(config-if)#exit	Exit loopback interface mode.
(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#neighbor 2.2.2.1 remote-as 100	Specify the neighbor's IP address and ASN value.
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#network 88.88.1.2/32	Specify the network to be advertised by the BGP routing process.
(config-router-af)#neighbor 2.2.2.1 activate	Activate the neighbor in address family mode
(config-router-af)#exit-address-family	Exitr address-family ipv4 unicast mode

Validation

```
#show ip bgp summary
BGP router identifier 192.168.56.102, local AS number 100
BGP table version is 7
2 BGP AS-PATH entries
```


© 2021 IP Infusion Inc. Proprietary

```
0 BGP community entries

Neighbor                  V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
1.1.1.1                   4   100    8          9       7      0      0
00:02:39               1
2.2.2.2                   4   200    4          4       7      0      0
00:00:38               1

Total number of neighbors 2

Total number of Established sessions 2
#show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 192.168.52.3, remote router ID 150.1.1.1
  BGP state = Established, up for 00:02:54
  Last read 00:02:54, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 8 messages, 0 notifications, 0 in queue
  Sent 9 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 7, neighbor version 7
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.2, Local port: 49238
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 1.1.1.2
Nexthop global: fe80::a00:27ff:fea6:6e3
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 2.2.2.2, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 88.88.1.2
  local router ID 192.168.52.3
  BGP state = Established, up for 00:00:53
  Last read 00:00:53, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 7, neighbor version 7
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes
```

```
 Connections established 1; dropped 0
Local host: 2.2.2.1, Local port: 179
Foreign host: 2.2.2.2, Foreign port: 50072
Nexthop: 2.2.2.1
Nexthop global: fe80::a00:27ff:fe77:264e
Nexthop local: ::
BGP connection: non shared network

#show ip route database bgp
IP Route Table for VRF "default"
B    *> 88.88.1.2/32 [12/0] via 2.2.2.2, eth2, 00:01:19
B    *> 150.1.0.0/16 [120/0] is a summary, Null, 00:02:49
B    *> 150.1.1.0/24 [200/0] via 1.1.1.1, eth1, 00:02:49

Gateway of last resort is not set
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
C    *>  1.1.1.0/24 is directly connected, eth1, 00:13:39
C    *>  2.2.2.0/24 is directly connected, eth3, 00:13:04
B    *>  88.88.1.2/32 [12/0] via 2.2.2.2, eth3, 00:06:37
C    *>  127.0.0.0/8 is directly connected, lo, 00:22:15
B    *>  150.1.0.0/16 [120/0] is a summary, Null, 00:11:19
B    *>  150.1.1.0/24 [200/0] via 1.1.1.1, eth1, 00:11:19
C    *>  192.168.52.0/24 is directly connected, eth0, 00:22:13

Gateway of last resort is not set

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     1.1.1.0/24 is directly connected, eth1, 00:17:38
C     2.2.2.0/24 is directly connected, eth3, 00:17:03
B     88.88.1.2/32 [12/0] via 2.2.2.2, eth3, 00:10:36
C     127.0.0.0/8 is directly connected, lo, 00:26:14
B     150.1.0.0/16 [120/0] is a summary, Null, 00:15:18
B     150.1.1.0/24 [200/0] via 1.1.1.1, eth1, 00:15:18
C     192.168.52.0/24 is directly connected, eth0, 00:26:12

Gateway of last resort is not set
```


© 2021 IP Infusion Inc. Proprietary

```
#show ip bgp
BGP table version is 4, local router ID is 192.168.52.3
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric     LocPrf       Weight Path
*>   88.88.1.2/32     2.2.2.2               0         100            0       200
i
*>   150.1.0.0        0.0.0.0               0         100            32768    i
s>i  150.1.1.0/24     1.1.1.1               0         100            0         i

Total number of prefixes 3
```

BGP Weight per Peer

A different weight can be assigned per address family of a peer. For example, a system can be configured to prefer VPN4 routes from peer A and IPv4 routes from peer B.

If the neighbor weight command is given under a specific address-family mode, the peer weight is set for that specific address family. If the address family is not specifically set, the weight is updated for the default address-family.

Topology

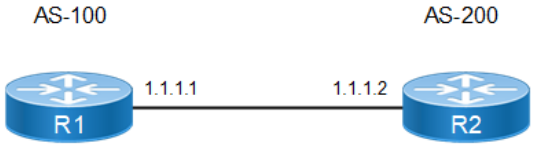


Figure 9-166: BGP Weight Per Peer

R1

`#configure terminal`	Enter configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the router.
`(config-router)#neighbor 1.1.1.2 remote-as 200`	Specify the neighbor's IP address and ASN value.
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#neighbor 1.1.1.2 activate`	Activate the neighbor in address family mode
`(config-router-af)#exit-address-family`	Exit address-family ipv4 unicast mode

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the router.
`(config-router)#neighbor 1.1.1.1 remote-as 100`	Specify the neighbor's IP address and ASN value.

`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#neighbor 1.1.1.1 weight 500`	Add a weight of 500 to all the routes coming from the neighbor, 1.1.1.1 (only IPv4 routes).
`(config-router-af)#neighbor 1.1.1.1 activate`	Activate the neighbor in address family mode
`(config-router-af)#exit-address-family`	Exit address-family ipv4 unicast mode

Validation

R1

```
#show ip bgp summary
BGP router identifier 192.168.56.101, local AS number 100
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
Neighbor V AS MsgRcv MsgSen TblVer InQ OutQ Up/Dow
n State/PfxRcd
1.1.1.2 4 200 6 7 1 0 0 00:02:00
0
Total number of neighbors 1
Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 1.1.1.2, remote AS 200, local AS 100, external link
  BGP version 4, local router ID 192.168.52.2, remote router ID 192.168.52.3
  BGP state = Established, up for 00:01:17
  Last read 00:00:17, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 5 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.1, Local port: 179
Foreign host: 1.1.1.2, Foreign port: 34619
Nexthop: 1.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
```


© 2021 IP Infusion Inc. Proprietary

```
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     1.1.1.0/24 is directly connected, eth1, 00:09:10
C     127.0.0.0/8 is directly connected, lo, 00:15:56
C     192.168.52.0/24 is directly connected, eth0, 00:15:52

Gateway of last resort is not set
```

R2

```
#show ip bgp summary
BGP router identifier 192.168.56.102, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
Neighbor V AS MsgRcv MsgSen TblVer InQ OutQ Up/Dow
n State/PfxRcd
1.1.1.1 4 100 3 3 1 0 0 00:00:34
0
Total number of neighbors 1
Total number of Established sessions 1


#show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 200, external link
  BGP version 4, local router ID 192.168.52.3, remote router ID 192.168.52.2
  BGP state = Established, up for 00:07:14
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 16 messages, 0 notifications, 0 in queue
  Sent 16 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
 Weight500
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.2, Local port: 34619
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 1.1.1.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

```
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
          ia - IS-IS inter area, E - EVPN,
          v - vrf leaked
          * - candidate default

    IP Route Table for VRF "default"
    C     1.1.1.0/24 is directly connected, eth1, 00:11:26
    C     127.0.0.0/8 is directly connected, lo, 00:21:36
    C     192.168.52.0/24 is directly connected, eth0, 00:21:32

    Gateway of last resort is not set
```

OSPF as PE-CE Protocol for VPNs

In an MPLS VPN environment, customer networks are connected to an MPLS VPN-enabled provider backbone. As shown in Figure 9-167, Customer A areas, Areas 0 and 1, are connected to an MPLS VPN–enabled provider network. Area 0 and Area 1 have routers CE1 and CE2 running OSPF. MP-iBGP is used between PE1 and PE2 to propagate routes between Site 1 (Area 0) and Site 2 (Area 1). Traditional OSPF-BGP redistribution is performed at PE routers, PE1 and PE2. In this case, routes distributed by CE1 into the MP-iBGP cloud are sent to CE2 as external routes, even though both CE1 and CE2 belong to the same customer.

This behavior can be changed with the additional domain ID configuration. Each VRF should be configured a domain ID on the PE routers. If a PE router gets a route through the MP-iBGP cloud and has to send to any customer site, it checks the domain ID value against the list of stored domain ID values. If the incoming domain ID matches any of the stored IDs, that route is inserted into the customer site with the same type, as it was inserted into the MP-BGP cloud; otherwise, it is inserted as external route.

Topology

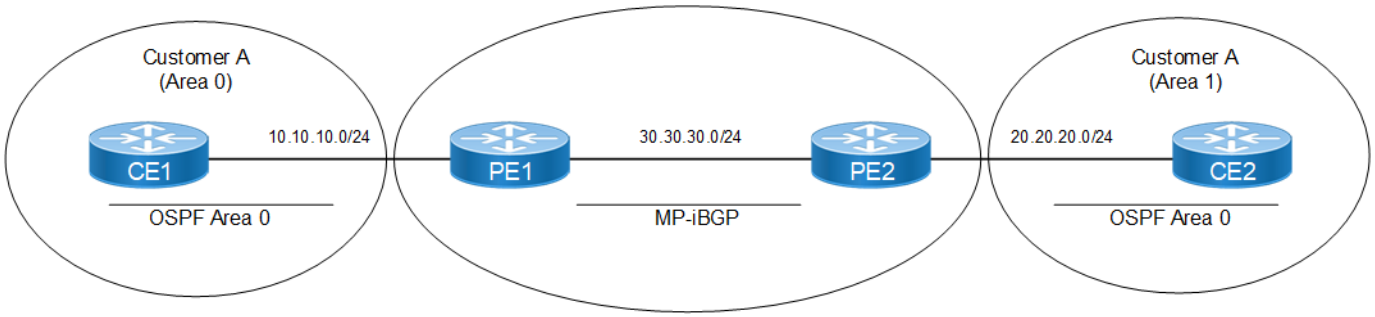


Figure 9-167: OSPF as PE-CE Protocol

Configuration

CE1

`#configure terminal`	Enter configure mode
`(config)#interface lo`	Enter loopback interface mode
`(config-if)#ip address 60.1.1.1/24 secondary`	Specify IP address for the interface
`(config-if)#exit`	Exit loopback interface mode

© 2021 IP Infusion Inc. Proprietary

(config)#router ospf 1	Configure the routing process and specify the Process ID (1).
(config-router)#network 10.10.10.0/24 area 0	Advertise the network in OSPF
(config-router)#network 60.1.1.0/24 area 0	Advertise the loopback IP address in area 0 of router OSPF 1.

PE1

#configure terminal	Enter configure mode.
(config)#ip vrf ABC	Specify the name of the VRF (ABC) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 10:100	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip vrf forwarding ABC	Associate interface eth1 to vrf ABC.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1 ABC	Configure OSPF for VRF.
(config-router)#network 10.10.10.0/24 area 0	Advertise the network for OSPF adjacency with CE1.
(config-router)#domain-id 1.1.1.1	Configure the primary domain ID.
(config-router)#domain-id 2.2.2.2 secondary	Configure a secondary domain ID.
(config-router)#domain-id 3.3.3.3 secondary	Configure a secondary domain ID.
(config-router)#exit	Exit Router mode and return to Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#neighbor 30.30.30.2 remote-as 100	Configure neighbor 30.30.30.2 for iBGP.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 30.30.30.2 activate	Activate neighbor 30.30.30.2.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf ABC	Enter Address-Family-VRF mode.
(config-router-af)#redistribute ospf	Specify redistributing routes from OSPF into BGP.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.

PE2

#configure terminal	Enter configure mode.
(config)#ip vrf ABC	Specify the name of the VRF (ABC) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 10:100	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.

(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip vrf forwarding ABC	Associate interface eth1 to vrf ABC.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1 ABC	Configure OSPF for VRF.
(config-router)#network 20.20.20.0/24 area 0	Advertise the network for OSPF adjacency with CE1.
(config-router)#domain-id 1.1.1.1	Configure the primary domain ID.
(config-router)#domain-id 2.2.2.2 secondary	Configure a secondary domain ID.
(config-router)#domain-id 3.3.3.3 secondary	Configure a secondary domain ID.
(config-router)#exit	Exit Router mode and return to Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#neighbor 30.30.30.1 remote-as 100	Configure neighbor 30.30.30.1 for iBGP.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 30.30.30.1 activate	Activate neighbor 30.30.30.1.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf ABC	Enter Address-Family-VRF mode.
(config-router-af)#redistribute ospf	Specify redistributing routes from OSPF into BGP.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.

CE2

#configure terminal	Enter configure mode.
(config)#router ospf 1	Configure the routing process, and specify the Process ID (1).
(config-router)#network 20.20.20.0/24 area 0	Advertise the network in OSPF.

Validation

```
#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 10:100 (Default for VRF ABC)
*>   10.10.10.0/24    0.0.0.0               2         100           32768    ?
*>   60.1.1.1/32      10.10.10.1            12        100           32768    ?
 Announced routes count = 2
 Accepted routes count = 0
#
```


© 2021 IP Infusion Inc. Proprietary

BGP Multipath for IPv4

BGP supports multipath for IPv4 prefixes. BGP Multipath allows load-balancing traffic among multiple BGP routes. It supports both iBGP and eBGP routes. In case of eBGP, the routes should arrive from same AS number.

Topology

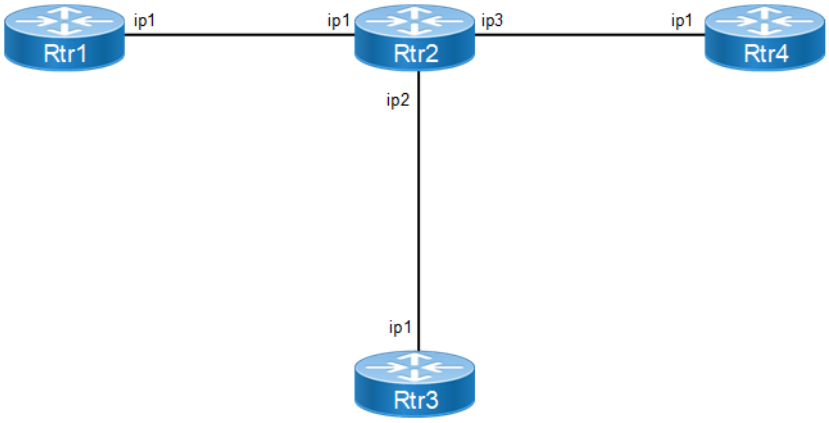


Figure 9-168: Multipath iBGP for IPv4

Configuration

Rtr1

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the BGP router.
`(config-router)#bgp router-id 2.2.2.2`	Configure a fixed Router ID (2.2.2.2).
`(config-router)#neighbor 30.30.30.9 remote-as 100`	Configure neighbor 30.30.30.9 for iBGP.
`(config-router)# address-family ipv4 unicast`	.Under address family, Redistribute the static routes.
`(config-router-af)#redistribute static`	Redistribute the static routes.
`config-router-af)# neighbor 30.30.30.9 activate`	Activate the neighbor
`(config-router-af)#exit-address-family`	Exit address-family mode.
`(config-router)#exit`	Exit the BGP Router mode and return to the Configure mode.
`(config)#ip route 88.88.0.0/16 Null`	Configure static route.

Rtr3

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the BGP router.
`(config-router)#bgp router-id 4.4.4.4`	Configure a fixed Router ID (4.4.4.4).
`(config-router)#neighbor 40.40.40.9 remote-as 100`	Configure neighbor 40.40.40.9 for iBGP.

(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#redistribute static	Redistribute the static routes.
config-router-af)# neighbor 40.40.40.9 activate	Activate the neighbor
(config-router-af)#exit-address-family	Exit address-family mode
(config-router)#exit	Exit the BGP Router mode and return to the Configure mode.
(config)#ip route 88.88.0.0/16 Null	Configure static route.

Rtr4

#configure terminal	Enter the Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#bgp router-id 6.6.6.6	Configure a fixed Router ID (6.6.6.6).
(config-router)#neighbor 50.50.50.9 remote-as 100	Configure neighbor 50.50.50.9 for iBGP.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#redistribute static	Redistribute the static routes.
config-router-af)# neighbor 50.50.50.9 activate	Activate the neighbor
(config-router-af)#exit-address-family	Exit address-family mode
(config-router)#exit	Exit the BGP Router mode and return to the Configure mode.
(config)#ip route 88.88.0.0/16 Null	Configure static route.

Rtr2

#configure terminal	Enter the Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config)#bgp router-id 9.9.9.9	Configure a fixed Router ID (9.9.9.9).
(config-router)#neighbor 30.30.30.2 remote-as 100	Configure neighbor 30.30.30.2 for iBGP.
(config-router)#neighbor 40.40.40.4 remote-as 100	Configure neighbor 40.40.40.4 for iBGP.
(config-router)#neighbor 50.50.50.6 remote-as 100	Configure neighbor 50.50.50.6 for iBGP.
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
config-router-af)# neighbor 30.30.30.2 activate	Activate the neighbor
config-router-af)# neighbor 40.40.40.4 activate	Activate the neighbor
config-router-af)# neighbor 50.50.50.6 activate	Activate the neighbor
config-router-af)# max-paths ibgp 2	Configure iBGP max-paths (2).
(config-router-af)#exit-address-family	Exit address-family mode

© 2021 IP Infusion Inc. Proprietary

Validation

```
#show ip bgp 88.88.0.0
BGP routing table entry for 88.88.0.0/16
Paths: (3 available, best #1, table Default-IP-Routing-Table) Not advertised to any peer
Local
30.30.30.2 from 30.30.30.2 (2.2.2.2)
Origin incomplete, metric 0, localpref 100, valid, internal, multipath- candidate, installed, best
Last update: Wed Mar2 15:17:38 2016

Local
50.50.50.6 from 50.50.50.6 (6.6.6.6)
Origin incomplete, metric 0, localpref 100, valid, internal, multipath- candidate
Last update: Wed Mar2 15:23:58 2016

Local
40.40.40.4 from 40.40.40.4 (4.4.4.4)
Origin incomplete, metric 0, localpref 100, valid, internal, multipath- candidate, installed
Last update: Wed Mar2 15:21:45 2016

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked
* - candidate default

IP Route Table for VRF "default"
C   30.30.30.0/24 is directly connected, eth1, 00:15:04 C   40.40.40.0/24 is directly connected, eth6, 00:14:30 C   50.50.50.0/24 is directly connected, eth3, 00:14:46 B 88.88.0.0/16 [200/0] via 40.40.40.4, eth6, 00:02:58
[200/0] via 30.30.30.2, eth1
C  127.0.0.0/8 is directly connected, lo, 00:19:21
C  192.168.52.0/24 is directly connected, eth0, 00:19:16 Gateway of last resort is not set
Gateway of last resort is not set

#show running-config router bgp
!
router bgp 100

bgp router-id 9.9.9.9
max-paths ibgp 2
neighbor 30.30.30.2remote-as100
neighbor 40.40.40.4remote-as100
neighbor 50.50.50.6remote-as100

!
```

```
 address-family ipv4 unicast
 max-paths ibgp 2
  neighbor 30.30.30.2 activate
neighbor 40.40.40.4 activate
neighbor 50.50.50.6 activate
 exit-address-family
!
```

Multipath eBGP

Topology

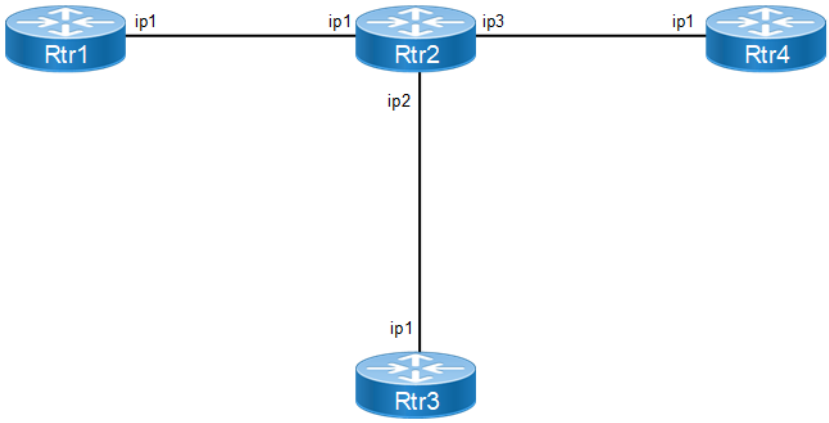


Figure 9-169: Multipath eBGP for IPv4

Configuration

Rtr1

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the BGP router.
`(config-router)#bgp router-id 2.2.2.2`	Configure a fixed Router ID (2.2.2.2).
`(config-router)#neighbor 30.30.30.9 remote-as 100`	Configure neighbor 30.30.30.9 for eBGP.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#redistribute static`	Redistribute the static routes.
`config-router-af)# neighbor 30.30.30.9 activate`	Activate the neighbor
`(config-router-af)#exit-address-family`	Exit address-family mode
`(config-router)#exit`	Exit the BGP Router mode and return to the Configure mode.
`(config)#ip route 88.88.0.0/16 Null`	Configure static route.

© 2021 IP Infusion Inc. Proprietary

Rtr3

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the BGP router.
`(config-router)#bgp router-id 4.4.4.4`	Configure a fixed Router ID (4.4.4.4).
`(config-router)#neighbor 40.40.40.9 remote-as 100`	Configure neighbor 40.40.40.9 for eBGP.
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#redistribute static`	Redistribute the static routes.
`config-router-af)# neighbor 40.40.40.9 activate`	Activate the neighbor
`(config-router-af)#exit-address-family`	Exit address-family mode
`(config-router)#exit`	Exit the BGP Router mode and return to the Configure mode.
`(config)#ip route 88.88.0.0/16 Null`	Configure static route.

Rtr4

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the BGP router.
`(config-router)#bgp router-id 6.6.6.6`	Configure a fixed Router ID (6.6.6.6).
`(config-router)#neighbor 50.50.50.9 remote-as 100`	Configure neighbor 50.50.50.9 for eBGP.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#redistribute static`	Redistribute the static routes.
`config-router-af)# neighbor 50.50.50.9 activate`	Activate the neighbor
`(config-router-af)#exit-address-family`	Exit address-family mode
`(config)#exit`	Exit the BGP Router mode and return to the Configure mode.
`(config)#ip route 88.88.0.0/16 Null`	Configure static route.

Rtr2

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the BGP router.
`(config)#bgp router-id 9.9.9.9`	Configure a fixed Router ID (9.9.9.9).
`(config-router)#neighbor 30.30.30.2 remote-as 200`	Configure neighbor 30.30.30.2 for eBGP.
`(config-router)#neighbor 40.40.40.4 remote-as 200`	Configure neighbor 40.40.40.4 for eBGP.
`(config-router)#neighbor 50.50.50.6 remote-as 200`	Configure neighbor 50.50.50.6 for eBGP.
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`config-router-af)# neighbor 30.30.30.2 activate`	Activate the neighbor

config-router-af)# neighbor 40.40.40.4 activate	Activate the neighbor
config-router-af)# neighbor 50.50.50.6 activate	Activate the neighbor
config-router-af)# max-paths ebgp 2	Configure eBGP max-paths (2).
(config-router-af)#exit-address-family	Exit address-family mode
(config-router)#exit	Exit the Router mode and return to Configure mode.

Validation

#**show ip bgp 88.88.0.0**

```
BGP routing table entry for 88.88.0.0/16
Paths: (3 available, best #3, table Default-IP-Routing-Table) Advertised to non peer-group peers:
30.30.30.2 50.50.50.6
200
30.30.30.2 from 30.30.30.2 (2.2.2.2)
Origin incomplete metric 0, localpref 100, valid, external, multipath-candidate, installed
Last update: Sat Jan3 02:06:25 1970



200
50.50.50.6 from 50.50.50.6 (6.6.6.6)
Origin incomplete metric 0, localpref 100, valid, external, multipath-candidate Last update: Sat Jan3 02:05:39 1970

200
40.40.40.4 from 40.40.40.4 (4.4.4.4)
Origin incomplete metric 0, localpref 100, valid, external, multipath-candidate, installed, best
Last update: Sat Jan3 02:05:11 1970

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked
* - candidate default

IP Route Table for VRF "default"
C   30.30.30.0/24 is directly connected, eth1, 05:26:26
C   40.40.40.0/24 is directly connected, eth6, 05:25:52
C   50.50.50.0/24 is directly connected, eth3, 05:26:08
B   88.88.0.0/16 [20/0] via 40.40.40.4, eth6, 00:01:38
    [20/0] via 30.30.30.2, eth1
C   127.0.0.0/8 is directly connected, lo, 05:30:43
```


© 2021 IP Infusion Inc. Proprietary

```
C   192.168.52.0/24 is directly connected, eth0, 05:30:38
Gateway of last resort is not set #show running-config router bgp
!
router bgp 100
bgp router-id 9.9.9.9
max-paths ebgp 2
neighbor 30.30.30.2 remote-as 200
neighbor 40.40.40.4 remote-as 200
neighbor 50.50.50.6 remote-as 200
!
 address-family ipv4 unicast
 neighbor 30.30.30.2 activate
 neighbor 40.40.40.4 activate
 neighbor 50.50.50.6 activate
 exit-address-family
!
```

Multipath eiBGP

Use this command to set the number of equal-cost multi-path (ECMP) routes for both eBGP and iBGP. This feature allows to configure multipath load balancing with both external BGP (eBGP) and internal BGP (iBGP) paths in Border Gateway Protocol.

When enabled, this feature can perform load balancing on eBGP and/or iBGP paths. With multiple eBGP and iBGP paths, selection is per all paths sorted according to BGP rules and hence either of all eBGP or iBGP or both will be marked as candidates for multipath programming i.e., it is possible either all eBGP paths or all iBGP paths or both eBGP and iBGP are programmed as multipaths.

Exceptions during path selections when eiBGP is enabled:

- AS Path length check is ignored.
- Origin Check is ignored.
- Peer type check is ignored.

IGP Metric check is ignored.

Topology

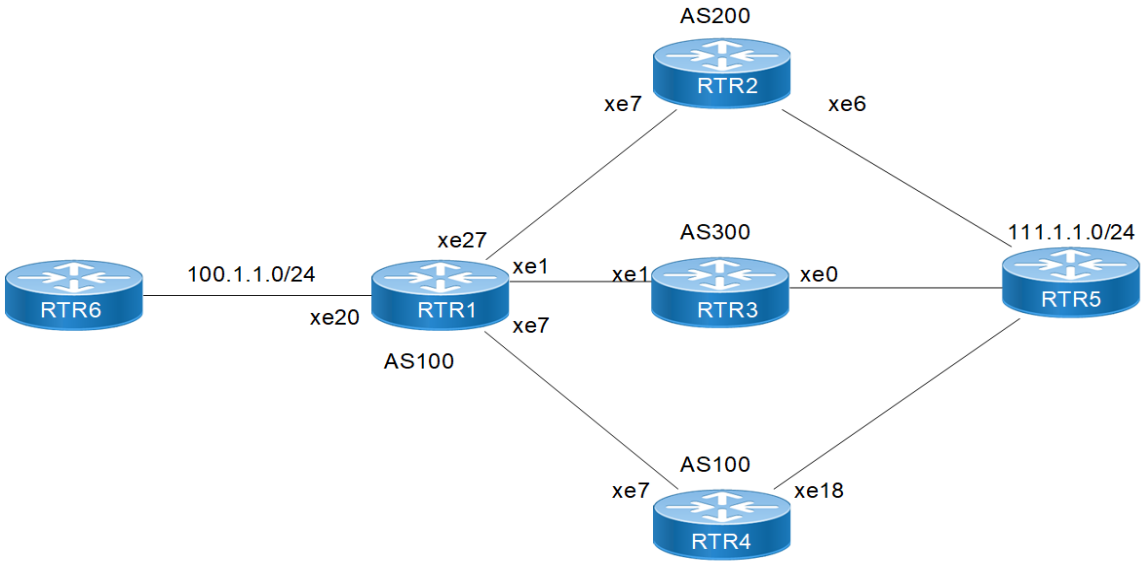


Figure 9-170: Multipath eiBGP topology

Configuration

RTR1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter Interface mode
`(config-if)# ip address 41.41.41.41/32 secondary`	Assign IP address to interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe27`	Enter Interface mode
`(config-if)# ip address 21.1.1.1/24`	Assign IP address to interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe1`	Enter Interface mode
`(config-if)# ip address 22.1.1.1/24`	Assign IP address to interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe7`	Enter Interface mode
`(config-if)# ip address 23.1.1.1/24`	Assign IP address to interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe20`	Enter Interface mode
`(config-if)# ip address 100.1.1.1/24`	Assign IP address to interface
`(config-if)#exit`	Exit interface mode
`(config)# router bgp 100`	Enter Router BGP mode
`(config-router)# neighbor 21.1.1.2 remote-as 200`	Define BGP neighbors. 21.1.1.2 is the IP address of the neighbor (RTR2) and 200 is the neighbors AS number

© 2021 IP Infusion Inc. Proprietary

(config-router)# neighbor 22.1.1.2 remote-as 300	Define BGP neighbors. 22.1.1.2 is the IP address of the neighbor (RTR3) and 300 is the neighbors AS number
(config-router)# neighbor 23.1.1.2 remote-as 100	Define BGP neighbors. 23.1.1.2 is the IP address of the neighbor (RTR4) and 100 is the neighbors AS number
(config-router)# address-family ipv4 unicast	Enter into BGP address family IPv4
(config-router-af)#max-paths eibgp 4	Configure eiBGP max-paths (4).
(config-router-af)#redistribute connected	Redistribute connected routes into BGP
(config-router-af)#neighbor 21.1.1.2 activate	Activate the neighbor
(config-router-af)#neighbor 22.1.1.2 activate	Activate the neighbor
(config-router-af)#neighbor 23.1.1.2 activate	Activate the neighbor
(config-router-af)# commit	Commit the configurations
(config-router-af)# end	Return to privilege mode

RTR2

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode
(config-if)# ip address 45.45.45.45/32 secondary	Assign IP address to interface
(config-if)#exit	Exit interface mode
(config)#interface xe7	Enter Interface mode
(config-if)# ip address 21.1.1.2/24	Assign IP address to interface
(config-if)#exit	Exit interface mode
(config)#interface xe6	Enter Interface mode
(config-if)# ip address 111.1.1.11/24	Assign IP address to interface
(config-if)#exit	Exit interface mode
(config)# router bgp 200	Enter Router BGP mode
(config-router)# neighbor 21.1.1.1 remote-as 100	Define BGP neighbors. 21.1.1.1 is the IP address of the neighbor (RTR1) and 100 is the neighbors AS number
(config-router)# address-family ipv4 unicast	Enter into BGP address family IPv4
(config-router-af)#redistribute connected	Redistribute connected routes
(config-router-af)#neighbor 21.1.1.1 activate	Activate the neighbor
(config-router-af)# commit	Commit the configurations
(config-router-af)# end	Return to privilege mode

RTR3

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode
(config-if)# ip address 42.42.42.42/32 secondary	Assign IP address to interface

(config-if)#exit	Exit interface mode
(config)#interface xe0	Enter Interface mode
(config-if)# ip address 111.1.1.42/24	Assign IP address to interface
(config-if)#exit	Exit interface mode
(config)#interface xe1	Enter Interface mode
(config-if)# ip address 22.1.1.2/24	Assign IP address to interface
(config-if)#exit	Exit interface mode
(config)# router bgp 300	Enter Router BGP mode
(config-router)# neighbor 22.1.1.1 remote-as 100	Define BGP neighbors. 22.1.1.1 is the IP address of the neighbor (RTR1) and 100 is the neighbors AS number
(config-router)# address-family ipv4 unicast	Enter into BGP address family IPv4
(config-router-af)#redistribute connected	Redistribute connected routes
(config-router-af)#neighbor 22.1.1.1 activate	Activate the neighbor
(config-router-af)# commit	Commit the configurations
(config-router-af)# end	Return to privilege mode

RTR4

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode
(config-if)# ip address 43.43.43.43/32 secondary	Assign IP address to interface
(config-if)#exit	Exit interface mode
(config)#interface xe7	Enter Interface mode
(config-if)# ip address 23.1.1.2/24	Assign IP address to interface
(config-if)#exit	Exit interface mode
(config)#interface xe18	Enter Interface mode
(config-if)# ip address 111.1.1.43/24	Assign IP address to interface
(config-if)#exit	Exit interface mode
(config)# router bgp 100	Enter Router BGP mode
(config-router)# neighbor 23.1.1.1 remote-as 100	Define BGP neighbors. 23.1.1.1 is the IP address of the neighbor (RTR1) and 100 is the neighbors AS number
(config-router)# address-family ipv4 unicast	Enter into BGP address family IPv4
(config-router-af)#redistribute connected	Redistribute connected routes
(config-router-af)#neighbor 23.1.1.1 activate	Activate the neighbor
(config-router-af)# commit	Commit the configurations
(config-router-af)# end	Return to privilege mode

© 2021 IP Infusion Inc. Proprietary

Validation

RTR1

```
# sh ip bgp summary
BGP router identifier 15.1.1.2, local AS number 100
BGP table version is 4
3 BGP AS-PATH entries
0 BGP community entries
4  Configured ebgp ECMP multipath: Currently set at 4

Neighbor    V   AS   MsgRcv  MsgSen TblVer   InQ   OutQ    Up/Down State/PfxRcd
21.1.1.2    4   200   13       16       4      0      0  00:04:28             3
22.1.1.2    4   300   10       14       4      0      0  00:03:05             4
23.1.1.2    4   100    7        9       4      0      0  00:01:49             4

Total number of neighbors 3

Total number of Established sessions 3

#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
B            11.1.1.0/24 [200/0] via 23.1.1.2, xe7, 00:11:26
B            11.11.11.11/32 [20/0] via 21.1.1.2, xe27, 00:10:14
B            17.1.1.0/24 [20/0] via 22.1.1.2, xe1, 00:10:54
C            21.1.1.0/24 is directly connected, xe27, 00:47:36
C            22.1.1.0/24 is directly connected, xe1, 00:49:33
C            23.1.1.0/24 is directly connected, xe7, 00:49:11
C            41.41.41.41/32 is directly connected, lo, 01:30:34
B            42.42.42.42/32 [20/0] via 22.1.1.2, xe1, 00:10:54
B            43.43.43.43/32 [200/0] via 23.1.1.2, xe7, 00:11:26
B            45.45.45.45/32 [20/0] via 21.1.1.2, xe27, 00:10:56
C            100.1.1.0/24 is directly connected, xe20, 00:08:31
B            111.1.1.0/24 [200/0] via 23.1.1.2, xe7, 00:11:26
                          [200/0] via 22.1.1.2, xe1,
                          [200/0] Via 21.1.1.2, xe27
C            127.0.0.0/8 is directly connected, lo, 01:39:19

Gateway of last resort is not set

#sh interface counters rate mbps
```

```
-----------------------------------------------------------------------

Interface

Rx mbps

Rx pps

Tx mbps

Tx pps

-----------------------------------------------------------------------
xe1                 0.00            0               264.30          22024
xe7                 0.00            0               254.86          21238
xe20                822.35          68529           0.02            3
xe27                0.00            0               215.04          17920
```

6BGP AS-PATH Multipath-relax

BGP will not load balance across multiple paths by default. We can configure it to do so with the `max-paths ebgp <no-of-multipaths>` command. The criterion of this command is that all attributes must match (Weight, Local preference, AS Path, etc). This is acceptable if we are multi-homed to a single AS, but what if we are multi-homed to different AS.

BGP AS PATH multipath relax effectively allows for ECMP to be done across different neighboring ASN's.

Topology

Below topology explains about BGP AS PATH multipath relax functionality.

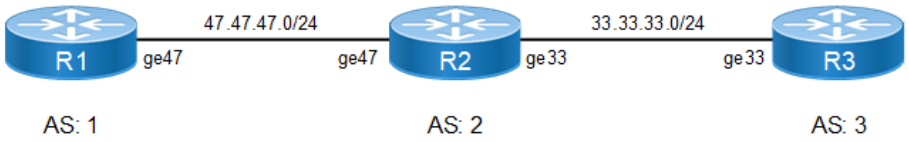


Figure 9-171: BGP AS-PATH Multipath-relax Topology

Configuration

R1

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter Interface loopback
`(config-if)#ip address 100.1.1.1/24 secondary`	Configure IP address for interface
`(config-if)#exit`	Exit interface mode
`(config)#interface ge47`	Enter Interface loopback

© 2021 IP Infusion Inc. Proprietary

(config-if)#ip address 47.47.47.1/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter the Configure mode
(config)#router bgp 1	Assign the ASN value (1) to the BGP router
(config-router)#neighbor 47.47.47.2 remote-as 2	Configure eBGP neighbor.
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#neighbor 47.47.47.2 activate	Activate neighbor
(config-router-af)#network 100.1.1.0/24	Advertise the loopback network into BGP.
(config-router-af)#end	Exit from router BGP and address-family config mode

R2

#configure terminal	Enter the Configure mode.
(config)#interface ge33	Enter interface mode
(config-if)#ip address 33.33.33.2/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter the Configure mode
(config)#interface ge47	Enter interface mode
(config-if)#ip address 47.47.47.2/24	Configure IP address for interface.
(config-if)#exit	Exit from interface mode and enter the Configure mode
(config)#router bgp 2	Assign the ASN value (2) to the BGP router.
(config-router)#neighbor 33.33.33.3 remote-as 3	Configure eBGP neighbor.
(config-router)#neighbor 47.47.47.1 remote-as 1	Configure eBGP neighbor.
(config-router)#address-family ipv4 unicast	Enter the address family IPv4 unicast mode
(config-router-af)# neighbor 33.33.33.3 activate	Activate the neighbor
config-router-af)# neighbor 47.47.47.1 activate	Activate the neighbor
(config-router-af)# max-paths ebgp 8	Configure eBGP Multipath.
(config-router-af)# bgp bestpath as-path multipath-relax	Configure BGP AS PATH Multipath relax.
(config-router-af)#end	End the address family mode.

R3

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter Interface loopback.
(config-if)#ip address 100.1.1.1/24 secondary	Configure IP address for interface.
(config-if)#exit	Exit from interface mode and enter the Configure mode.
(config)#interface ge33	Enter Interface loopback.
(config-if)#ip address 33.33.33.3/24	Configure IP address for interface.
(config-if)#exit	Exit from interface mode and enter the Configure mode.

(config)#router bgp 3	Assign the ASN value (3) to the BGP router.
(config-router)#neighbor 33.33.33.2 remote-as 2	Configure eBGP neighbor.
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# neighbor 33.33.33.2 activate	Activate the neighbor
(config-router-af)#network 100.1.1.0/24	Advertise the loopback network into BGP.
(config-router-af)#end	Exit from router BGP and address-family config mode

Validation

```
R2#show running-config bgp
!
router bgp 2
bgp bestpath as-path multipath-relax max-paths ebgp 8
neighbor 33.33.33.3 remote-as 3
neighbor 47.47.47.1 remote-as 1
!
 address-family ipv4 unicast
 neighbor 33.33.33.3 activate
 neighbor 47.47.47.1  activate
 max-paths ebgp 8
 bgp bestpath as-path multipath-relax
 exit-address-family
!
R2#show ip bgp 100.1.1.0
BGP routing table entry for 100.1.1.0/24
Paths: (2 available, best #1, table Default-IP-Routing-Table) Advertised to non peer-group peers:
47.47.47.1
3
33.33.33.3 from 33.33.33.3 (33.33.33.3)
Origin IGP, metric 0, localpref 100, valid, external, multipath- candidate, installed, best
Last update: Tue Feb 23 03:13:14 2016
1
47.47.47.1 from 47.47.47.1 (62.57.1.1)
Origin IGP, metric 0, localpref 100, valid, external, multipath-
candidate, installed
Last update: Tue Feb 23 03:13:15 2016

R2#show ip bgp summary
BGP router identifier 192.168.52.3, local AS number 2 BGP table version is 2
2 BGP AS-PATH entries


0 BGP community entries
8  Configured ebgp ECMP multipath: Currently set at 8
1  Configured ibgp ECMP multipath: Currently set at 1
```


© 2021 IP Infusion Inc. Proprietary

```
1   Configured eibgp ECMP multipath: Currently set at 1

NeighborVASMsgRcvMsgSen TblVerInQOutQUp/ DownState/PfxRcd
33.33.33.3
00:01:101
47.47.47.1
00:06:331

Total number of neighbors 2

Total number of Established sessions 2

R2#show ip bgp
BGP table version is 2, local router ID is 192.168.52.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

NetworkNext HopMetricLocPrfWeightPath
*> 100.1.1.0/2447.47.47.1010001 i
*   33.33.33.301000  3 i

Total number of prefixes 1
```

BGP FIB Install (Selective Route Download)

The BGP—Selective Route Download feature allows a network administrator to selectively download some or none of the BGP routes into the Routing Information Base (RIB). The primary application for this feature is to suppress the unnecessary downloading of certain BGP routes to the RIB or Forwarding Information Base (FIB) on a dedicated route reflector, which propagates BGP updates without carrying transit traffic. The feature thereby helps to maximize resources available and to improve routing scalability and convergence on the dedicated route reflector.

With RFC 4456, the concept of route reflection was defined; this would allow configuring designated one or more BGP routers in iBGP network as route reflectors. BGP relaxes the re-advertising restriction on these route reflectors, allowing them to accept and propagate IBGP routes to their clients.

The role of a dedicated route reflector (RR) is to propagate BGP updates without participating in the actual forwarding of transit traffic. That means the RR does not need to have all BGP routes downloaded into its RIB or FIB. It is beneficial for the RR to preserve its resources by not processing and storing those routes.

By default, BGP routes are downloaded to the RIB. To save resources on a dedicated route reflector, such downloading can be reduced or prevented by configuring a table map. A table map is so named because it controls what is put into the BGP routing table.

By reducing the route installation in the dedicated route reflectors, we can maximize availability of resources and improve routing scalability and convergence.

A new command ‘table map’ is being introduced to achieve this. A table map controls what is put into the BGP routing table. When configured it would reduce or prevent downloading routes to RIB.

Table map command references ‘route map’ rules available in BGP to control the routes going into the BGP routing table.

Table-map command can be used in two ways:

- When a simple table-map command is given (without filter option), the route map referenced in the table-map command shall be used to set certain properties (such as the traffic index) of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.
- When the option ‘filter’ is given in the table map command, the route map referenced is used to control whether a BGP route is to be downloaded to the IP RIB (hence the filter). A BGP route is not downloaded to the RIB if it is denied by the route map.

Topology

Below topology explains about BGP FIB Install functionality

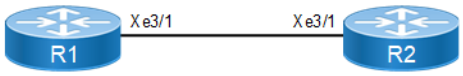


Figure 9-172: BFP FIB Install Topology

Configuration

R1

`#configure terminal`	Enter the Configure mode.
`(config)#interface xe3/1`	Enter interface mode.
`(config-if)#ip address 20.1.1.1/24`	Configure IP address for interface
`(config-if)#exit`	Exit interface mode
`(config)# router bgp 100`	Assign the ASN value (100) to the BGP router.
`(config-router)#neighbor 20.1.1.2 remote-as 100`	Configure neighbor in IBGP
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#redistribute static`	Redistribute static routes to advertise to its neighbor
`(config-router-af)#neighbor 20.1.1.2 activate`	Activate the neighbor
`(config-router-af)#exit-address-family`	Exit address-family mode
`(config-router)#exit`	Exit Router mode and enter Configure mode
`(config)#ip route 1.1.1.0/24 xe3/1`	Configure static route.
`(config)#ip route 2.2.2.0/24 xe3/1`	Configure static route.
`(config)#ip route 3.3.3.0/24 xe3/1`	Configure static route.
`(config)#ip route 4.4.4.0/24 xe3/1`	Configure static route.
`(config)#ip route 5.5.5.0/24 xe3/1`	Configure static route.
`(config)#ip route 6.6.6.0/24 xe3/1`	Configure static route.

R2

`#configure terminal`	Enter the Configure mode.
`(config)#interface xe3/1`	Configure IP address for interface
`(config-if)#ip address 20.1.1.2/24`	Configure IP address for interface

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit from interface mode and enter into Configure mode
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#neighbor 20.1.1.1 remote-as 100	Configure neighbor iBGP.
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#redistribute static	Redistribute the static routes.
(config-router-af)#neighbor 20.1.1.1 activate	Activate the neighbor
(config-router-af)#exit-address-family	Exit address-family mode
(config-router)#exit	Exit the BGP Router mode and return to the Configure mode.
(config)#ip access-list 1	Login to Configure access-list parameters
(config-ip-acl)#permit ipip 2.2.2.0 0.0.0.225 any	Configure access-list by allowing only one route to install in FIB table.
(config-ip-acl)#exit	Exit assess list mode
(config)# route-map test permit 1	Configure route-map to match access-list
(config-route-map)# match ip address 1	Match the above configured access-list 1
(config-route-map)#exit	Exit from route-map Configure mode and enter into Configure mode
(config)#router bgp 100	Enter into BGP router mode
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)# table-map test filter	Apply table-map with route-map created and with filter option
(config-router-af)#end	Exit from router and Configure mode

Validation

Table-map with Filter Option

Verify BGP neighborship is up between R1 and R2. Before applying table-map in R2, all routes will be installed in FIB table, as in below output.

R1

```
#show ip bgp summary
BGP router identifier 20.1.1.1, local AS BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries
number 100
NeighborVASMsgRcvMsgSen TblVerInQOutQUp/Dow
n   State/PfxRcd
20.1.1.241005
6   3
0
0
00:01:31
0
Total number of neighbors 1
Total number of Established sessions 1
```

```
#show ip bgp
BGP table version is 1, local router ID is 192.168.52.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete


   NetworkNext HopMetricLocPrfWeight Path
*> 1.1.1.0/240.0.0.0010032768?
*> 2.2.2.0/240.0.0.0010032768?
*> 3.3.3.0/240.0.0.0010032768?
*> 4.4.4.0/240.0.0.0010032768?
*> 5.5.5.0/240.0.0.0010032768?
*> 6.6.6.0/240.0.0.0010032768?

Total number of prefixes 6 #

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter
area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type
1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked
* - candidate default

IP Route Table for VRF "default"
S   1.1.1.0/24[1/0]isdirectlyconnected,eth1,00:06:54
S   2.2.2.0/24[1/0]isdirectlyconnected,eth1,00:06:35
S   3.3.3.0/24[1/0]isdirectlyconnected,eth1,00:06:26
S   4.4.4.0/24[1/0]isdirectlyconnected,eth1,00:06:17
S   5.5.5.0/24[1/0]isdirectlyconnected,eth1,00:06:09
S   6.6.6.0/24[1/0]isdirectlyconnected,eth1,00:06:01
C   20.1.1.0/24 is directly connected, eth1, 00:07:32 C127.0.0.0/8 is directly
connected, lo, 00:08:21
C   192.168.52.0/24 is directly connected, eth0, 00:08:17

Gateway of last resort is not set #
```

R2

```
#show ip bgp
BGP table version is 1, local router ID is 192.168.52.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   NetworkNext HopMetricLocPrfWeight Path
*> 1.1.1.0/240.0.0.0010032768?
*> 2.2.2.0/240.0.0.0010032768?
*> 3.3.3.0/240.0.0.0010032768?
*> 4.4.4.0/240.0.0.0010032768?
*> 5.5.5.0/240.0.0.0010032768?
```

 © 2021 IP Infusion Inc. Proprietary

```
*> 6.6.6.0/240.0.0.0010032768?


Total number of prefixes 6 #

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter
area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type
1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked
* - candidate default

IP Route Table for VRF "default"
B   1.1.1.0/24[200/0]via20.1.1.1,eth1,00:13:44
B   2.2.2.0/24[200/0]via20.1.1.1,eth1,00:13:44
B   3.3.3.0/24[200/0]via20.1.1.1,eth1,00:13:44
B   4.4.4.0/24[200/0]via20.1.1.1,eth1,00:13:44
B   5.5.5.0/24[200/0]via20.1.1.1,eth1,00:13:44
B   6.6.6.0/24[200/0]via20.1.1.1,eth1,00:13:44
C   20.1.1.0/24 is directly connected, eth1, 00:14:12 C127.0.0.0/8 is directly
connected, lo, 00:25:26
C   192.168.52.0/24 is directly connected, eth0, 00:25:23

Gateway of last resort is not set #
```

Table-map With Filter Option

Now verify after applying table-map with filter option, only one route will be installed in FIB table according to route-map and access-list configured, BGP table remains same, table-map effect will be seen only for FIB table.

After applying table-map, clear BGP with "clear ip bgp table-map."

```
(config)#router bgp 100
(config-router)#address-family ipv4-unicast (config-router-af)#table-map test filter
(config-router-af)#end
#clear ip bgp table-map

#show ip bgp
BGP table version is 2, local router ID is 192.168.52.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   NetworkNext HopMetricLocPrfWeightPath
*>i 1.1.1.0/2420.1.1.101000?
*>i 2.2.2.0/2420.1.1.101000?
*>i 3.3.3.0/2420.1.1.101000?
*>i 4.4.4.0/2420.1.1.101000?


*>i 5.5.5.0/2420.1.1.101000?
```

```
*>i 6.6.6.0/2420.1.1.101000?

Total number of prefixes 6 #

#show ip bgp summary
BGP router identifier 192.168.52.5, local AS number 100 BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

NeighborVASMsgRcvMsgSen TblVerInQOutQUp/DownState/ PfxRcd
20.1.1.141004039 2   0   0   00:18:33
6

Total number of neighbors 1

Total number of Established sessions 1 #

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter
area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type
1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked
* - candidate default

IP Route Table for VRF "default"
B   2.2.2.0/24 [200/0] via 20.1.1.1, eth1, 00:00:26
C   20.1.1.0/24 is directly connected, eth1, 00:19:01 C127.0.0.0/8 is directly
connected, lo, 00:30:15
C   192.168.52.0/24 is directly connected, eth0, 00:30:12

Gateway of last resort is not set
```

Table-map Without Filter Option

Remove filter option while applying table-map as below in R2

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Enter into BGP router mode
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# table-map test`	Apply table-map with route-map created and with filter option
`(config-router-af)#end`	Exit from router and configure mode

```
#show running-config bgp
!
router bgp 100 redistribute static
neighbor 20.1.1.1 remote-as 100 table-map test
```

 © 2021 IP Infusion Inc. Proprietary

```
!
 address-family ipv4 unicast
 neighbor 20.1.1.1 activate
 exit-address-family
!
#clear ip bgp table-map

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter
area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type
1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked
* - candidate default

IP Route Table for VRF "default"
B   1.1.1.0/24[200/0]via20.1.1.1,eth1,00:00:04
B   2.2.2.0/24[200/0]via20.1.1.1,eth1,00:00:04
B   3.3.3.0/24[200/0]via20.1.1.1,eth1,00:00:04
B   4.4.4.0/24[200/0]via20.1.1.1,eth1,00:00:04
B   5.5.5.0/24[200/0]via20.1.1.1,eth1,00:00:04
B   6.6.6.0/24[200/0]via20.1.1.1,eth1,00:00:04
C   20.1.1.0/24 is directly connected, eth1, 00:31:16 C127.0.0.0/8 is directly
connected, lo, 00:42:30
C   192.168.52.0/24 is directly connected, eth0, 00:42:27

Gateway of last resort is not set #
```

Note: Same can be tried with IPV6 VRF–v4 and VRF–v6 address-families and this feature is not supported for VPNV4 address-family

Route Target Constraint

BGP/MPLS IP VPNs use PE routers to Route Target (RT) extended communities and control the distribution of routes into the VRFs. Within a given iBGP mesh, PE routers hold routes marked with RouteTargets pertaining to VRFs that have local CE attachments.

BGP RT Constrained Route Distribution is a feature that can be used by service providers in Multiprotocol Label Switching (MPLS) Layer 3 VPNs to reduce the number of unnecessary routing updates that route reflectors (RRs) send to Provider Edge (PE) routers. The reduction in “routing updates” saves resources by allowing RRs, Autonomous System Boundary Routers (ASBRs), and PEs to carry fewer routes. Route targets are used to constrain routing updates.

With (MPLS)VPNs, the (iBGP) peers or Route Reflectors send all VPN4 and/or VPN6 prefixes to the PE routers. The PE routers drop the VPN4/6 prefixes for which there is no importing VPN route forwarding (VRF).

Topology

The topology below shows Route-target filtering in an L3VPN—with Route Target Constraint (RTC), the RR sends only wanted VPN4/6 prefixes to the PE; wanted” means that the PEs have the VRFs importing the specific prefixes.

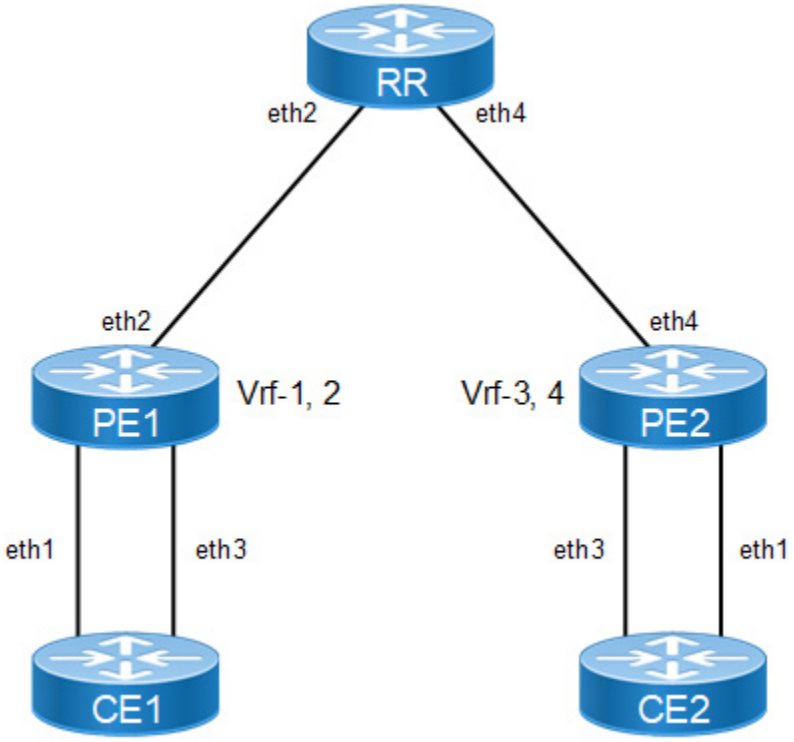


Figure 9-173: Route-target Filter Topology

Configuration

CE1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 80.1.1.1/24`	Configure IP address for interface
`(config-if)#exit`	Exit from interface mode and enter into Configure mode
`(config)#interface eth3`	Enter interface mode
`(config-if)#ip address 90.1.1.1/24`	Configure IP address for interface
`(config-if)#exit`	Exit from interface mode and enter into Configure mode
`(config)# router bgp 200`	Assign the ASN value (100) to the BGP router
`(config-router)#neighbor 80.1.1.2 remote-as 100`	Configure neighbor (RR) in IBGP
`(config-router)#neighbor 90.1.1.2 remote-as 100`	Configure neighbor (RR) in IBGP
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#redistribute static`	Redistribute static routes into BGP
`(config-router-af)#neighbor 80.1.1.2 activate`	Activate neighbor
`(config-router-af)#neighbor 90.1.1.2 activate`	Activate neighbor
`(config-router-af)#exit-address-family`	Exit address-family mode

© 2021 IP Infusion Inc. Proprietary

(config-router)#exit	Exit from router mode and enter configure mode
(config)#ip route vrf 1 1.1.1.0/24 eth1	Configure static route with VRF 1 instance
(config)#ip route vrf 2 3.3.3.0/24 eth3	Configure static route with VRF 2 instance
(config)#ip route vrf 2 4.4.4.0/24 eth3	Configure static route with VRF 2 instance

CE2

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode
(config-if)#ip address 101.1.1.1/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter into Configure mode
(config)#interface eth3	Enter interface mode
(config-if)#ip address 100.1.1.1/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter into Configure mode
(config)# router bgp 200	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 100.1.1.2 remote-as 100	Configure neighbor (RR) in IBGP
(config-router)#neighbor 101.1.1.2 remote-as 100	Configure neighbor (RR) in IBGP
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#neighbor 100.1.1.2 activate	Activate neighbor
(config-router-af)#neighbor 101.1.1.2 activate	Activate neighbor
(config-router-af)#exit-address-family	Exit from address family ipv4 unicast mode
(config-router)#end	Exit from router and configure mode

PE1

#configure terminal	Enter configure mode.
(config)#ip vrf 1	Create a VRF instance 1
(config-vrf)#rd 1:100	Configure unique RD value for VRF to identify VRF instance
(config-vrf)#route-target export 1:200	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)
(config-vrf)#exit	Exit VRF mode and enter Configure mode
(config)#ip vrf 2	Create a VRF instance 2
(config-vrf)#rd 1:300	Configure unique RD value for VRF to identify VRF instance
(config-vrf)#route-target both 1:400	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)
(config-vrf)#exit	Exit VRF mode and enter Configure mode
(config)#router ldp	Enable LDP.
(config-router)#exit	Exit router LDP mode

© 2021 IP Infusion Inc. Proprietary

(config)#interface lo	Enter loopback interface mode
(config-if)#ip address 11.11.11.11/32 secondary	Configure IP address for loopback interface
(config-if)# enable-ldp ipv4	Enable LDP on loopback interface
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip vrf forwarding 1	Bind interface to VRF 1
(config-if)#ip address 80.1.1.2/24	Configure IP address for VRF binded interface
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode
(config-if)#ip address 40.1.1.1/24	Configure an IP address for interface
(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE1 and RR
(config-if)#exit	Exit interface mode
(config)#interface eth3	Enter interface mode
(config-if)#ip vrf forwarding 2	Bind interface to VRF 1
(config-if)#ip address 90.1.1.2/24	Configure IP address for VRF binded interface
(config-if)#exit	Exit interface mode
(config)#router ospf	Enable OSPF process between PE1 and RR
(config-router)#network 11.11.11.11/32 area 0.0.0.0 (config-router)#network 40.1.1.0/24 area 0.0.0.0	Advertise loopback network in OSPF area 0
(config-router)#exit	Exit router OSPF mode
(config)# router bgp 100	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 22.22.22.22 remote-as 100	Configure neighbor (RR) in IBGP
(config-router)#neighbor 22.22.22.22 update-source lo	Enable neighbor with loopback interface.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 22.22.22.22 activate	Activate RR neighbor
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family rtfilter unicast	Enable RT filter address-family mode
(config-router-af)#neighbor 22.22.22.22 activate	Activate neighbor
(config-router-af)#exit-address-family	Exit RTfilter Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf 1	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 80.1.1.1 remote-as 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 80.1.1.1 activate	Activate neighbor in VRF
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.

© 2021 IP Infusion Inc. Proprietary

(config-router)#address-family ipv4 vrf 2	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 90.1.1.1 remote-as 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 90.1.1.1 activate	Activate neighbor in VRF
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#end	Exit from router mode and configure mode

RR

(config)#router ldp	Enable LDP
(config-router)#exit	Exit router LDP mode
(config)#interface lo	Enter loopback interface
(config-if)#ip address 22.22.22.22/32 secondary (config-if)#ip address 44.44.44.44/32 secondary	Configure IP address for loopback interface
(config-if)# enable-ldp ipv4	Enable LDP on loopback interface
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode
(config-if)#ip address 40.1.1.2/24	Configure IP address for interface connecting to PE2
(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE1 and RR
(config-if)#exit	Exit interface mode
(config)#interface eth4	Enter into interface mode
(config-if)#ip address 50.1.1.1/24	Configure an IP address for interface connecting to PE1
(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE1 and RR
(config-if)#exit	Exit interface mode
(config)#router ospf	Enable OSPF process between PE1 and RR
(config-router)#network 22.22.22.22/32 area 0.0.0.0	Advertise loopback network in OSPF area 0
(config-router)#network 40.1.1.0/24 area 0 (config-router)#network 44.44.44.44/32 area 0.0.0.0 (config-router)#network 50.1.1.0/24 area 0.0.0.0	Advertise PE1 to RR connected network in OSPF
(config-router)#exit	Exit from router OSPF mode
(config)# router bgp 100	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 11.11.11.11 remote-as 100	Configure neighbor (PE1) in IBGP
(config-router)#neighbor 11.11.11.11 update-source 22.22.22.22	Enable neighbor with loopback interface
(config-router)#neighbor 33.33.33.33 remote-as 100	Configure neighbor (PE2) in IBGP

(config-router)#neighbor 33.33.33.33 update-source 44.44.44.44	Enable neighbor with loopback interface
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 11.11.11.11 activate	Activate PE1 neighbor
(config-router-af)#neighbor 33.33.33.33 activate	Activate PE2 neighbor
(config-router-af)#neighbor 11.11.11.11 route-reflector-client	Configure PE1 as Route Reflector client
(config-router-af)#neighbor 33.33.33.33 route-reflector-client	Configure PE2 as Route Reflector client
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family rtfilter unicast	Enable RT filter address-family mode
(config-router-af)#neighbor 11.11.11.11 activate	Activate PE1 neighbor in RTfilter family
(config-router-af)#neighbor 33.33.33.33 activate	Activate PE2 neighbor in RTfilter family
(config-router-af)#neighbor 33.33.33.33 route-reflector-client	Configure PE2 as Route Reflector client
(config-router-af)#neighbor 11.11.11.11 route-reflector-client	Configure PE1 as Route Reflector client
(config-router-af)#exit-address-family	Exit RTfilter Address-Family mode
(config-router)#end	Exit from Address-Family, Router and Configure mode.

PE2

#configure terminal	Enter configure mode.
(config)#ip vrf 3	Create a VRF instance 3
(config-vrf)#rd 1:600	Configure unique RD value for VRF to identify VRF instance
(config-vrf)#route-target export 1:200	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)
(config-vrf)#exit	Exit VRF mode and enter Configure mode
(config)#ip vrf 4	Create a VRF instance 4
(config-vrf)#rd 1:900	Configure unique RD value for VRF to identify VRF instance
(config-vrf)#route-target both 1:400	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)
(config-vrf)#exit	Exit VRF mode and enter Configure mode
(config)#router ldp	Enable LDP.
(config-router)#exit	Exit router LDP mode
(config)#interface lo	Enter loopback interface mode
(config-if)#ip address 33.33.33.33/32 secondary	Configure IP address for loopback interface
(config-if)# enable-ldp ipv4	Enable LDP on loopback interface
(config-if)#exit	Exit interface mode

© 2021 IP Infusion Inc. Proprietary

(config)#interface eth1	Enter interface mode
(config-if)#ip vrf forwarding 3	Bind interface to VRF 3
(config-if)#ip address 101.1.1.2/24	Configure IP address for VRF binded interface
(config-if)#exit	Exit interface mode
(config)#interface eth3	Enter interface mode
(config-if)#ip vrf forwarding 4	Bind interface to VRF 3
(config-if)#ip address 100.1.1.2/24	Configure IP address for VRF binded interface
(config-if)#exit	Exit interface mode
(config)#interface eth4	Enter interface mode
(config-if)#ip address 50.1.1.2/24	Configure an IP address for interface
(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE2 and RR
(config-if)#exit	Exit interface mode
(config)#router ospf	Enable OSPF process between PE2 and RR
(config-router)#network 33.33.33.33/32 area 0.0.0.0	Advertise loopback network in OSPF area 0
(config-router)#network 50.1.1.0/24 area 0	Advertise PE2 to RR connected network in OSPF
(config-router)#exit	Exit router OSPF mode
(config)# router bgp 100	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 44.44.44.44 remote-as 100	Configure neighbor (RR) in IBGP
(config-router)#neighbor 44.44.44.44 update-source 33.33.33.33	Enable neighbor with loopback interface.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 44.44.44.44 activate	Activate RR neighbor
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family rtfilter unicast	Enable RT filter address-family mode
(config-router-af)#neighbor 44.44.44.44 activate	Activate neighbor
(config-router-af)#exit-address-family	Exit RTfilter Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf 3	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 101.1.1.1 remote-as 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 101.1.1.1 activate	Activate neighbor in VRF
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf 4	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 100.1.1.1 remote-as 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 100.1.1.1 activate	Activate neighbor in VRF

© 2021 IP Infusion Inc. Proprietary

(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router-af)#end	Exit router and configure mode

Validation

Through RTfilter address-family RT values will be exchanged between RR and PE's. Neighbors are activated under this address-family and configured clients as well in this. RR will learn routes from PE's and send to other PE's if it has any peer requesting for that particular routes based on their RT import values

Below outputs shows the routes sent and learned in PE's and installed in VRF's and display's RT filter values exchanged between them.

CE1

```
CE1#show ip bgp
BGP table version is 6, local router ID is 192.160.50.5
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   1.1.1.0/24       0.0.0.0              0         100           32768    ?
*>   3.3.3.0/24       0.0.0.0              0         100           32768    ?
*>   4.4.4.0/24       0.0.0.0              0         100           32768    ?

Total number of prefixes 3
```

PE1

```
PE1#sh ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:100 (Default for VRF 1)
*>   1.1.1.0/24       80.1.1.1             0         100           0       200
?
*>   3.3.3.0/24       80.1.1.1             0         100           0       200
?
*>   4.4.4.0/24       80.1.1.1             0         100           0       200
?
 Announced routes count = 3
 Accepted routes count = 0
Route Distinguisher: 1:300 (Default for VRF 2)
*>   1.1.1.0/24       90.1.1.1             0         100           0       200
?
*>   3.3.3.0/24       90.1.1.1             0         100           0       200
?
*>   4.4.4.0/24       90.1.1.1             0         100           0       200
?
 Announced routes count = 3
 Accepted routes count = 0
PE1#
```


© 2021 IP Infusion Inc. Proprietary

```
PE1#show ip bgp rtfilter all
RTFilter's Received
*******************
peer-ip 22.22.22.22
100:2:1:400
RTFilter's Sent
*******************
peer-ip 22.22.22.22
100:2:1:400
PE1#
```

RR

```
RR#sh ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:300
*>i  1.1.1.0/24       11.11.11.11           0         100           0       200
?
*>i  3.3.3.0/24       11.11.11.11           0         100           0       200
?
*>i  4.4.4.0/24       11.11.11.11           0         100           0       200
?
 Announced routes count = 0
 Accepted routes count = 3
RR#


RR#show ip bgp rtfilter all
RTFilter's Received
*******************
peer-ip 11.11.11.11
100:2:1:400
peer-ip 33.33.33.33
100:2:1:400
RTFilter's Sent
*******************
peer-ip 11.11.11.11
100:2:1:400
peer-ip 33.33.33.33
100:2:1:400
```

PE2

```
PE2#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:300
```

```
*>i  1.1.1.0/24       11.11.11.11          0         100           0       200
?
*>i  3.3.3.0/24       11.11.11.11          0         100           0       200
?
*>i  4.4.4.0/24       11.11.11.11          0         100           0       200
?
 Announced routes count = 0
 Accepted routes count = 3
Route Distinguisher: 1:900 (Default for VRF 4)
*>i  1.1.1.0/24       11.11.11.11          0         100           0       200
?
*>i  3.3.3.0/24       11.11.11.11          0         100           0       200
?
*>i  4.4.4.0/24       11.11.11.11          0         100           0       200
?
 Announced routes count = 0
 Accepted routes count = 3
PE2#


PE2#show ip bgp rtfilter all
RTFilter's Received
********************
peer-ip 44.44.44.44
100:2:1:400
RTFilter's Sent
********************
peer-ip 44.44.44.44
100:2:1:400
PE2#
```

BGP Best Path Selection Process

BGP assigns the first valid path as the current best path. BGP then compares the best path with the next path in the list, until BGP reaches the end of the list of valid paths. Below steps provides the rules that are used to determine the best path:

1. Prefer the path with the highest WEIGHT.
2. Prefer the path with the highest LOCAL_PREF.
3. Prefer the path that was locally originated via a network or aggregate BGP subcommand or through redistribution from an IGP.
4. Prefer the path with the shortest AS_PATH.

Note: Beware of these items:

- This step is skipped if user has configured the `bgp bestpath as-path ignore` command.
- If `bgp bestpath compare-confed-aspath` is configured then Prefer the path with the shortest AS_CONFED path.

5. Prefer the path with the lowest ORIGIN type.

Note: Beware of below listed items:

- IGP is lower than Exterior Gateway Protocol (EGP), and EGP is lower than INCOMPLETE.

© 2021 IP Infusion Inc. Proprietary

6. Prefer the path with the lowest multi-exit discriminator (MED).

Note: Beware of these items:

- By default, MED is compared in these cases:
  - MEDs are compared only if the first AS in the AS_SEQUENCE is the same for multiple paths
  - If both the paths are internal as routes
  - If paths have confederation as-path then MEDs are compared only if the first AS in the BGP_AS_CONFED_SEQUENCE is the same for multiple paths
  - To override all above checks, user can configure `bgp always-compare-med` command

7. Prefer eBGP over iBGP paths.

Note: Beware of below listed item:

- EBGP is preferred over IGBP or EBGP is preferred over CONFED.

8. Path learned from LU Address-family is preferred over IPv4 Unicast Address-family.

Note: Beware of these items:

- This is Exception Rule for IPv4 Labeled-Unicast Address-family.
- This rule applicable only for IPv4 Labeled-Unicast/Unicast routes over default VRF.

9. Prefer the path with the lowest IGP metric to the BGP next hop.

10. Determine if multiple paths require installation in the routing table for BGP Multipath and mark the ECMP candidate.

11. When both paths are external, prefer the path that was received first (the oldest one). This step minimizes route-flap, since a newer path won't displace an older one, even if it was the preferred route based on the additional decision criteria below. This has to be enabled by BGP command `bestpath tie-break-on-age`

Note: Beware of these items:

- Skip this step if any of these items are true:
  - If `bgp bestpath compare-routerid` is configured in addition to `bestpath tie-break-on-age`, then this step will be skipped.
  - If the router ID is same for multiple paths, because the routes were received from the same router, then this step will be skipped.

12. Router ID and Originator Id:

- If `bgp bestpath compare-routerid` is configured, then prefer the route that comes from the BGP router with the lowest Router ID.
- If `bgp bestpath dont-compare-originator-id` is not configured, prefer the route that comes from the BGP router with the lowest Router ID.

Note: Beware of the below listed item:

- If a path contains Route Reflector (RR) attributes, the Originator ID is substituted for the Router ID in the path selection process.
- If `bgp bestpath dont-compare-originator-id` is configured, prefer the route that comes from the BGP router with the lowest router ID. In this case, Originator ID is not compared even if the RR attribute is present.

13. If the originator or Router ID is the same for multiple paths, prefer the path with the minimum cluster list length.

Prefer the path that comes from the lowest neighbor address.

BGP Dampening

BGP supports route dampening for IPv4 and IPv6 prefixes. Route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the suppress limit, the advertisement of the route is suppressed. This penalty is decayed according to the configured half time value. Once the penalty is lower than the reuse limit, the route advertisement is unsuppressed. The dampening information is purged from the router once the penalty becomes less than half of the reuse limit.

Topology

In this example, a successful TCP connection is being established between the routers.

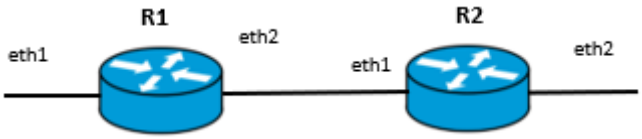


Figure 9-174: BGP dampening

IPv4 Configuration

R1

`#configure terminal`	Enter configure mode
`(config)#interface lo`	Enter loopback interface mode
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure the secondary loopback address
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 10.1.1.1/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 101.1.0.1/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 100`	Configure BGP with the AS number 100
`(config-router)#neighbor 10.1.1.2 remote-as 200`	Define the BGP neighbor, and establish a TCP session. 10.1.1.2 is the IP address of one of the neighbors (R2), and 200 is the neighbor's AS number.
`(config-router)#neighbor 100.1.0.2 remote-as 300`	Define the BGP neighbor, and establish a TCP session. 100.1.0.2 is the IP address of one of the neighbors on interface eth1, and 300 is the neighbor's AS number.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#redistribute connected`	Enable redistribute connected
`(config-router-af)#neighbor 10.1.1.2 activate`	Activate the neighbor

© 2021 IP Infusion Inc. Proprietary

`(config-router-af)#neighbor 100.1.0.2 activate`	Activate the neighbor
`(config-router-af)#exit-address-family`	Exit address-family mode

R2

`#configure terminal`	Enter configure mode
`(config)#interface lo`	Enter loopback interface mode
`(config-if)# ip address 2.2.2.2/32 secondary`	Configure the secondary loopback address
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 10.1.1.2/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 101.1.0.1/24`	Configure the IP address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Configure BGP with the AS number 100
`(config-router)#neighbor 10.1.1.1 remote-as 100`	Define the BGP neighbor, and establish a TCP session. 10.1.1.1 is the IP address of one of the neighbors (R1), and 100 is the neighbor's AS number.
`(config-router)#neighbor 101.1.0.2 remote-as 400`	Define the BGP neighbor, and establish a TCP session.101.1.0.2 is the IP address of one of the neighbors on eth2 interface, and 400 is the neighbor's AS number.
`(config-router)#neighbor 100.1.0.2 remote-as 300`	Define the BGP neighbor, and establish a TCP session. 100.1.0.2 is the IP address of one of the neighbors of router R1 on eth1 interface, and 300 is the neighbor's AS number.
`(config-router)#neighbor 100.1.0.2 ebgp-multihop 2`	Increase BGP neighbors with ebgp-multihop value
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#neighbor 10.1.1.1 activate`	Activate BGP neighbor
`(config-router-af)#neighbor 101.1.0.2 activate`	Activate BGP neighbor
`(config-router-af)#redistribute connected`	Enable redistribute connected
`(config-router-af)#bgp dampening`	Enable BGP dampening with default values: • Reachability half-life is 15 minutes • Reuse limit is 750: • Suppress limit is 2000 • Max-suppress value is 60 minutes • Un-reachability half-life is 15 minutes

© 2021 IP Infusion Inc. Proprietary

Validation

R2

Verify the BGP dampening parameters.

```
#show ip bgp dampening parameters

dampening 15 750 2000 60 15 Dampening Control Block(s):
Reachability Half-Life time : 15 min Reuse penalty: 750
Suppress penalty: 2000
Max suppress time: 60 min Un-reachability Half-Life time : 15 min Max penalty (ceil):
11999
Min penalty (floor): 375
```

Verify BGP dampened paths for flapping networks.

```
#show ip bgp dampening dampened-paths
BGP table version is 21, local router ID is 4.4.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   NetworkFromReusePath
d  200.1.0.010.1.1.100:29:00 100300i
d  200.2.0.010.1.1.100:28:20 100300i
d  200.3.0.010.1.1.100:28:20 100300i
d  200.4.0.010.1.1.100:28:20 100300i
d  200.5.0.010.1.1.100:28:20 100300i
d  200.6.0.010.1.1.100:28:20 100300i
d  200.7.0.010.1.1.100:28:20 100300i
d  200.8.0.010.1.1.100:28:20 100300i
d  200.9.0.010.1.1.100:28:20 100300i
d  200.10.0.010.1.1.100:28:20 100300i
```

Verify BGP dampening flap statistics for flapping networks.

```
#show ip bgp dampening flap-statistics
BGP table version is 21, local router ID is 4.4.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   NetworkFromFlapsDurationReusePath
d  200.1.0.010.1.1.1800:18:3700:29:10100 300i
d  200.2.0.010.1.1.1700:14:2200:29:00100 300i
d  200.3.0.010.1.1.1700:14:2200:29:00100 300i
d  200.4.0.010.1.1.1700:14:2200:29:00100 300i
d  200.5.0.010.1.1.1700:14:2200:29:00100 300i
d  200.6.0.010.1.1.1700:14:2200:29:00100 300i
d  200.7.0.010.1.1.1700:14:2200:29:00100 300i
d  200.8.0.010.1.1.1700:14:2200:29:00100 300i
```


© 2021 IP Infusion Inc. Proprietary

```
d   200.9.0.010.1.1.1700:14:2200:29:00100 300i
d   200.10.0.010.1.1.1700:14:2200:29:00100 300i
```

IPv6 Configuration

R1

`#configure terminal`	Enter configure mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 address 2000:0:0:1::1/64`	Configure the IPv6 address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 2000:0:2:1::1/64`	Configure the IPv6 address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 100`	Configure BGP with the AS number 100
`(config-router)#neighbor 2000:0:0:1::2 remote-as 300`	Define the BGP neighbor, and establish a TCP session. 2000:0:0:1::2 is the IP address of one of the neighbors on interface eth1, and 300 is the neighbor's AS number.
`(config-router)#neighbor 2000:0:2:1::2 remote-as 200`	Define the BGP neighbor, and establish a TCP session. 2000:0:2:1::2 is the IP address of one of the neighbors (R2), and 200 is the neighbor's AS number.
`(config-router)#address-family ipv6 unicast`	Enter IPv6 address family
`(config-router)#redistribute connected`	Enable redistribute connected
`(config-router-af)neighbor 2000:0:0:1::2 activate`	Activate BGP neighbor
`(config-router-af)neighbor 2000:0:2:1::2 activate`	Activate BGP neighbor

R2

`#configure terminal`	Enter configure mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 2000:0:2:1::2/64`	Configure the IPv6 address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 2000:0:1:1::1/64`	Configure the IPv6 address of the interface
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Configure BGP with the AS number 200
`(config-router)#address-family ipv6 unicast`	Enter IPv6 address family
`(config-router-af)#redistribute connected`	Enable redistribute connected
`(config-router-af)#exit-address-family`	Exit address-family mode.
`(config-router)#neighbor 2000:0:1:1::2 remote-as 400`	Define the BGP neighbor, and establish a TCP session. 2000:0:1:1::2 is the IP address of one of the neighbors on interface eth2, and 400 is the neighbor's AS number.

© 2021 IP Infusion Inc. Proprietary

`(config-router)#neighbor 2000:0:2:1::1 remote-as 100`	Define the BGP neighbor, and establish a TCP session. 2000:0:2:1::1 is the IP address of one of the neighbors (R1), and 100 is the neighbor's AS number.
`(config-router)#address-family ipv6 unicast`	Enter IPv6 address-family
`(config-router-af)#bgp dampening`	Enable BGP dampening with default values: • Reachability half-life is 15 minutes • Reuse limit is 750 • Suppress limit is 2000 • Max-suppress value is 60 minutes • Un-reachability half-life is 15 minutes
`(config-router-af)#neighbor 2000:0:1:1::2 activate`	Activate BGP neighbor
`(config-router-af)#neighbor 2000:0:2:1::1 activate`	Activate BGP neighbor

Validation

R2

Verify the IPv6 BGP dampening parameters.

```
#sh bgp dampening parameters

 dampening 15 750 2000 60 15
 Dampening Control Block(s):
  Reachability Half-Life time    : 15 min
  Reuse penalty                  : 750
  Suppress penalty               : 2000
  Max suppress time              : 60 min
  Un-reachability Half-Life time : 15 min
  Max penalty (ceil)             : 11999
  Min penalty (floor)            : 375
```

Verify IPv6 BGP dampened paths for flapping networks.

```
#sh bgp dampening dampened-paths
BGP table version is 7, local router ID is 4.4.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            From                 Reuse    Path
*d   3000:0:1:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    00:18:30 100 300 i
*d   3000:0:2:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    00:18:30 100 300 i
*d   3000:0:3:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    00:18:30 100 300 i
*d   3000:0:4:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    00:18:30 100 300 i
```


© 2021 IP Infusion Inc. Proprietary

```
*d   3000:0:5:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    00:18:30 100 300 i
*d   3000:0:6:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    00:18:30 100 300 i
*d   3000:0:7:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    00:18:30 100 300 i
*d   3000:0:8:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    00:18:30 100 300 i
*d   3000:0:9:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    00:18:30 100 300 i
*d   3000:0:a:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                    00:18:30 100 300 i
```

Verify IPv6 BGP dampening flap statistics for flapping networks.

```
#sh bgp dampening flap-statistics
BGP table version is 7, local router ID is 4.4.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            From                Flaps  Duration  Reuse    Path
*d   3000:0:1:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                  4  00:05:19  00:18:30  100 300 i
*d   3000:0:2:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                  4  00:05:19  00:18:30  100 300 i
*d   3000:0:3:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                  4  00:05:19  00:18:30  100 300 i
*d   3000:0:4:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                  4  00:05:19  00:18:30  100 300 i
*d   3000:0:5:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                  4  00:05:19  00:18:30  100 300 i
*d   3000:0:6:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                  4  00:05:19  00:18:30  100 300 i
*d   3000:0:7:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                  4  00:05:19  00:18:30  100 300 i
*d   3000:0:8:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                  4  00:05:19  00:18:30  100 300 i
*d   3000:0:9:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                  4  00:05:19  00:18:30  100 300 i
*d   3000:0:a:1::/64  2000:0:2:1::1(fe80::ba6a:97ff:fed6:23d4)
                                                  4  00:05:19  00:18:30  100 300 i
```

BGP Authentication

BGP authentication allows users to receive selected routing information, enhancing security of their network traffic. When BGP authentication is enabled on a router, the router verifies routing packets it receives by exchanging a password that is configured on both the sending and receiving routers.

In this example, both R1 and R2 have ABC as the password. Configure the same password on all routers that are to communicate using BGP in a network.

Topology

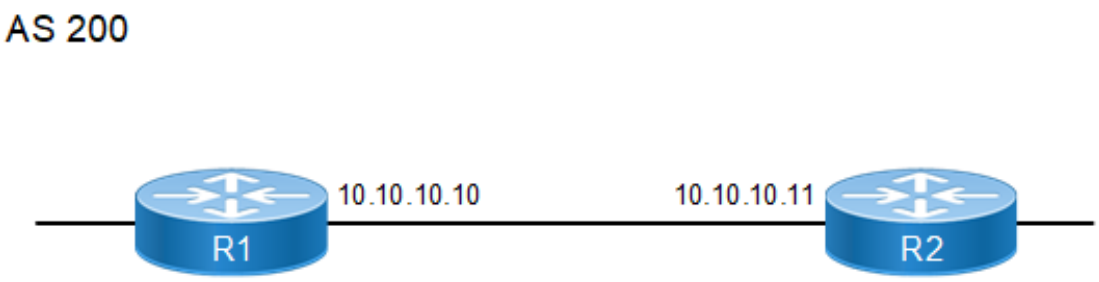


Figure 9-175: BGP Authentication

Configuration

R1

`#configure terminal`	Enter configure mode
`(config)#interface xe0`	Enter interface mode
`(config-if)#ip address 10.10.10.10/24`	Assign ip address
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Enter BGP router mode
`(config-router)#neighbor 10.10.10.11 remote-as 300`	Configure neighborship
`(config-router)#neighbor 10.10.10.11 authentication-key 0 ABC`	Configure authentication for BGP neighbors
`(config-router)#address-family ipv4 unicast`	Enter ipv4 address family
`(config-router-af)#neighbor 10.10.10.11 activate`	Activate neighborship
`(config-router-af)#exit-address-family`	Exit address family
`(config-router)#end`	End config mode

R2

`#configure terminal`	Enter configure mode
`(config)#interface ce2/1`	Enter interface mode
`(config-if)#ip address 10.10.10.11/24`	Assign ip address
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Enter BGP router mode

© 2021 IP Infusion Inc. Proprietary

`(config-router)#neighbor 10.10.10.10 remote-as 200`	Configure neighborship
`(config-router)#neighbor 10.10.10.10 authentication-key 0 ABC`	Configure authentication for BGP neighbors
`(config-router)#address-family ipv4 unicast`	Enter ipv4 address family
`(config-router-af)#neighbor 10.10.10.10 activate`	Activate neighborship
`(config-router-af)#exit-address-family`	Exit address family
`(config-router)#end`	End config mode

Validation

R1

```
#show running-config bgp
!
router bgp 200
 neighbor 10.10.10.11 remote-as 300
 neighbor 10.10.10.11 authentication-key 0x624ac41428f81e33
 !
 address-family ipv4 unicast
 neighbor 10.10.10.11 activate
 exit-address-family
!
#show ip bgp neighbors
BGP neighbor is 10.10.10.11, remote AS 300, local AS 200, external link
  BGP version 4, local router ID 22.22.22.22, remote router ID 2.2.2.2
  BGP state = Established, up for 00:09:14
  Last read 00:00:19, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 23 messages, 0 notifications, 0 in queue
  Sent 24 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.10, Local port: 179
Foreign host: 10.10.10.11, Foreign port: 37590
Nexthop: 10.10.10.10
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

R2

```
#show running-config bgp
!
router bgp 300
 neighbor 10.10.10.10 remote-as 200
 neighbor 10.10.10.10 authentication-key 0x624ac41428f81e33
 !
 address-family ipv4 unicast
 neighbor 10.10.10.10 activate
 exit-address-family
!
#show ip bgp neighbors
BGP neighbor is 10.10.10.10, remote AS 200, local AS 300, external link
  BGP version 4, local router ID 2.2.2.2, remote router ID 22.22.22.22
  BGP state = Established, up for 00:13:57
  Last read 00:00:22, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 33 messages, 0 notifications, 0 in queue
  Sent 34 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.11, Local port: 37590
Foreign host: 10.10.10.10, Foreign port: 179
Nexthop: 10.10.10.11
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

BGP Unnumbered

This chapter contains configurations for BGP unnumbered interface which provides BGP peering with minimal configuration.

Overview

BGP protocol is used to exchange IP prefixes between AS. For BGP neighbor ship to be established, IPv4 address configuration on peer is pre-requisite. In a large network, this can consume a lot of your address space, requiring a separate IP address for each peer-facing interface apart from administrator effort in configuration. When a BGP peer advertises an IPv4 prefix, it must include an IPv4 next hop address, which is usually the address of the advertising router; for this each BGP peer should have an IPv4 address. This feature is to enable BGP peering with minimal configuration, less IPv4 address-space.

For DC use-case, where hundreds of switches can be connected in CLOS topology, configuring each neighbor is both time consuming and (IPv4) address hungry.

 © 2021 IP Infusion Inc. Proprietary

To minimize this, BGP unnumbered can, avoid the need for an IP address on each BGP interface and by removing the need to configure the IP address and ASN of each neighbor. This feature uses link local ipv6 address of interface as per RFC-5549.

Topology

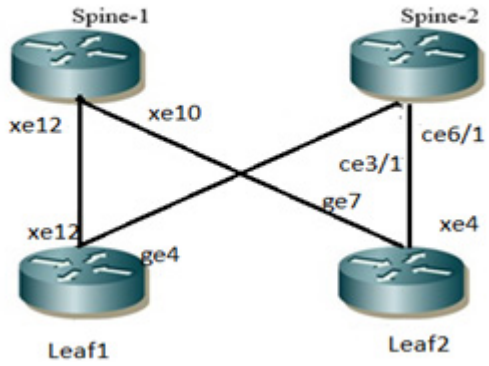


Figure 9-176: BGP-Unnumbered

Configuration

Spine 1

`configure terminal`	Enter configure mode
`(config)#interface lo`	Enter interface mode for loopback interface
`(config-if)#ip add 1.1.1.1/32 secondary`	Assign secondary interface to loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface xe12`	Enter interface mode
`(config-if)#no ipv6 nd suppress-ra`	Disable Suppress IPv6 Router Advertisements
`(config-if)# ipv6 nd ra-interval 4`	Assign the IPv6 Router Advertisements interval
`(config-if)#exit`	Exit interface mode
`(config)#interface xe10`	Enter interface mode
`(config-if)# ip address 10.10.10.2/31`	Assign IP address to the interface in /31 subnet
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 100`	Enter bgp router mode
`(config-router)#bgp router-id 1.1.1.1`	Assign router id for BGP
`(config-router)#bgp unnumbered-mode`	Enter bgp unnumbered mode
`(config-router-unnum)#neighbor xe12 remote-as internal`	Configure iBGP neighborship
`(config-router-unnum)#neighbor xe10 remote-as internal`	Configure iBGP neighborship
`(config-router-unnum)# exit-unnumbered-mode`	Exit unnumbered mode
`(config-router)#address-family ipv4 unicast`	Enter address family mode for IPv4 unicast
`(config-router-af)# bgp v4-unnumbered-mode`	Enter unnumbered mode under ipv4 unicast af
`(config-router-v4-unnum)# neighbor xe10 activate`	Activate the neighbor
`(config-router-v4-unnum)# neighbor xe12 activate`	Activate the neighbor
`(config-router-v4-unnum)# exit-v4-unnumbered-mode`	Exit unnumbered mode under ipv4 unicast af
`(config-router-af)# exit-address-family`	Exit address family mode for IPv4 unicast
`(config-router)#end`	End Config mode

Spine 2

`configure terminal`	Enter configure mode
`(config)#interface lo`	Enter interface mode for loopback interface
`(config-if)# ip address 2.2.2.2/32 secondary`	Assign secondary interface to loopback
`(config-if)#exit`	Exit interface mode
`(config)# interface ce6/1`	Enter interface mode
`(config-if)#no ipv6 nd suppress-ra`	Disable Suppress IPv6 Router Advertisements
`(config-if)# ipv6 nd ra-interval 4`	Assign the IPv6 Router Advertisements interval

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit interface mode
(config)# interface ce3/1	Enter interface mode
(config-if)# ip address 20.20.20.2/31	Assign IP address to the interface in /31 subnet
(config-if)#exit	Exit interface mode
(config)#router bgp 100	Enter bgp router mode
(config-router)#bgp router-id 2.2.2.2	Assign router id for BGP
(config-router)#bgp unnumbered-mode	Enter bgp unnumbered mode
(config-router-unnum)#neighbor ce3/1 remote-as internal	Configure iBGP neighborship
(config-router-unnum)#neighbor ce6/1 remote-as internal	Configure iBGP neighborship
(config-router-unnum)# exit-unnumbered-mode	Exit unnumbered mode
(config-router)#address-family ipv4 unicast	Enter address family mode for IPv4 unicast
(config-router-af)# bgp v4-unnumbered-mode	Enter unnumbered mode under ipv4 unicast af
(config-router-v4-unnum)# neighbor ce3/1 activate	Activate the neighbor
(config-router-v4-unnum)# neighbor ce6/1 activate	Activate the neighbor
(config-router-v4-unnum)# exit-v4-unnumbered-mode	Exit unnumbered mode under ipv4 unicast af
(config-router-af)# exit-address-family	Exit address family mode for IPv4 unicast
(config-router)#end	End Config mode

Leaf 1

configure terminal	Enter configure mode
(config)#interface lo	Enter interface mode for loopback interface
(config-if)# ip address 3.3.3.3/32 secondary	Assign secondary interface to loopback
(config-if)#exit	Exit interface mode
(config)#interface xe12	Enter interface mode
(config-if)#no ipv6 nd suppress-ra	Disable Suppress IPv6 Router Advertisements
(config-if)# ipv6 nd ra-interval 4	Assign the IPv6 Router Advertisements interval
(config-if)#exit	Exit interface mode
(config)#interface ge4	Enter interface mode
(config-if)# ip address 10.10.10.3/31	Assign IP address to the interface in /31 subnet
(config-if)#exit	Exit interface mode
(config)#router bgp 100	Enter bgp router mode
(config-router)#bgp router-id 3.3.3.3	Assign router id for BGP
(config-router)#bgp unnumbered-mode	Enter bgp unnumbered mode
(config-router-unnum)#neighbor xe12 remote-as internal	Configure iBGP neighborship
(config-router-unnum)#neighbor ge4 remote-as internal	Configure iBGP neighborship
(config-router-unnum)# exit-unnumbered-mode	Exit unnumbered mode

(config-router)#address-family ipv4 unicast	Enter address family mode for IPv4 unicast
(config-router-af)# bgp v4-unnumbered-mode	Enter unnumbered mode under ipv4 unicast af
(config-router-v4-unnum)# neighbor ge4 activate	Activate the neighbor
(config-router-v4-unnum)# neighbor xe12 activate	Activate the neighbor
(config-router-v4-unnum)# exit-v4-unnumbered-mode	Exit unnumbered mode under ipv4 unicast af
(config-router-af)# exit-address-family	Exit address family mode for IPv4 unicast
(config-router)#end	End Config mode

Leaf 2

configure terminal	Enter configure mode
(config)#interface lo	Enter interface mode for loopback interface
(config-if)#ip address 4.4.4.4/32 secondary	Assign secondary interface to loopback
(config-if)#exit	Exit interface mode
(config)#interface xe4	Enter interface mode
(config-if)#no ipv6 nd suppress-ra	Disable Suppress IPv6 Router Advertisements
(config-if)# ipv6 nd ra-interval 4	Assign the IPv6 Router Advertisements interval
(config-if)#exit	Exit interface mode
(config)#interface ge7	Enter interface mode
(config-if)# ip address 10.10.10.2/31	Assign IP address to the interface in /31 subnet
(config-if)#exit	Exit interface mode
(config)#router bgp 100	Enter bgp router mode
(config-router)#bgp router-id 4.4.4.4	Assign router id for BGP
(config-router)#bgp unnumbered-mode	Enter bgp unnumbered mode
(config-router-unnum)#neighbor xe4 remote-as internal	Configure iBGP neighborship
(config-router-unnum)#neighbor ge7 remote-as internal	Configure iBGP neighborship
(config-router-unnum)# exit-unnumbered-mode	Exit unnumbered mode
(config-router)#address-family ipv4 unicast	Enter address family mode for IPv4 unicast
(config-router-af)# bgp v4-unnumbered-mode	Enter unnumbered mode under ipv4 unicast af
(config-router-v4-unnum)# neighbor ge7 activate	Activate the neighbor
(config-router-v4-unnum)# neighbor xe4 activate	Activate the neighbor
(config-router-v4-unnum)# exit-v4-unnumbered-mode	Exit unnumbered mode under ipv4 unicast af
(config-router-af)# exit-address-family	Exit address family mode for IPv4 unicast
(config-router)#end	End Config mode

© 2021 IP Infusion Inc. Proprietary

Validation

Spine 1:

```
Spine1#show ip bgp neighbors
BGP neighbor is 10.10.10.3, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 1.1.1.1, remote router ID 4.4.4.4
  BGP state = Established, up for 00:22:12
  Last read 00:00:06, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 54 messages, 0 notifications, 0 in queue
  Sent 54 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.2, Local port: 179
Foreign host: 10.10.10.3, Foreign port: 49242
Nexthop: 10.10.10.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is fe80::eac5:7aff:fefe:97e0, remote AS 100, local AS 100, internal
link
  BGP version 4, local router ID 1.1.1.1, remote router ID 3.3.3.3
  BGP state = Established, up for 00:29:54
  Last read 00:00:12, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
```

```
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 71 messages, 0 notifications, 0 in queue
  Sent 74 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: fe80::eac5:7aff:fe8b:a82a, Local port: 179
Foreign host: fe80::eac5:7aff:fefe:97e0, Foreign port: 37116
Nexthop: 1.1.1.1
Nexthop global: fe80::eac5:7aff:fe8b:a82a
Nexthop local: fe80::eac5:7aff:fe8b:a82a
BGP connection: shared network
```

Spine 2:

```
Spine2#show ip bgp neighbors
BGP neighbor is 20.20.20.3, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 2.2.2.2, remote router ID 3.3.3.3
  BGP state = Established, up for 00:21:15
  Last read 00:00:12, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 52 messages, 0 notifications, 0 in queue
  Sent 51 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
```

 © 2021 IP Infusion Inc. Proprietary

```
 Connections established 1; dropped 0
Local host: 20.20.20.2, Local port: 59380
Foreign host: 20.20.20.3, Foreign port: 179
Nexthop: 20.20.20.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is fe80::36ef:b6ff:fe31:dd3f, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 2.2.2.2, remote router ID 4.4.4.4
  BGP state = Established, up for 00:29:31
  Last read 00:00:21, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 70 messages, 0 notifications, 0 in queue
  Sent 72 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: fe80::ce37:abff:fe3f:9f63, Local port: 179
Foreign host: fe80::36ef:b6ff:fe31:dd3f, Foreign port: 33368
Nexthop: 2.2.2.2
Nexthop global: fe80::ce37:abff:fe3f:9f63
Nexthop local: fe80::ce37:abff:fe3f:9f63
BGP connection: shared network
```

Leaf 1

```
Leaf1#show ip bgp neighbors
BGP neighbor is 20.20.20.2, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 3.3.3.3, remote router ID 2.2.2.2
  BGP state = Established, up for 00:21:32
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 52 messages, 0 notifications, 0 in queue
  Sent 54 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
```

```
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 20.20.20.3, Local port: 179
Foreign host: 20.20.20.2, Foreign port: 59380
Nexthop: 20.20.20.3
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is fe80::eac5:7aff:fe8b:a82a, remote AS 100, local AS 100, internal
 link
  BGP version 4, local router ID 3.3.3.3, remote router ID 1.1.1.1
  BGP state = Established, up for 00:30:46
  Last read 00:00:06, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 74 messages, 0 notifications, 0 in queue
  Sent 73 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: fe80::eac5:7aff:fefe:97e0, Local port: 37116
Foreign host: fe80::eac5:7aff:fe8b:a82a, Foreign port: 179
Nexthop: 3.3.3.3
Nexthop global: fe80::eac5:7aff:fefe:97e0
Nexthop local: fe80::eac5:7aff:fefe:97e0
BGP connection: shared network
```

Leaf 2

```
Leaf2#show ip bgp neighbors
BGP neighbor is 10.10.10.2, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 4.4.4.4, remote router ID 1.1.1.1
  BGP state = Established, up for 00:23:24
  Last read 00:00:09, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 56 messages, 0 notifications, 0 in queue
  Sent 57 messages, 0 notifications, 0 in queue
```

 © 2021 IP Infusion Inc. Proprietary

```
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.10.3, Local port: 49242
Foreign host: 10.10.10.2, Foreign port: 179
Nexthop: 10.10.10.3
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is fe80::ce37:abff:fe3f:9f63, remote AS 100, local AS 100, internal
 link
  BGP version 4, local router ID 4.4.4.4, remote router ID 2.2.2.2
  BGP state = Established, up for 00:30:09
  Last read 00:00:08, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 72 messages, 0 notifications, 0 in queue
  Sent 72 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: fe80::36ef:b6ff:fe31:dd3f, Local port: 33368
Foreign host: fe80::ce37:abff:fe3f:9f63, Foreign port: 179
Nexthop: 4.4.4.4
Nexthop global: fe80::36ef:b6ff:fe31:dd3f
Nexthop local: fe80::36ef:b6ff:fe31:dd3f
BGP connection: shared network
```

BGP Blackhole Community Attribute

A blackhole route is used to forward unwanted or undesirable traffic into a black hole. In other words, a special logical interface called a null interface, is used to create the black hole. Static routes are created for destinations that are not

desirable, and the static route configuration points to the null interface. Any traffic that has a destination address that has a best match of the black hole static route automatically will be dropped.

Note: 65535:666 is reserved for Blackhole community.

Topology

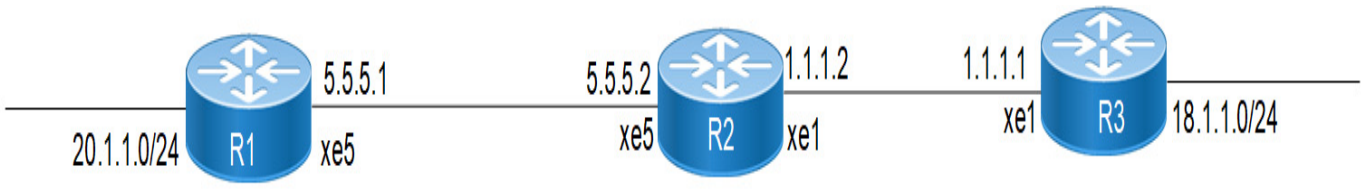


Figure 9-177: BGP Blackhole Community Attribute topology

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface xe5`	Enter Interface mode
`(config-if)# ip address 5.5.5.1/24`	Assign IP address to interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe20`	Enter Interface mode
`(config-if)# ip address 20.1.1.1/24`	Assign IP address to interface
`(config-if)#exit`	Exit interface mode
`(config)# router bgp 100`	Enter Router BGP mode
`(config-router)# neighbor 5.5.5.2 remote-as 200`	Define BGP neighbors. 5.5.5.2 is the IP address of the neighbor (R2) and 200 is the neighbors AS number
`(config-router)# address-family ipv4 unicast`	Enter into BGP address family IPv4
`(config-router-af)#neighbor 5.5.5.2 activate`	Activate the neighbor
`(config-router-af)#network 20.1.1.0/24`	Advertise networks with prefix
`(config-router-af)# commit`	Commit the configurations
`(config-router-af)# end`	Return to privilege mode

R2

`#configure terminal`	Enter Configure mode.
`(config)#interface xe5`	Enter Interface mode
`(config-if)# ip address 5.5.5.2/24`	Assign IP address to interface
`(config-if)#exit`	Exit interface mode
`(config)#interface xe1`	Enter Interface mode
`(config-if)# ip address 1.1.1.2/24`	Assign IP address to interface
`(config-if)#exit`	Exit interface mode
`(config)# router bgp 200`	Enter Router BGP mode

© 2021 IP Infusion Inc. Proprietary

(config-router)# neighbor 5.5.5.1 remote-as 100	Define BGP neighbors. 5.5.5.1 is the IP address of the neighbor (R1) and 100 is the neighbors AS number
(config-router)# neighbor 1.1.1.1 remote-as 300	Define BGP neighbors. 1.1.1.1 is the IP address of the neighbor (R3) and 100 is the neighbors AS number
(config-router)# address-family ipv4 unicast	Enter into BGP address family IPv4
(config-router-af)#neighbor 5.5.5.1 activate	Activate the neighbor
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor
(config-router-af)# commit	Commit the configurations
(config-router-af)# end	Return to privilege mode

R3

#configure terminal	Enter Configure mode.
(config)#interface xe1	Enter Interface mode
(config-if)# ip address 1.1.1.1/24	Assign IP address to interface
(config-if)#exit	Exit interface mode
(config)#interface xe18	Enter Interface mode
(config-if)# ip address 18.1.1.1/24	Assign IP address to interface
(config-if)#exit	Exit interface mode
(config)# router bgp 300	Enter Router BGP mode
(config-router)# neighbor 1.1.1.2 remote-as 200	Define BGP neighbors. 1.1.1.2 is the IP address of the neighbor (R2) and 200 is the neighbors AS number
(config-router)# address-family ipv4 unicast	Enter into BGP address family IPv4
(config-router-af)#neighbor 1.1.1.2 activate	Activate the neighbor
(config-router-af)#network 18.1.1.0/24	Advertise networks with prefix
(config-router-af)# commit	Commit the configurations
(config-router-af)# end	Return to privilege mode

Black Hole configuration on R3

#configure terminal	Enter Configure mode.
(config)#route-map D permit 10	Enter Route-map mode to set the match operation
(config-route-map)#set community no-export 65535:666 additive	Configure Reserved Black hole community in Route-map mode
(config-route-map)#commit	Commit the configuration
(config-route-map)#exit	Return to configuration mode
(config)#router bgp 300	Enter Router BGP mode
(config-router)#address-family ipv4 unicast	Enter into BGP address family IPv4
(config-router-af)#neighbor 1.1.1.2 route-map D out	Apply Route-map for the neighbor 1.1.1.2 in out direction
(config-router-af)#commit	Commit the configurations
(config-router-af)#end	Return to privilege mode
#clear ip bgp * soft out	Soft reset after applying Route-map

Validation

R2

```
# show ip bgp community
BGP table version is 4, local router ID is 5.5.5.2
Status codes: s suppressed, d damped, h history, a add-path, * valid, > best,
i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf   Weight Path
*>   18.1.1.0/24      1.1.1.1               0        100       0   300 i

Total number of prefixes 1

#show ip bgp 18.1.1.0/24
BGP routing table entry for 18.1.1.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table, not advertised
to EBGP peer)
  Not advertised to any peer
  AS path:300
   Nexthop:1.1.1.1 from 1.1.1.1 (Remote Id:1.1.1.1)
      Origin IGP, metric 0, localpref 100      valid, external, best, source
safi: 1
      Community: 65535:666 no-export
      Not advertised to any peer
      Last update: Tue Apr 16 21:48:01 2019

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            1.1.1.0/24 is directly connected, xe1, 00:10:22
C            5.5.5.0/24 is directly connected, xe5, 00:10:49
B            18.1.1.0/24 [20/0] is a summary, Null, 00:02:00
B            20.1.1.0/24 [20/0] via 5.5.5.1, xe5, 00:05:46
C            127.0.0.0/8 is directly connected, lo, 00:35:31

Gateway of last resort is not set
```

R1

```
#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
```


© 2021 IP Infusion Inc. Proprietary

```
       * - candidate default

IP Route Table for VRF "default"
C            5.5.5.0/24 is directly connected, xe5, 00:15:41
C            20.1.1.0/24 is directly connected, xe20, 00:14:06
C            127.0.0.0/8 is directly connected, lo, 00:37:28

Gateway of last resort is not set
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 10 BGP Labeled Unicast

As well as distributing routes, BGP with Multiprotocol Extensions (MP-BGP) can advertise MPLS label mappings that are mapped to routes. BGP Labeled Unicast (BGP-LU) attaches an MPLS label to an advertised IGP prefix and distributes the MPLS label mapped to the prefix to its peers.

With BGP-LU, a network can be divided into multiple regions to limit the total number of LSPs and enable failures to be contained and restored in a single region These regions operate separate instances of the IGP and use BGP-LU to advertise route information between inter-region routers.

A configuration for BGP-LU uses these type of nodes:

- Provider Edge (PE) nodes advertise label bindings to remote PEs in other regions. These advertisements only affect the PE routers and the ABRs and not provider routers (“P”) in the core network.
- Area Border Router (ABR) nodes advertise the label bindings to remote PEs in other regions.

BGP Labeled Unicast as Transport

Topology

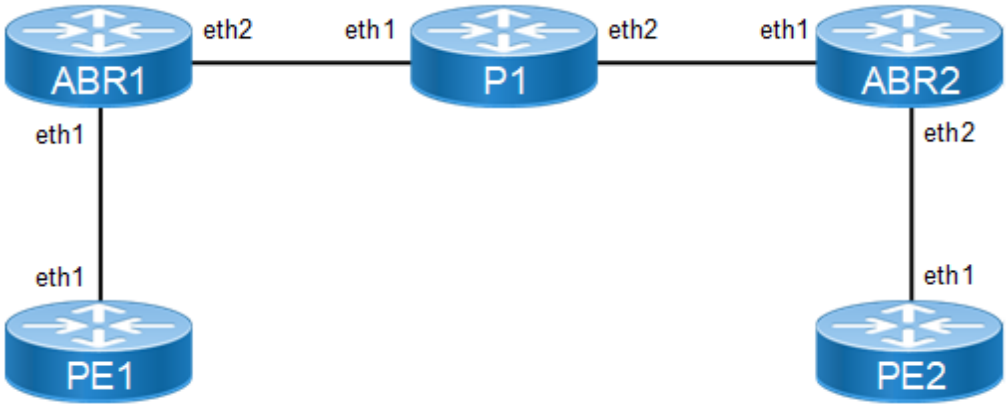


Figure 10-178: BGP labeled unicast

Configuration

PE1

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 11.11.11.55/32 secondary`	Configure the IP address of the interface loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface xe16`	Enter interface mode

(config-if)#ip address 172.4.5.55/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process OSPF with process Id 1
(config-router)#network 172.4.5.0/24 area 0	Define the interface (172.4.5.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 11.11.11.55/32 area 0	Define the interface (11.11.11.55/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)# neighbor 21.21.21.56 update-source lo	Add loopback ip of PE2 as neighbor with neighbor AS
(config-router)#neighbor 21.21.21.56 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#neighbor 172.4.5.52 remote-as 100	Add neighbor with neighbor AS
(config-router)#allocate-label all	Allocate labels
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 172.4.5.52 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#exit-address-family	Exit from address family IPv4 labeled unicast
(config-router)#address-family vpnv4 unicast	Enter into vpnv4 unicast address family
(config-router-af)#neighbor 21.21.21.56 activate	Activate the neighbor inside vpnv4 address family
(config-router-af)#exit-address-family	Exit from address family vpnv4.
(config-router)#address-family ipv4 unicast	Enter into ipv4 unicast address family
(config-router-af)#network 11.11.11.55/32	Advertise the loopback of RTR1 in BGP
(config-router-af)#exit-address-family	Exit from address family vpnv4
(config-router)#exit	Exit from router BGP mode
(config)# ip vrf vrf1	Specify the name of the VRF (vrf1) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 100:300	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface xe10	Enter interface mode
(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 172.10.20.55/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode

© 2021 IP Infusion Inc. Proprietary

(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router-af)# redistribute connected	Redistribute connected routes
(config-router-af)#end	Exit from router mode into privilege mode

ABR1

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 22.22.22.52/32 secondary	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface xe16	Enter interface mode
(config-if)#ip address 172.4.5.52/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#interface xe12	Enter interface mode
(config-if)#ip address 172.6.7.52/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process OSPF with process Id 1
(config-router)#network 172.4.5.0/24 area 0	Define the interface (172.4.5.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 172.6.7.0/24 area 0	Define the interface (172.6.7.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)# neighbor 172.4.5.55 remote-as 100	Add neighbor with neighbor AS
(config-router)# neighbor 172.6.7.54 remote-as 100	Add neighbor with neighbor AS
(config-router)#allocate-label all	Allocate labels
(config-router)# address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 172.6.7.54 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#neighbor 172.4.5.55 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)# neighbor 172.4.5.55 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 172.6.7.54 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 172.4.5.55 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast

(config-router-af)# neighbor 172.6.7.54 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)#exit-address-family	Exit address-family mode
(config-router)#exit	Exit from router BGP mode
(config)#end	Exit from config mode

P1

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)# ip address 200.200.200.54/32 secondary	Configure the IP address of the interface loopbak
(config-if)#exit	Exit interface mode
(config)#interface xe16	Enter interface mode
(config-if)#ip address 172.1.2.54/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#interface xe12	Enter interface mode
(config-if)#ip address 172.6.7.54/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process OSPF with process Id 1
(config-router)#network 172.1.2.0/24 area 0	Define the interface (172.1.2.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 172.6.7.0/24 area 0	Define the interface (172.6.7.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)# neighbor 172.1.2.53 remote-as 100	Add neighbor with neighbor AS
(config-router)# neighbor 172.6.7.52 remote-as 100	Add neighbor with neighbor AS
(config-router)#allocate-label all	Allocate labels
(config-router)# address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 172.6.7.52 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#neighbor 172.1.2.53 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)# neighbor 172.1.2.53 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 172.6.7.52 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast

© 2021 IP Infusion Inc. Proprietary

(config-router-af)# neighbor 172.1.2.53 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 172.6.7.52 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router)# exit-address-family	Exit from address family.
(config-router)#exit	Exit from router BGP mode
(config)#end	Exit from config mode

ABR2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)# ip address 44.44.44.53/32 secondary	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface xe16	Enter interface mode
(config-if)#ip address 172.1.2.53/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#interface xe10	Enter interface mode
(config-if)#ip address 172.3.4.53/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process OSPF with process Id 1
(config-router)#network 172.1.2.0/24 area 0	Define the interface (172.1.2.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 172.3.4.0/24 area 0	Define the interface (172.3.4.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)# neighbor 172.1.2.54 remote-as 100	Add neighbor with neighbor AS
(config-router)# neighbor 172.3.4.56 remote-as 100	Add neighbor with neighbor AS
(config-router)#allocate-label all	Allocate labels
(config-router)# address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 172.3.4.56 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#neighbor 172.1.2.54 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)# neighbor 172.3.4.56 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast

`(config-router-af)# neighbor 172.1.2.54 route-reflector-client`	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
`(config-router-af)# neighbor 172.3.4.56 next-hop-self`	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
`(config-router-af)# neighbor 172.1.2.54 next-hop-self`	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
`(config-router-af)#exit-address-family`	Exit from address family vpnv4
`(config-router)#exit`	Exit from router BGP mode
`(config)#end`	Exit from config mode

PE2

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 21.21.21.56/32 secondary`	Configure the IP address of the interface loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface xe10`	Enter interface mode
`(config-if)#ip address 172.3.4.56/24`	Configure the IP address of the interface eth1
`(config-if)#label-switching`	Enable label-switching on interface eth1
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process OSPF with process Id 1
`(config-router)#network 172.3.4.0/24 area 0`	Define the interface (172.3.4.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 21.21.21.56/32 area 0`	Define the interface (21.21.21.56/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#exit`	Exit from router ospf mode
`(config)#router bgp 100`	Enter Router BGP mode
`(config-router)#neighbor 11.11.11.55 remote-as 100`	Add loopback ip of PE1 as neighbor with neighbor AS
`(config-router)#neighbor 11.11.11.55 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)# neighbor 172.3.4.53 remote-as 100`	Add neighbor with neighbor AS
`(config-router)#allocate-label all`	Allocate labels
`(config-router)# address-family ipv4 labeled-unicast`	Enter into labeled-unicast address family
`(config-router-af)#neighbor 172.3.4.53 activate`	Activate the neighbor inside labeled-unicast address family
`(config-router-af)#exit-address-family`	Exit from address family IPv4 labeled unicast
`(config-router)#address-family  vpnv4 unicast`	Enter into vpnv4 unicast address family
`(config-router-af)#neighbor 11.11.11.55 activate`	Activate the neighbor inside vpnv4 address family
`(config-router-af)#exit-address-family`	Exit from address family vpnv4

© 2021 IP Infusion Inc. Proprietary

(config-router-af)#network 21.21.21.56/32	Advertise the loopback in BGP
(config-router-af)#exit-address-family	Exit from address family ipv4 unicast
(config-router)#exit	Exit from router BGP mode
(config)# ip vrf vrf1	Specify the name of the VRF (vrf1) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 100:300	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface xe0	Enter interface mode
(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 172.23.4.56/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router)# redistribute connected	Redistribute connected routes
(config-router)#end	Exit from router mode into privilege mode

Validation

PE1

```
PE1#show ip bgp neighbors 21.21.21.56
BGP neighbor is 21.21.21.56, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 11.11.11.55, remote router ID 21.21.21.56
  BGP state = Established, up for 00:01:32
  Last read 00:00:21, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family VPNv4 Unicast: advertised and received
  Received 7 messages, 0 notifications, 0 in queue
  Sent 9 messages, 0 notifications, 0 in queue
  Route refresh request: received 1, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: VPNv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 11.11.11.55, Local port: 179
Foreign host: 21.21.21.56, Foreign port: 38231
Nexthop: 11.11.11.55
Nexthop global: ::
Nexthop local: ::
```

```
BGP connection: non shared network


PE1#show ip bgp neighbors 172.4.5.52
BGP neighbor is 172.4.5.52, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 11.11.11.55, remote router ID 22.22.22.52
  BGP state = Established, up for 00:26:00
  Last read 00:00:07, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 67 messages, 2 notifications, 0 in queue
  Sent 70 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Labeled-Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 3; dropped 2
Local host: 172.4.5.55, Local port: 179
Foreign host: 172.4.5.52, Foreign port: 34324
Nexthop: 172.4.5.55
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:26:00, due to Administratively Reset (Cease Notification sent)
Notification Error Message: (Cease/Administratively Reset.)

PE1#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
S - stale
     Network          Next Hop        In Label     Out Label
*>  11.11.11.55/32   0.0.0.0          24320          -
*>i 21.21.21.56/32   172.4.5.52       24322        24321

PE1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type
O
ut-Label    Out-Intf    ELC   Nexthop
   B>   21.21.21.56/32      1         2         -           -     LSP_DEFAULT
2
4321        xe16        No    172.4.5.52
PE1#

PE1#show mpls ilm-table
```


© 2021 IP Infusion Inc. Proprietary

```
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown

Code    FEC/VRF/L2CKT    ILM-ID      In-Label    Out-Label   In-Intf    Out-
Intf
/VRF       Nexthop                  LSP-Type
   B>   vrf1               2          24321       Nolabel     N/A        vrf1
           N/A                      LSP_DEFAULT
   B>   11.11.11.55/32     1          24320       Nolabel     N/A        N/A
           127.0.0.1                LSP_DEFAULT
   B>   21.21.21.56/32     3          24322       24321       N/A        N/A
           172.4.5.52               LSP_DEFAULT
PE1#
```

ABR1

```
ABR1#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 1 VRF(default):
Neighbor ID    Pri   State           Dead Time   Address         Interface
Instance ID
11.11.11.55      1   Full/DR         00:00:35   172.4.5.55     xe16
0
200.200.200.54   1   Full/Backup     00:00:32   172.6.7.54     xe12
0
ABR1#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 11.11.11.55/32   172.4.5.55        24320        24320
*>i 21.21.21.56/32   172.6.7.54        24321        24321

ABR1#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 11.11.11.55/32   172.4.5.55        24320        24320
*>i 21.21.21.56/32   172.6.7.54        24321        24321

ABR1#show mpls forwarding-table | include 11.11.11.55
   B>    11.11.11.55/32     1       0          Yes   LSP_DEFAULT    24320
xe16         No         172.4.5.55
```

P1

```
P1#show ip bgp neighbors 172.6.7.52
BGP neighbor is 172.6.7.52, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 200.200.200.54, remote router ID 22.22.22.52
```

```
  BGP state = Established, up for 01:33:27
  Last read 00:00:12, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 229 messages, 0 notifications, 0 in queue
  Sent 227 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Labeled-Unicast
  BGP table version 7, neighbor version 7
  Index 1, Offset 0, Mask 0x2
  Route-Reflector Client
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 3; dropped 2
Local host: 172.6.7.54, Local port: 47560
Foreign host: 172.6.7.52, Foreign port: 179
Nexthop: 172.6.7.54
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 01:33:32, due to Configuration Change (Cease Notification sent)
Notification Error Message: (Cease/Other Configuration Change.)

P1#show ip bgp neighbors 172.1.2.53
BGP neighbor is 172.1.2.53, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 200.200.200.54, remote router ID 44.44.44.53
  BGP state = Established, up for 01:35:08
  Last read 00:00:19, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 230 messages, 2 notifications, 0 in queue
  Sent 233 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Labeled-Unicast
  BGP table version 7, neighbor version 7
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 3; dropped 2
Local host: 172.1.2.54, Local port: 179
Foreign host: 172.1.2.53, Foreign port: 58824
Nexthop: 172.1.2.54
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

 © 2021 IP Infusion Inc. Proprietary

```
Last Reset: 01:35:13, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

P1#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 11.11.11.55/32   172.6.7.52        24320        24320
*>i 21.21.21.56/32   172.1.2.53        24321        24321

P1#show mpls forwarding-table | include 11.11.11.55
   B>   11.11.11.55/32      1          1          -           -     LSP_DEFAULT
24320        xe12        No    172.6.7.52
```

ABR2

```
ABR2#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
S - stale
     Network          Next Hop        In Label     Out Label
*>i 11.11.11.55/32   172.1.2.54        24320        24320
*>i 21.21.21.56/32   172.3.4.56        24321        24321

ABR2#show mpls forwarding-table | include 11.11.11.55
   B>   11.11.11.55/32      1          1          -           -     LSP_DEFAULT
24320        xe16        No    172.1.2.54

PE2#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 11.11.11.55/32   172.3.4.53        24320        24320
*>  21.21.21.56/32   0.0.0.0           24321          -

PE2#show mpls forwarding-table | include 11.11.11.55
   B>   11.11.11.55/32      1          1          -           -     LSP_DEFAULT
24320        xe10        No    172.3.4.53

PE2#show mpls ftn-table
 Primary FTN entry with FEC: 11.11.11.55/32, id: 1, row status: Active,
Tunnel-Policy: N/A
  Owner: BGP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0,
Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: BGP, Stale: NO, out intf: xe10, out
label: 24320
    Nexthop addr: 172.3.4.53        cross connect ix: 1, op code: Push

PE2#show mpls vrf-table
Output for IPv4 VRF table with id: 2
```

```
 Primary FTN entry with FEC: 172.10.20.0/24, id: 1, row status: Active,
Tunnel-Policy: N/A
  Owner: BGP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0,
Incoming DSCP: none
  Transport Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 2
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: BGP, Stale: NO, BGP out intf: xe10,
transport out intf: xe10, out label: 24321
    Nexthop addr: 11.11.11.55        cross connect ix: 3, op code: Push and
Lookup


PE2#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown

Code    FEC/VRF/L2CKT    ILM-ID      In-Label    Out-Label   In-Intf    Out-
Intf/VRF       Nexthop                  LSP-Type
  B>  21.21.21.56/32    2         24321      Nolabel    N/A       N/A
127.0.0.1                 LSP_DEFAULT
  B>  11.11.11.55/32    1         24320      24320      N/A       N/A
172.3.4.53                LSP_DEFAULT
  B>  vrf1              3         24322      Nolabel    N/A       vrf1
N/A                       LSP_DEFAULT
```

BGP Labeled Unicast with Seamless MPLS

Topology

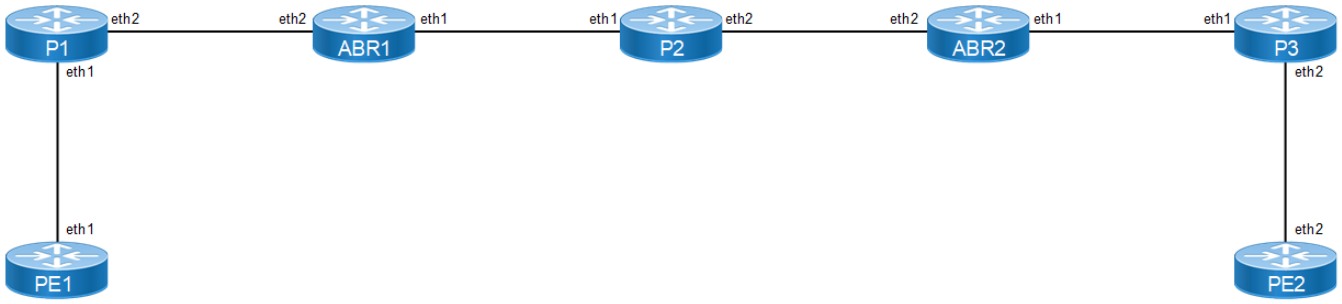


Figure 10-179: BGP_LU with MPLS

© 2021 IP Infusion Inc. Proprietary

Configuration

PE1

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 1.1.1.54/32 secondary`	Configure the IP address of the interface loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 10.1.1.54/24`	Configure the IP address of the interface eth1
`(config-if)#label-switching`	Enable label-switching on interface eth1
`(config-if)# enable-ldp ipv4`	Enable LDP process on eth1 interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 10`	Configure the routing process OSPF with process id 10
`(config-router)#network 1.1.1.54/32 area 0`	Define the interface (1.1.1.54/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 10.1.1.0/24 area 0`	Define the interface (10.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#exit`	Exit from router ospf mode
`(config)#router bgp 100`	Enter Router BGP mode
`(config-router)#neighbor 7.7.7.55 remote-as 100`	Add loopback ip of PE2 as neighbor with neighbor AS
`(config-router)#neighbor 7.7.7.55 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#neighbor 3.3.3.52 remote-as 100`	Add loopback ip of ABR1 as neighbor with neighbor AS
`(config-router)#neighbor 3.3.3.52 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#allocate-label all`	Allocate labels
`(config-router)#address-family ipv4 labeled-unicast`	Enter into labeled-unicast address family
`(config-router-af)#neighbor 3.3.3.52 activate`	Activate the neighbor inside labeled-unicast address family
`(config-router-af)#exit-address-family`	Exit from address family IPv4 labeled unicast
`(config-router)#address-family  vpnv4 unicast`	Enter into vpnv4 unicast address family
`(config-router-af)#neighbor 7.7.7.55 activate`	Activate the neighbor inside vpnv4 address family
`(config-router)#address-family ipv4 labeled-unicast`	Enter into labeled-unicast address family
`(config-router)#address-family ipv4 unicast`	Enter into ipv4 unicast address family
`(config-router-af)#network 1.1.1.54/32`	Advertise the loopback of RTR1 in BGP
`(config-router-af)#exit-address-family`	Exit from address family
`(config-router)#exit`	Exit from router BGP mode

(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 1.1.1.54 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip vrf vrf1	Specify the name of the VRF (vrf1) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 100:300	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth2	Enter interface mode
(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 61.1.1.54/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router-af)# redistribute connected	Redistribute connected routes
(config-router-af)#end	Exit from router mode into privilege mode

P1

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 2.2.2.23/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 10.1.1.23/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 20.1.1.23/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 10	Configure the routing process OSPF with process id 10
(config-router)#network 20.1.1.0/24 area 0	Define the interface (20.1.1.0/24)) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 10.1.1.0/24 area 0	Define the interface (10.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).

© 2021 IP Infusion Inc. Proprietary

(config-router)#network 2.2.2.23/32 area 0	Define the interface (2.2.2.23/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 2.2.2.23 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip route 7.7.7.55/32 20.1.1.52	Specify the destination prefix and mask for the network and a gateway.
(config)# end	Exit from config mode

ABR1

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 3.3.3.52/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 30.1.1.52/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 20.1.1.52/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 20	Configure the routing process OSPF with process id 20
(config-router)#network 3.3.3.52/32 area 0	Define the interface (3.3.3.52/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 20.1.1.0/24 area 0	Define the interface (20.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 3.3.3.52 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)#neighbor 1.1.1.54 remote-as 100	Add loopback ip of PE2 as neighbor with neighbor AS

(config-router)#neighbor 1.1.1.54 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#neighbor 5.5.5.56 remote-as 100	Add loopback ip of ABR1 as neighbor with neighbor AS
(config-router)#neighbor 5.5.5.56 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#allocate-label all	Allocate labels
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 1.1.1.54 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#neighbor 5.5.5.56 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)# neighbor 1.1.1.54 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 5.5.5.56 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 1.1.1.54 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 5.5.5.56 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)#exit-address-family	Exit from address family labeled-unicast
(config-router)#exit	Exit from router BGP mode

P2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 4.4.4.53/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 30.1.1.53/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 40.1.1.53/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode
(config)#router ospf 20	Configure the routing process OSPF with process id 20
(config-router)#network 30.1.1.0/24 area 0	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 40.1.1.0/24 area 0	Define the interface (40.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).

© 2021 IP Infusion Inc. Proprietary

(config-router)#network 4.4.4.53/32 area 0	Define the interface (4.4.4.53/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 4.4.4.53 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode

ABR2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 5.5.5.56/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 50.1.1.56/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 40.1.1.56/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 30	Configure the routing process OSPF with process id 20
(config-router)#network 5.5.5.56/32 area 0	Define the interface 5.5.5.56/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 50.1.1.0/24 area 0	Define the interface (50.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router ospf 20	Configure the routing process OSPF with process id 20
(config-router)#network 5.5.5.56/32 area 0	Define the interface 5.5.5.56/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 40.1.1.0/24 area 0	Define the interface (40.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 3.3.3.52 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode

(config)#router bgp 100	Enter Router BGP mode
(config-router)#neighbor 3.3.3.52 remote-as 100	Add loopback ip of PE2 as neighbor with neighbor AS
(config-router)#neighbor 3.3.3.52 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#neighbor 7.7.7.55 remote-as 100	Add loopback ip of ABR1 as neighbor with neighbor AS
(config-router)#neighbor 7.7.7.55 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 3.3.3.52 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#neighbor 7.7.7.55 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)# neighbor 3.3.3.52 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 7.7.7.55 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 3.3.3.52 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 7.7.7.55 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)#exit-address-family	Exit from address family labeled-unicast
(config-router)#exit	Exit from router BGP mode

P3

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 6.6.6.22/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 50.1.1.22/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 60.1.1.22/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode
(config)#router ospf 30	Configure the routing process OSPF with process id 20
(config-router)#network 50.1.1.0/24 area 0	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).

© 2021 IP Infusion Inc. Proprietary

(config-router)#network 60.1.1.0/24 area 0	Define the interface (40.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 6.6.6.22/32 area 0	Define the interface (4.4.4.53/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 6.6.6.22 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip route 1.1.1.54/32 50.1.1.56	Specify the destination prefix and mask for the network and a gateway.
(config)#exit	Exit from config mode

PE2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 7.7.7.55/32 secondary	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode
(config-if)#ip address 60.1.1.55/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 30	Configure the routing process OSPF with process id 10
(config-router)#network 7.7.7.55/32 area 0	Define the interface (7.7.7.55/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 60.1.1.0/24 area 0	Define the interface (60.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)#router bgp 100	Enter Router BGP mode
(config-router)#neighbor 1.1.1.54 remote-as 100	Add loopback ip of PE2 as neighbor with neighbor AS
(config-router)#neighbor 1.1.1.54 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#neighbor 5.5.5.56 remote-as 100	Add loopback ip of ABR1 as neighbor with neighbor AS
(config-router)#neighbor 5.5.5.56 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#allocate-label all	Allocate labels
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family

(config-router-af)#neighbor 5.5.5.56 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)#exit-address-family	Exit from address family IPv4 labeled unicast
(config-router)#address-family vpnv4 unicast	Enter into vpnv4 unicast address family
(config-router-af)#neighbor 1.1.1.54 activate	Activate the neighbor inside vpnv4 address family
(config-router-af)#exit-address-family	Exit from address family vpnv4
(config-router)#address-family ipv4 unicast	Enter into ipv4 unicast address family
(config-router-af)#network 7.7.7.55/32	Advertise the loopback of RTR1 in BGP
(config-router-af)#exit-address-family	Exit from address family
(config-router)#exit	Exit from router BGP mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 7.7.7.55 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip vrf vrf1	Specify the name of the VRF (vrf1) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 100:300	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth2	Enter interface mode
(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 62.1.1.55/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router-af)# redistribute connected	Redistribute connected routes
(config-router-af)#end	Exit from router mode into privilege mode

Validation

PE1

```
#show ip bgp neighbors 3.3.3.52
BGP neighbor is 3.3.3.52, remote AS 100, local AS 100, internal link
 BGP version 4, local router ID 1.1.1.54, remote router ID 3.3.3.52
 BGP state = Established, up for 00:00:06
 Last read 00:00:07, hold time is 90, keepalive interval is 30 seconds
Neighbor capabilities:
 Route refresh: advertised and received (old and new)
 Received 4 messages, 1 notifications, 0 in queue
 Sent 6 messages, 0 notifications, 0 in queue Route refresh request: received
0, sent 0
 Minimum time between advertisement runs is 5 seconds Update source is lo
 For address family: IPv4 Unicast
 BGP table version 1, neighbor version 1 Index 0, Offset 0, Mask 0x1
```


© 2021 IP Infusion Inc. Proprietary

```
 Community attribute sent to this neighbor (both)
 0accepted prefixes
 1announced prefixes

For address family: IPv4 Labeled-Unicast
BGP table version 1, neighbor version 1
Index 1, Offset 0, Mask 0x2
Community attribute sent to this neighbor (both)
0accepted prefixes
1announced prefixes

Connections established 2; dropped 1
Local host: 1.1.1.54, Local port: 179
Foreign host: 3.3.3.52, Foreign port: 46745
Nexthop: 1.1.1.54
Nexthop global: 54::54 Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:11, due to BGP Notification received Notification Error
Message: (Cease/Other Configuration Change.)

#show ip bgp neighbors 7.7.7.55
BGP neighbor is 7.7.7.55, remote AS 100, local AS 100, internal link
BGP version 4, local router ID 1.1.1.54, remote router ID 7.7.7.55
BGP state = Established, up for 00:01:10
Last read 00:00:11, hold time is 90, keepalive interval is 30 seconds Neighbor
capabilities:
Route refresh: advertised and received (old and new)
Received 8 messages, 1 notifications, 0 in queue
Sent 9 messages, 2 notifications, 0 in queue Route refresh request: received
0, sent 0
Minimum time between advertisement runs is 5 seconds Update source is lo
For address family: VPNv4 Unicast
BGP table version 3, neighbor version 3 Index 0, Offset 0, Mask 0x1
Community attribute sent to this neighbor (both)
1 accepted prefixes
1 announced prefixes

Connections established 3; dropped 2
Local host: 1.1.1.54, Local port: 179


Foreign host: 7.7.7.55, Foreign port: 58871
Nexthop: 1.1.1.54
Nexthop global: 54::54 Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:01:10, due to BGP Notification sent Notification Error Message:
(Cease/Administratively Reset.)


#show mpls vrf-table
Output for IPv4 VRF table with id: 2
Primary FTN entry with FEC: 62.1.1.0/24, id: 1, row status: Active
Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
Tunnel id: 0,Protected LSP id: 0, Description: N/A
Cross connect ix: 12, in intf: - in label: 0 out-segment ix: 11 Owner: BGP,
Persistent: No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 11, owner: BGP, out intf: eth1, out label: 24961 Nexthop
addr: 7.7.7.55cross connect ix: 12, op code: Push and
```

```
Lookup

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
NetworkNext HopIn LabelOut Label
*>1.1.1.54/320.0.0.024961-
*>i 7.7.7.55/323.3.3.52-24961
#show mpls forwarding-table | include 7.7.7.55
B>7.7.7.55/3240YesLSP_DEFAULT24961
eth13.3.3.52

#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM K - CLI ILM, T -
MPLS-TP, S - Stitched ILM

CodeFECILM-IDIn-LabelOut-LabelIn-IntfOut- IntfNexthopLSP-Type
>1.1.1.54/321124961N/AN/AN/A
127.0.0.1LSP_DEFAULT
>61.1.1.0/241324963N/AN/Aeth2
0.0.0.0LSP_DEFAULT

#show mpls ftn-table
Primary FTN entry with FEC: 2.2.2.23/32, id: 1, row status: Active
Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
Tunnel id: 0,Protected LSP id: 0, Description: N/A
Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1 Owner: LDP,
Persistent: No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 1, owner: LDP, out intf: eth1, out label: 3 Nexthop addr:
10.1.1.23cross connect ix: 1, op code: Push

Primary FTN entry with FEC: 3.3.3.52/32, id: 2, row status: Active
Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
Tunnel id: 0,Protected LSP id: 0, Description: N/A
Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2 Owner: LDP,
Persistent: No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 2, owner: LDP, out intf: eth1, out label: 24320


Nexthop addr: 10.1.1.23cross connect ix: 2, op code: Push

Primary FTN entry with FEC: 7.7.7.55/32, id: 4, row status: Active
Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
Tunnel id: 0,Protected LSP id: 0, Description: N/A
Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3 Owner: BGP,
Persistent: No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 3, owner: BGP, out intf: eth1, out label: 24961 Nexthop
addr: 3.3.3.52cross connect ix: 4, op code: Push and
Lookup


Primary FTN entry with FEC: 20.1.1.0/24, id: 3, row status: Active
Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
Tunnel id: 0,Protected LSP id: 0, Description: N/A
Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1 Owner: LDP,
Persistent: No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 1, owner: LDP, out intf: eth1, out label: 3 Nexthop addr:
10.1.1.23cross connect ix: 1, op code: Push
```

 © 2021 IP Infusion Inc. Proprietary

P1

```
#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 10 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.54          1   Full/Backup     00:00:38    10.1.1.54       eth1
0
3.3.3.52          1   Full/DR         00:00:39    20.1.1.52       eth2
0
#show ldp session
Peer IP Address           IF Name    My Role    State       KeepAlive  UpTime
1.1.1.54                  eth1       Active    OPERATIONAL   30    00:00:21
3.3.3.52                  eth2       Passive   OPERATIONAL   30    00:00:15
```

ABR1

```
#show ip bgp neighbors 1.1.1.54
BGP neighbor is 1.1.1.54, remote AS 100, local AS 100, internal link BGP
version 4, local router ID 3.3.3.52, remote router ID 1.1.1.54 BGP state =
Established, up for 00:00:09
Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds Neighbor
capabilities:
Route refresh: advertised and received (old and new) Address family IPv4
Unicast: advertised and received Address family IPv4 Labeled-Unicast:
advertised and received
Received 5 messages, 0 notifications, 0 in queue
Sent 4 messages, 1 notifications, 0 in queue Route refresh request: received
0, sent 0
Minimum time between advertisement runs is 5 seconds Update source is lo
For address family: IPv4 Unicast
BGP table version 1, neighbor version 1 Index 0, Offset 0, Mask 0x1
Community attribute sent to this neighbor (both)
1 accepted prefixes


0announced prefixes

For address family: IPv4 Labeled-UnicastBGP table version 2, neighbor version
2 Index 0, Offset 0, Mask 0x1
Route-Reflector Client NEXT_HOP is always this router
Community attribute sent to this neighbor (both)
1accepted prefixes
0announced prefixes

Connections established 2; dropped 1
Local host: 3.3.3.52, Local port: 46745
Foreign host: 1.1.1.54, Foreign port: 179
Nexthop: 3.3.3.52
Nexthop global: 52::52 Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:14, due to BGP Notification sent Notification Error Message:
(Cease/Other Configuration Change.)

#show ip bgp neighbors 5.5.5.56
```

```
BGP neighbor is 5.5.5.56, remote AS 100, local AS 100, internal link BGP
version 4, local router ID 3.3.3.52, remote router ID 5.5.5.56 BGP state =
Established, up for 00:00:11
Last read 00:00:02, hold time is 90, keepalive interval is 30 seconds Neighbor
capabilities:
Route refresh: advertised and received (old and new) Address family IPv4
Unicast: advertised and received Address family IPv4 Labeled-Unicast:
advertised and received
Received 4 messages, 0 notifications, 0 in queue
Sent 6 messages, 2 notifications, 0 in queue Route refresh request: received
0, sent 0
Minimum time between advertisement runs is 5 seconds Update source is lo
For address family: IPv4 Unicast
BGP table version 1, neighbor version 1 Index 1, Offset 0, Mask 0x2
Community attribute sent to this neighbor (both)
1 accepted prefixes
1 announced prefixes

For address family: IPv4 Labeled-UnicastBGP table version 3, neighbor version
2 Index 1, Offset 0, Mask 0x2
Route-Reflector Client NEXT_HOP is always this router
Community attribute sent to this neighbor (both)
1 accepted prefixes
1 announced prefixes

Connections established 2; dropped 1
Local host: 3.3.3.52, Local port: 179
Foreign host: 5.5.5.56, Foreign port: 40440
Nexthop: 3.3.3.52
Nexthop global: 52::52 Nexthop local: ::


BGP connection: non shared network
Last Reset: 00:00:11, due to BGP Notification sent Notification Error Message:
(Cease/Administratively Reset.)

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.54/32       1.1.1.54        24960        24961
*>i 7.7.7.55/32       5.5.5.56        24961        24961

#show mpls forwarding-table | include 1.1.1.54
   L>    1.1.1.54/32        1       0          Yes   LSP_DEFAULT     24321
eth2          20.1.1.23
   B     1.1.1.54/32        7       0          Yes   LSP_DEFAULT     24961
eth2          1.1.1.54

#show mpls forwarding-table | include 7.7.7.55
   B>    7.7.7.55/32        8       0          Yes   LSP_DEFAULT     24961
eth1          5.5.5.56

#show mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.54/32, id: 1, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
```


© 2021 IP Infusion Inc. Proprietary

```
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth2, out label: 24321
    Nexthop addr: 20.1.1.23        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 1.1.1.54/32, id: 7, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 11, in intf: - in label: 0 out-segment ix: 10
      Owner: BGP, Persistent: No, Admin Status: Down, Oper Status: Down
       Out-segment with ix: 10, owner: BGP, out intf: eth2, out label: 24961
    Nexthop addr: 1.1.1.54        cross connect ix: 11, op code: Push and
Lookup


 Primary FTN entry with FEC: 2.2.2.23/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 20.1.1.23        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 4.4.4.53/32, id: 4, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 30.1.1.53        cross connect ix: 7, op code: Push


 Primary FTN entry with FEC: 5.5.5.56/32, id: 5, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 10, in intf: - in label: 0 out-segment ix: 9
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 9, owner: LDP, out intf: eth1, out label: 24320
    Nexthop addr: 30.1.1.53        cross connect ix: 10, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 8, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 12, in intf: - in label: 0 out-segment ix: 11
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 11, owner: BGP, out intf: eth1, out label: 24961
    Nexthop addr: 5.5.5.56        cross connect ix: 12, op code: Push and
Lookup


 Primary FTN entry with FEC: 10.1.1.0/24, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
```

```
          Out-segment with ix: 4, owner: LDP, out intf: eth2, out label: 3
       Nexthop addr: 20.1.1.23        cross connect ix: 5, op code: Push


    Primary FTN entry with FEC: 40.1.1.0/24, id: 6, row status: Active
     Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
     Tunnel id: 0,   Protected LSP id: 0, Description: N/A
        Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
         Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
          Out-segment with ix: 6, owner: LDP, out intf: eth1, out label: 3
       Nexthop addr: 30.1.1.53        cross connect ix: 7, op code: Push
```

P2

```
#show ip ospf neighbor

Total number of full neighbors: 2 OSPF process 20 VRF(default):
Neighbor IDPriStateDead TimeAddressInterface Instance ID
3.3.3.521Full/Backup00:00:3930.1.1.52eth1
0
5.5.5.561Full/DR00:00:4040.1.1.56eth2
0

#show ldp session
Peer IP AddressIF NameMy RoleStateKeepAliveUpTime
3.3.3.52eth1ActiveOPERATIONAL3000:00:21
5.5.5.56eth2PassiveOPERATIONAL3000:00:19
```

ABR2

```
#show ip bgp neighbors 3.3.3.52


BGP neighbor is 3.3.3.52, remote AS 100, local AS 100, internal link BGP
version 4, local router ID 5.5.5.56, remote router ID 3.3.3.52 BGP state =
Established, up for 00:00:12
Last read 00:00:07, hold time is 90, keepalive interval is 30 seconds Neighbor
capabilities:
Route refresh: advertised and received (old and new) Address family IPv4
Unicast: advertised and received Address family IPv4 Labeled-Unicast:
advertised and received
Received 5 messages, 1 notifications, 0 in queue
Sent 5 messages, 0 notifications, 0 in queue Route refresh request: received
0, sent 0
Minimum time between advertisement runs is 5 seconds Update source is lo
For address family: IPv4 Unicast
BGP table version 1, neighbor version 1 Index 0, Offset 0, Mask 0x1
Community attribute sent to this neighbor (both)
1 accepted prefixes
1 announced prefixes

For address family: IPv4 Labeled-UnicastBGP table version 2, neighbor version
2 Index 0, Offset 0, Mask 0x1
Route-Reflector Client NEXT_HOP is always this router
Community attribute sent to this neighbor (both)
1 accepted prefixes
1 announced prefixes
```

 © 2021 IP Infusion Inc. Proprietary

```
Connections established 2; dropped 1
Local host: 5.5.5.56, Local port: 40440
Foreign host: 3.3.3.52, Foreign port: 179
Nexthop: 5.5.5.56
Nexthop global: 56::56 Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:17, due to BGP Notification received Notification Error
Message: (Cease/Other Configuration Change.)

#show ip bgp neighbors 7.7.7.55
BGP neighbor is 7.7.7.55, remote AS 100, local AS 100, internal link BGP
version 4, local router ID 5.5.5.56, remote router ID 7.7.7.55 BGP state =
Established, up for 00:00:13
Last read 00:00:08, hold time is 90, keepalive interval is 30 seconds Neighbor
capabilities:
Route refresh: advertised and received (old and new) Address family IPv4
Unicast: advertised and received Address family IPv4 Labeled-Unicast:
advertised and received
Received 3 messages, 0 notifications, 0 in queue
Sent 4 messages, 0 notifications, 0 in queue Route refresh request: received
0, sent 0
Minimum time between advertisement runs is 5 seconds Update source is lo
For address family: IPv4 Unicast
BGP table version 1, neighbor version 1 Index 1, Offset 0, Mask 0x2
Community attribute sent to this neighbor (both)


1 accepted prefixes
1 announced prefixes

For address family: IPv4 Labeled-UnicastBGP table version 2, neighbor version
2 Index 1, Offset 0, Mask 0x2
Route-Reflector Client NEXT_HOP is always this router
Community attribute sent to this neighbor (both)
1 accepted prefixes
1 announced prefixes

Connections established 1; dropped 0
Local host: 5.5.5.56, Local port: 35004
Foreign host: 7.7.7.55, Foreign port: 179
Nexthop: 5.5.5.56
Nexthop global: 56::56 Nexthop local: ::
BGP connection: non shared network

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.54/32       3.3.3.52        24960        24960
*>i 7.7.7.55/32       7.7.7.55        24961        24960

#show mpls forwarding-table | include 1.1.1.54
   B>    1.1.1.54/32        7       0          Yes   LSP_DEFAULT    24960
eth2           3.3.3.52

#show mpls forwarding-table | include 7.7.7.55
   L>    7.7.7.55/32        5       0          Yes   LSP_DEFAULT    24320
eth1            50.1.1.22
```

```
   B     7.7.7.55/32        8       0          Yes   LSP_DEFAULT     24960
eth1            7.7.7.55

#show mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.54/32, id: 7, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 11, in intf: - in label: 0 out-segment ix: 10
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 10, owner: BGP, out intf: eth2, out label: 24960
    Nexthop addr: 3.3.3.52        cross connect ix: 11, op code: Push and
Lookup


 Primary FTN entry with FEC: 3.3.3.52/32, id: 1, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: eth2, out label: 24321
    Nexthop addr: 40.1.1.53        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 4.4.4.53/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 40.1.1.53        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 6.6.6.22/32, id: 4, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 50.1.1.22        cross connect ix: 7, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 5, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 10, in intf: - in label: 0 out-segment ix: 9
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 9, owner: LDP, out intf: eth1, out label: 24320
    Nexthop addr: 50.1.1.22        cross connect ix: 10, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 8, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 12, in intf: - in label: 0 out-segment ix: 11
      Owner: BGP, Persistent: No, Admin Status: Down, Oper Status: Down
       Out-segment with ix: 11, owner: BGP, out intf: eth1, out label: 24960
```


© 2021 IP Infusion Inc. Proprietary

```
    Nexthop addr: 7.7.7.55        cross connect ix: 12, op code: Push and
Lookup


 Primary FTN entry with FEC: 30.1.1.0/24, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 40.1.1.53        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 60.1.1.0/24, id: 6, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 50.1.1.22        cross connect ix: 7, op code: Push
```

P3

```
#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 30 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
5.5.5.56          1   Full/Backup     00:00:39    50.1.1.56       eth1
0
7.7.7.55          1   Full/DR         00:00:39    60.1.1.55       eth2
0

#show ldp session
Peer IP Address           IF Name    My Role    State       KeepAlive  UpTime
5.5.5.56                  eth1        Active    OPERATIONAL   30    00:00:30
7.7.7.55                  eth2       Passive   OPERATIONAL   30    00:00:28
```

PE2

```
#show ip bgp neighbors 5.5.5.56
BGP neighbor is 5.5.5.56, remote AS 100, local AS 100, internal link BGP
version 4, local router ID 7.7.7.55, remote router ID 5.5.5.56 BGP state =
Established, up for 00:00:16
Last read 00:00:11, hold time is 90, keepalive interval is 30 seconds Neighbor
capabilities:
Route refresh: advertised and received (old and new) Address family IPv4
Unicast: advertised and received Address family IPv4 Labeled-Unicast:
advertised and received
Received 3 messages, 0 notifications, 0 in queue
Sent 4 messages, 0 notifications, 0 in queue Route refresh request: received
0, sent 0
Minimum time between advertisement runs is 5 seconds Update source is lo
For address family: IPv4 Unicast
BGP table version 1, neighbor version 1 Index 1, Offset 0, Mask 0x2
Community attribute sent to this neighbor (both)
1 accepted prefixes
1 announced prefixes
```

```
For address family: IPv4 Labeled-UnicastBGP table version 2, neighbor version
2 Index 1, Offset 0, Mask 0x2
Community attribute sent to this neighbor (both)
1 accepted prefixes
1 announced prefixes

Connections established 1; dropped 0
Local host: 7.7.7.55, Local port: 179
Foreign host: 5.5.5.56, Foreign port: 35004
Nexthop: 7.7.7.55
Nexthop global: 55::55 Nexthop local: ::
BGP connection: non shared network

#show mpls vrf-table
Output for IPv4 VRF table with id: 2
Primary FTN entry with FEC: 61.1.1.0/24, id: 1, row status: Active
Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
Tunnel id: 0,Protected LSP id: 0, Description: N/A
Cross connect ix: 11, in intf: - in label: 0 out-segment ix: 10


Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 10, owner: BGP, out intf: eth2, out label: 24963 Nexthop
addr: 1.1.1.54cross connect ix: 11, op code: Push and
Lookup

#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
NetworkNext HopIn LabelOut Label
*>i 1.1.1.54/325.5.5.56-24960
*>7.7.7.55/320.0.0.024960-
#show mpls forwarding-table | include 1.1.1.54
B>1.1.1.54/3240YesLSP_DEFAULT24960
eth25.5.5.56

#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM K - CLI ILM, T -
MPLS-TP, S - Stitched ILM

CodeFECILM-IDIn-LabelOut-LabelIn-IntfOut- IntfNexthopLSP-Type
>7.7.7.55/32924960N/AN/AN/A
127.0.0.1LSP_DEFAULT
>62.1.1.0/241024961N/AN/Aeth1
0.0.0.0LSP_DEFAULT

#show mpls ftn-table
Primary FTN entry with FEC: 1.1.1.54/32, id: 4, row status: Active
Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
Tunnel id: 0,Protected LSP id: 0, Description: N/A
Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3 Owner: BGP,
Persistent: No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 3, owner: BGP, out intf: eth2, out label: 24960 Nexthop
addr: 5.5.5.56cross connect ix: 4, op code: Push and
Lookup

Primary FTN entry with FEC: 5.5.5.56/32, id: 1, row status: Active
```

 © 2021 IP Infusion Inc. Proprietary

```
Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
Tunnel id: 0,Protected LSP id: 0, Description: N/A
Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1 Owner: LDP,
Persistent: No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 1, owner: LDP, out intf: eth2, out label: 24321 Nexthop
addr: 60.1.1.22cross connect ix: 1, op code: Push

Primary FTN entry with FEC: 6.6.6.22/32, id: 2, row status: Active
Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
Tunnel id: 0,Protected LSP id: 0, Description: N/A
Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2 Owner: LDP,
Persistent: No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 2, owner: LDP, out intf: eth2, out label: 3 Nexthop addr:
60.1.1.22cross connect ix: 2, op code: Push

Primary FTN entry with FEC: 50.1.1.0/24, id: 3, row status: Active


Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
Tunnel id: 0,Protected LSP id: 0, Description: N/A
Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2 Owner: LDP,
Persistent: No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 2, owner: LDP, out intf: eth2, out label: 3 Nexthop addr:
60.1.1.22cross connect ix: 2, op code: Push
```

BGP Labeled Unicast with Inter-AS

Topology

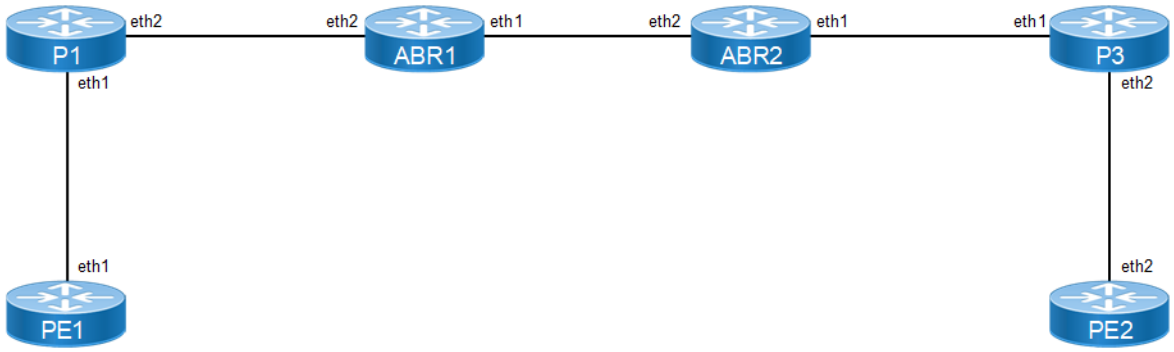


Figure 10-180: BGP Labeled unicast with Inter-AS

Configurations

PE1

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 1.1.1.54/32 secondary`	Configure the IP address of the interface loopback
`(config-if)#exit`	Exit interface mode

`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 10.1.1.54/24`	Configure the IP address of the interface eth1
`(config-if)#label-switching`	Enable label-switching on interface eth1
`(config-if)# enable-ldp ipv4`	Enable LDP process on eth1 interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 10`	Configure the routing process OSPF with process id 10
`(config-router)#network 1.1.1.54/32 area 0`	Define the interface (1.1.1.54/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 10.1.1.0/24 area 0`	Define the interface (10.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#exit`	Exit from router ospf mode
`(config)#router bgp 100`	Enter Router BGP mode
`(config-router)#neighbor 7.7.7.55 remote-as 100`	Add loopback ip of PE2 as neighbor with neighbor AS
`(config-router)#neighbor 7.7.7.55 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#neighbor 3.3.3.52 remote-as 100`	Add loopback ip of ABR1 as neighbor with neighbor AS
`(config-router)#neighbor 3.3.3.52 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#allocate-label all`	Allocate labels
`(config-router)#address-family ipv4 labeled-unicast`	Enter into labeled-unicast address family
`(config-router-af)#neighbor 3.3.3.52 activate`	Activate the neighbor inside labeled-unicast address family
`(config-router-af)#exit-address-family`	Exit from address family IPv4 labeled unicast
`(config-router)#address-family  vpnv4 unicast`	Enter into vpnv4 unicast address family
`(config-router-af)#neighbor 7.7.7.55 activate`	Activate the neighbor inside vpnv4 address family
`(config-router-af)#network 1.1.1.54/32`	Advertise the loopback of RTR1 in BGP
`(config-router-af)#exit-address-family`	Exit from address family vpnv4
`(config-router)#exit`	Exit from router BGP mode
`(config)# router ldp`	Configure Router LDP instance
`(config-router)# transport-address ipv4 1.1.1.54 0`	Configure Transport address for LDP with label space value 0
`(config-router)#exit`	Exit from router mode
`(config)# ip vrf vrf1`	Specify the name of the VRF (vrf1) to be created.
`(config-vrf)#rd 10:100`	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
`(config-vrf)#route-target both 100:300`	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
`(config-vrf)#exit`	Exit VRF mode, and return to Configure mode.
`(config)#interface eth2`	Enter interface mode

© 2021 IP Infusion Inc. Proprietary

(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 61.1.1.54/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router-af)# redistribute connected	Redistribute connected routes
(config-router-af)#end	Exit from router mode into privilege mode

P1

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 2.2.2.23/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 10.1.1.23/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 20.1.1.23/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 10	Configure the routing process OSPF with process id 10
(config-router)#network 20.1.1.0/24 area 0	Define the interface (20.1.1.0/24)) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 10.1.1.0/24 area 0	Define the interface (10.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 2.2.2.23/32 area 0	Define the interface (2.2.2.23/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 2.2.2.23 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip route 7.7.7.55/32 20.1.1.52	Specify the destination prefix and mask for the network and a gateway.
(config)# end	Exit from config mode

ABR1

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 3.3.3.52/32`	Configure the IP address of the interface loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip address 52.56.1.52/24`	Configure the IP address of the interface eth1
`(config-if)#label-switching`	Enable label-switching on interface eth1
`(config-if)# enable-ldp ipv4`	Enable LDP process on eth1 interface
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 20.1.1.52/24`	Configure the IP address of the interface eth2
`(config-if)#label-switching`	Enable label-switching on interface eth2
`(config-if)# enable-ldp ipv4`	Enable LDP process on eth2 interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 10`	Configure the routing process OSPF with process id 20
`(config-router)#network 3.3.3.52/32 area 0`	Define the interface (3.3.3.52/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 20.1.1.0/24 area 0`	Define the interface (20.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#exit`	Exit from router ospf mode
`(config)# router ldp`	Configure Router LDP instance
`(config-router)# transport-address ipv4 3.3.3.52 0`	Configure Transport address for LDP with label space value 0
`(config-router)#exit`	Exit from router mode
`(config)#router bgp 100`	Enter Router BGP mode
`(config-router)#neighbor 1.1.1.54 remote-as 100`	Add loopback ip of PE2 as neighbor with neighbor AS
`(config-router)#neighbor 1.1.1.54 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#neighbor 52.56.1.56 remote-as 100`	Add loopback ip of ABR1 as neighbor with neighbor AS
`(config-router)#allocate-label all`	Allocate labels
`(config-router)#address-family ipv4 labeled-unicast`	Enter into labeled-unicast address family
`(config-router-af)#neighbor 1.1.1.54 activate`	Activate the neighbor inside labeled-unicast address family
`(config-router-af)#neighbor 52.56.1.56 activate`	Activate the neighbor inside labeled-unicast address family
`(config-router-af)# neighbor 1.1.1.54 route-reflector-client`	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast

© 2021 IP Infusion Inc. Proprietary

(config-router-af)# neighbor 1.1.1.54 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 52.56.1.56 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)#exit-address-family	Exit from address family labeled-unicast
(config-router)#exit	Exit from router BGP mode

ABR2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 5.5.5.56/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 50.1.1.56/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 52.56.1.56/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)#exit	Exit interface mode.
(config)#router ospf 30	Configure the routing process OSPF with process Id 1
(config-router)#network 5.5.5.56/32 area 0	Define the interface (5.5.5.56/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 50.1.1.0/24 area 0	Define the interface (50.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 5.5.5.56 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)#router bgp 200	Enter Router BGP mode
(config-router)#neighbor 52.56.1.52 remote-as 100	Add neighbor peer ip and neighbor AS
(config-router)#neighbor 7.7.7.55 remote-as 100	Add loopback ip of PE2 as neighbor with neighbor AS
(config-router)#neighbor 7.7.7.55 update-source lo	Update the source for that particular neighbor as loopback interface
(config-router)#allocate-label all	Allocate labels
(config-router)#address-family ipv4 labeled-unicast	Enter into labeled-unicast address family
(config-router-af)#neighbor 52.56.1.52 activate	Activate the neighbor inside labeled-unicast address family

(config-router-af)#neighbor 7.7.7.55 activate	Activate the neighbor inside labeled-unicast address family
(config-router-af)# neighbor 7.7.7.55 route-reflector-client	Enable Route reflector client for the neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 52.56.1.52 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)# neighbor 7.7.7.55 next-hop-self	Enable next hop self for the particular neighbor inside address family IPv4 labeled unicast
(config-router-af)#exit-address-family	Exit from address family vpnv4
(config-router)#exit	Exit from router BGP mode
(config)#end	Exit from config mode

P2

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 6.6.6.22/32	Configure the IP address of the interface loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 50.1.1.22/24	Configure the IP address of the interface eth1
(config-if)#label-switching	Enable label-switching on interface eth1
(config-if)# enable-ldp ipv4	Enable LDP process on eth1 interface
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode
(config-if)#ip address 60.1.1.22/24	Configure the IP address of the interface eth2
(config-if)#label-switching	Enable label-switching on interface eth2
(config-if)# enable-ldp ipv4	Enable LDP process on eth2 interface
(config-if)#exit	Exit interface mode
(config)#router ospf 30	Configure the routing process OSPF with process id 20
(config-router)#network 50.1.1.0/24 area 0	Define the interface (30.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 60.1.1.0/24 area 0	Define the interface (40.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#network 6.6.6.22/32 area 0	Define the interface (4.4.4.53/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
(config-router)#exit	Exit from router ospf mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 6.6.6.22 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip route 1.1.1.54/32 50.1.1.56	Specify the destination prefix and mask for the network and a gateway.
(config)#exit	Exit from Cofig mode

© 2021 IP Infusion Inc. Proprietary

PE2

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 7.7.7.55/32 secondary`	Configure the IP address of the interface loopback
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 60.1.1.55/24`	Configure the IP address of the interface eth1
`(config-if)#label-switching`	Enable label-switching on interface eth1
`(config-if)# enable-ldp ipv4`	Enable LDP process on eth1 interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 30`	Configure the routing process OSPF with process id 10
`(config-router)#network 7.7.7.55/32 area 0`	Define the interface (7.7.7.55/32) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#network 60.1.1.0/24 area 0`	Define the interface (60.1.1.0/24) on which OSPF runs, and associate the area ID (0) with the interface (area ID 0 specifies the backbone area).
`(config-router)#exit`	Exit from router ospf mode
`(config)#router bgp 200`	Enter Router BGP mode
`(config-router)#neighbor 1.1.1.54 remote-as 100`	Add loopback ip of PE2 as neighbor with neighbor AS
`(config-router)#neighbor 1.1.1.54 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#neighbor 1.1.1.54 ebgp-multihop`	Enable neighbor connection between two eBGP
`(config-router)#neighbor 5.5.5.56 remote-as 200`	Add loopback ip of ABR1 as neighbor with neighbor AS
`(config-router)#neighbor 5.5.5.56 update-source lo`	Update the source for that particular neighbor as loopback interface
`(config-router)#allocate-label all`	Allocate labels
`(config-router)#address-family ipv4 labeled-unicast`	Enter into labeled-unicast address family
`(config-router-af)#neighbor 5.5.5.56 activate`	Activate the neighbor inside vpnv4 address family
`(config-router-af)#exit-address-family`	Exit from address family IPv4 labeled unicast
`(config-router)#address-family  vpnv4 unicast`	Enter into vpnv4 unicast address family
`(config-router-af)#neighbor 1.1.1.54 allow-ebgp-vpn`	Allow eBGP neighbor to be a vpn peer.
`(config-router-af)#neighbor 1.1.1.54 activate`	Activate the neighbor inside labeled-unicast address family
`(config-router-af)#exit-address-family`	Exit from address family vpnv4
`(config-router)#address-family ipv4 unicast`	Enter into ipv4 unicast address family
`(config-router-af)#network 7.7.7.55/32`	Advertise the loopback of RTR1 in BGP
`(config-router-af)#exit-address-family`	Exit from address family vpnv4

(config-router)#exit	Exit from router BGP mode
(config)# router ldp	Configure Router LDP instance
(config-router)# transport-address ipv4 7.7.7.55 0	Configure Transport address for LDP with label space value 0
(config-router)#exit	Exit from router mode
(config)# ip vrf vrf1	Specify the name of the VRF (vrf1) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 100:300	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth2	Enter interface mode
(config-if)# ip vrf forwarding vrf1	Bind the interface (eth2) to the VRF vrf1
(config-if)# ip address 62.1.1.55/24	Configure the IP address of the interface eth2
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)# address-family ipv4 vrf vrf1	Enter address family ipv4 vrf mode
(config-router-af)# redistribute connected	Redistribute connected routes
(config-router-af)#end	Exit from router mode into privilege mode

Validation

PE1

```
#sh ip bgp labeled-unicast
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S - stale
   Network Next HopIn LabelOut Label
*> 1.1.1.54/32 0.0.0.0  24969          -
*>i 7.7.7.55/32 3.3.3.52    -        24322


#sh mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, B - BGP FTN, K - CLI FTN, t - tunnel
L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

10.1.1.23
10.1.1.23
3.3.3.52
10.1.1.23

#sh mpls ftn-table

Nexthop
```


© 2021 IP Infusion Inc. Proprietary

```
Primary FTN entry with FEC: 2.2.2.23/32, id: 1, row status: Active
Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none Tunnel id:
0,  Protected LSP id: 0, Description: N/A
Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1 Owner: LDP, Persistent:
No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 1, owner: LDP, out intf: eth1, out label: 3 Nexthop addr: 10.1.1.23
cross connect ix: 1, op code: Push

Primary FTN entry with FEC: 3.3.3.52/32, id: 3, row status: Active
Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none Tunnel id:
0,  Protected LSP id: 0, Description: N/A
Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2 Owner: LDP, Persistent:
No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 2, owner: LDP, out intf: eth1, out label: 24321 Nexthop addr:
10.1.1.23cross connect ix: 2, op code: Push

Primary FTN entry with FEC: 7.7.7.55/32, id: 4, row status: Active
Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none Tunnel id:
0,  Protected LSP id: 0, Description: N/A
Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3 Owner: BGP, Persistent:
No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 3, owner: BGP, out intf: eth1, out label: 24322 Nexthop addr:
3.3.3.52cross connect ix: 4, op code: Push and
Lookup

Primary FTN entry with FEC: 20.1.1.0/24, id: 2, row status: Active
Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none Tunnel id:
0,  Protected LSP id: 0, Description: N/A
Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1 Owner: LDP, Persistent:
No, Admin Status: Up, Oper Status: Up
Out-segment with ix: 1, owner: LDP, out intf: eth1, out label: 3 Nexthop addr: 10.1.1.23
cross connect ix: 1, op code: Push
```

ABR1

```
#sh ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.54/32      1.1.1.54        24323        24969
*>  7.7.7.55/32      52.56.1.56      24322        24325

#sh mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Tunnel-id   Pri   LSP-Type        Out-
Label    Out-Intf       Nexthop
   L>   1.1.1.54/32        2       0          Yes   LSP_DEFAULT     24322
eth2          20.1.1.23
   B    1.1.1.54/32        5       0          Yes   LSP_DEFAULT     24969
eth2          1.1.1.54
```

```
   L>    2.2.2.23/32        3       0          Yes   LSP_DEFAULT     3
eth2          20.1.1.23
   B>    7.7.7.55/32        1       0          Yes   LSP_DEFAULT     24325
eth1          52.56.1.56
   L>    10.1.1.0/24        4       0          Yes   LSP_DEFAULT     3
eth2          20.1.1.23

#sh mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.54/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth2, out label: 24322
    Nexthop addr: 20.1.1.23        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 1.1.1.54/32, id: 5, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 8, in intf: - in label: 0 out-segment ix: 8
      Owner: BGP, Persistent: No, Admin Status: Down, Oper Status: Down
       Out-segment with ix: 8, owner: BGP, out intf: eth2, out label: 24969
    Nexthop addr: 1.1.1.54        cross connect ix: 8, op code: Push and
Lookup


 Primary FTN entry with FEC: 2.2.2.23/32, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 20.1.1.23        cross connect ix: 3, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 1, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 7
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 7, owner: BGP, out intf: eth1, out label: 24325
    Nexthop addr: 52.56.1.56        cross connect ix: 7, op code: Push


 Primary FTN entry with FEC: 10.1.1.0/24, id: 4, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: eth2, out label: 3
    Nexthop addr: 20.1.1.23        cross connect ix: 3, op code: Push
```

ABR2

```
#sh ip bgp labeled-unicast
```


© 2021 IP Infusion Inc. Proprietary

```
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>  1.1.1.54/32       52.56.1.52      24322        24323
*>i 7.7.7.55/32       7.7.7.55        24325        24967

#sh mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                 FTN-ID    Tunnel-id   Pri   LSP-Type        Out-
Label    Out-Intf       Nexthop
   B>    1.1.1.54/32         1         0          Yes   LSP_DEFAULT     24323
eth2           52.56.1.52
   L>    6.6.6.22/32         2         0          Yes   LSP_DEFAULT     3
eth1           50.1.1.22
   L>    7.7.7.55/32         3         0          Yes   LSP_DEFAULT     24322
eth1           50.1.1.22
   B     7.7.7.55/32         5         0          Yes   LSP_DEFAULT     24967
eth1           7.7.7.55
   L>    60.1.1.0/24         4         0          Yes   LSP_DEFAULT     3
eth1           50.1.1.22

#sh mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.54/32, id: 1, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 8, in intf: - in label: 0 out-segment ix: 8
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 8, owner: BGP, out intf: eth2, out label: 24323
    Nexthop addr: 52.56.1.52        cross connect ix: 8, op code: Push


 Primary FTN entry with FEC: 6.6.6.22/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 50.1.1.22        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: eth1, out label: 24322
    Nexthop addr: 50.1.1.22        cross connect ix: 3, op code: Push


 Primary FTN entry with FEC: 7.7.7.55/32, id: 5, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 7
      Owner: BGP, Persistent: No, Admin Status: Down, Oper Status: Down
```

```
       Out-segment with ix: 7, owner: BGP, out intf: eth1, out label: 24967
    Nexthop addr: 7.7.7.55        cross connect ix: 7, op code: Push and
Lookup


 Primary FTN entry with FEC: 60.1.1.0/24, id: 4, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, out intf: eth1, out label: 3
    Nexthop addr: 50.1.1.22        cross connect ix: 2, op code: Push
```

PE2

```
#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
    Network          Next Hop        In Label     Out Label
*>i 1.1.1.54/32       5.5.5.56           -            24322
*>  7.7.7.55/32      0.0.0.0         24967          -

#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
      B - BGP FTN, K - CLI FTN, t - tunnel
      L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
      U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                 FTN-ID    Tunnel-id   Pri   LSP-Type        Out-
Label    Out-Intf       Nexthop
  B>    1.1.1.54/32         4       0          Yes   LSP_DEFAULT     24322
eth2          5.5.5.56
  L>    5.5.5.56/32         3       0          Yes   LSP_DEFAULT     24321
eth2          60.1.1.22
  L>    6.6.6.22/32         2       0          Yes   LSP_DEFAULT     3
eth2          60.1.1.22
  L>    50.1.1.0/24         1       0          Yes   LSP_DEFAULT     3
eth2          60.1.1.22

#sh mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.54/32, id: 4, row status: Active
  Owner: BGP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 36, in intf: - in label: 0 out-segment ix: 37
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 37, owner: BGP, out intf: eth2, out label: 24322
    Nexthop addr: 5.5.5.56        cross connect ix: 36, op code: Push and
Lookup


 Primary FTN entry with FEC: 5.5.5.56/32, id: 3, row status: Active
  Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, out intf: eth2, out label: 24321
    Nexthop addr: 60.1.1.22        cross connect ix: 7, op code: Push
```

 © 2021 IP Infusion Inc. Proprietary

```
Primary FTN entry with FEC: 6.6.6.22/32, id: 2, row status: Active
 Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0,   Protected LSP id: 0, Description: N/A
    Cross connect ix: 9, in intf: - in label: 0 out-segment ix: 8
     Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 8, owner: LDP, out intf: eth2, out label: 3
   Nexthop addr: 60.1.1.22        cross connect ix: 9, op code: Push


Primary FTN entry with FEC: 50.1.1.0/24, id: 1, row status: Active
 Owner: LDP, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0,   Protected LSP id: 0, Description: N/A
    Cross connect ix: 9, in intf: - in label: 0 out-segment ix: 8
     Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 8, owner: LDP, out intf: eth2, out label: 3
   Nexthop addr: 60.1.1.22        cross connect ix: 9, op code: Push
```

BGP Peer Groups for Address-Family IPv4 Labeled Unicast

Topology

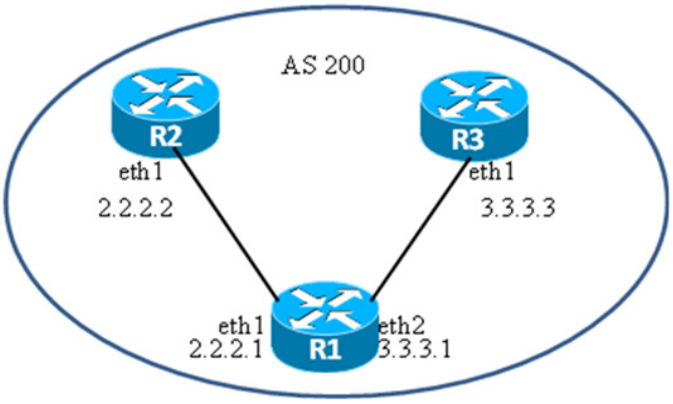


Figure 10-181: BGP Peer-Groups with IPv4 Labeled-Unicast Members

R1

`(config)# interface lo`	Enter interface mode for Loopback
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure ip address for Loopback interface
`(config-if)#ip address 11.11.11.11/32 secondary`	Configure ip address for Loopback interface
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Define the routing process. The number 200 specifies the AS number of R1.
`(config-router)#neighbor ABC peer-group`	Create a peer group named ABC.
`(config-router)#neighbor ABC remote-as 200`	Assign options to the peer group named ABC.
`(config-router)#neighbor 2.2.2.2 peer-group ABC`	Define neighbor 2.2.2.2 (R2) as a peer group member.

`(config-router)#neighbor 3.3.3.3 peer-group ABC`	Define neighbor 3.3.3.3 (R3) as a peer group member.
`(config-router)#address-family ipv4 labeled-unicast`	Enter address-family ipv4 labeled-unicast mode
`(config-router-af)#neighbor ABC activate`	Activate the peer-group ABC for address-family ipv4 labeled-unicast
`(config-router-af)#neighbor ABC route-reflector-client`	Configure the peer-group ABC to be route-reflector-client
`(config-router-af)# exit-address-family`	Exit address-family ipv4 labeled-unicast mode
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#network 1.1.1.1/32`	Advertise the network 1.1.1.1/32
`(config-router-af)#network 11.11.11.11/32`	Advertise the network 11.11.11.11/32
`(config-router-af)# exit-address-family`	Exit address-family ipv4 unicast mode
`(config-router)#allocate-label all`	Allocate labels for all IPv4 prefixes advertised
`(config-router)#exit`	Exit router bgp mode

© 2021 IP Infusion Inc. Proprietary

R2

#configure terminal	Enter configure mode.
(config)#router bgp 200	Define the routing process. The number 200 specifies the AS number of R2.
(config-router)#neighbor 2.2.2.1 remote-as 200	Create a TCP connection with neighbor 2.2.2.1 of AS 200.
config-router)#allocate-label all	Allocate labels for all IPv4 prefixes advertised
(config-router)#address-family ipv4 labeled-unicast	Enter address-family ipv4 labeled-unicast mode
(config-router-af)#neighbor 2.2.2.1 activate	Activate the neighbor R1 for address-family ipv4 labeled-unicast
(config-router-af)# exit-address-family	Exit address-family ipv4 labeled-unicast mode
(config-router)# exit	Exit router bgp mode

R3

#configure terminal	Enter configure mode.
(config)#router bgp 200	Define the routing process. The number 200 specifies the AS number of R3.
(config-router)#neighbor 3.3.3.1 remote-as 200	Create a TCP connection with neighbor 3.3.3.1 of AS 200.
config-router)#allocate-label all	Allocate labels for all IPv4 prefixes advertised
(config-router)#address-family ipv4 labeled-unicast	Enter address-family ipv4 labeled-unicast mode
(config-router-af)#neighbor 3.3.3.1 activate	Activate the neighbor R1 for address-family ipv4 labeled-unicast
(config-router-af)# exit-address-family	Exit address-family ipv4 labeled-unicast mode
(config-router)# exit	Exit router bgp mode

Validation

R1

```
R1#show ip bgp labeled-unicast summary
BGP router identifier 10.12.65.126, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
2.2.2.2                  4   200   18         22       1       0       0
00:00:57               0
3.3.3.3                  4   200   18         20       1       0       0
00:00:01               0

Total number of neighbors 2

Total number of Established sessions 2
R1#
```

```
R1#show bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.123
  BGP state = Established, up for 00:01:05
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 16 messages, 2 notifications, 0 in queue
  Sent 20 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 11, neighbor version 11
  Index 0, Offset 0, Mask 0x1
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 Connections established 5; dropped 4
Local host: 2.2.2.1, Local port: 51667
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:01:10, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 3.3.3.3, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.121
  BGP state = Established, up for 00:00:09
  Last read 00:00:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 16 messages, 2 notifications, 0 in queue
  Sent 20 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 11, neighbor version 11
```

 © 2021 IP Infusion Inc. Proprietary

```
  Index 1, Offset 0, Mask 0x2
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
  BGP table version 1, neighbor version 1
  Index 3, Offset 0, Mask 0x8
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 Connections established 5; dropped 4
Local host: 3.3.3.1, Local port: 41732
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 3.3.3.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:00:19, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

R1#
```

R2

```
R2#show ip bgp
BGP table version is 3, local router ID is 10.12.65.123
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>il 1.1.1.1/32       2.2.2.1               0         100           0        i
* i                   2.2.2.1               0         100           0        i
*>il 11.11.11.11/32   2.2.2.1               0         100           0        i
* i                   2.2.2.1               0         100           0        i

Total number of prefixes 2
R2#




R2#show ip bgp 1.1.1.1/32
BGP routing table entry for 1.1.1.1/32
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Local
    2.2.2.1 from 2.2.2.1 (10.12.65.126)
      Origin IGP, metric 0, localpref 100      valid, internal, best, source
safi: 4
      Last update: Tue Aug 25 10:01:05 2020
```

```
  Local
    2.2.2.1 from 2.2.2.1 (10.12.65.126)
      Origin IGP, metric 0, localpref 100      valid, internal, source safi: 1
      Last update: Tue Aug 25 10:01:05 2020

R2#
R2#show ip bgp 11.11.11.11/32
BGP routing table entry for 11.11.11.11/32
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Local
    2.2.2.1 from 2.2.2.1 (10.12.65.126)
      Origin IGP, metric 0, localpref 100      valid, internal, best, source
safi: 4
      Last update: Tue Aug 25 10:01:05 2020

  Local
    2.2.2.1 from 2.2.2.1 (10.12.65.126)
      Origin IGP, metric 0, localpref 100      valid, internal, source safi: 1
      Last update: Tue Aug 25 10:01:05 2020

R2#


R2#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.1/32       2.2.2.1           -            24320
*>i 11.11.11.11/32   2.2.2.1           -            24321
R2#
```

R3

```
R3#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.1/32       3.3.3.1           -            24320
*>i 11.11.11.11/32   3.3.3.1           -            24321
R3#
```

Peer group members inherit the properties of Outbound Policies configured for Peer-group under Address-family ipv4 Labeled-Unicast

R1

`#configure terminal`	Enter configure mode.
`(config)# ip access-list permit-1`	Configure access-list to permit 1.1.1.1/32
`(config-ip-acl)# permit any 1.1.1.1/32 any`	Configure a permit statement in the acl to permit 1.1.1.1/32

© 2021 IP Infusion Inc. Proprietary

(config-ip-acl)#exit	Exit ip access-list mode
(config)# route-map permit-only-1	Configure route-map
(config-route-map)# match ip address permit-1	Configure a match statement in the route-map to match the access-list permit-1
(config-route-map)#exit	Exit route-map mode
(config)#router bgp 200	Define the routing process. The number 200 specifies the AS number of R1.
(config-router)#no allocate-label all	Unconfiguring allocate label all
config-router)# allocate-label route-map permit-only-1	Allocate labels to the route map
(config-router)#address-family ipv4 labeled-unicast	Enter address-family ipv4 labeled-unicast mode
(config-router-af)# neighbor ABC route-map permit-only-1 out	Configure the peer-group ABC with route-map in the outbound direction
(config-router-af)#exit	Exit address-family mode
(config-router)#exit	Exit router bgp mode
(config# exit	Exit configure terminal mode
#clear ip bgp peer-group ABC ipv4 labeled-unicast soft out	Do outbound soft reset for the peer-group ABC for the policy to take affect for the labelled-unicast peer-group members

Validation

R1

```
R1#show bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.123
  BGP state = Established, up for 00:14:24
  Last read 00:00:22, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 46 messages, 2 notifications, 0 in queue
  Sent 53 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 11, neighbor version 11
  Index 0, Offset 0, Mask 0x1
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
```

```
  Outbound path policy configured
  Route map for outgoing advertisements is *permit-only-1
  0 accepted prefixes
  1 announced prefixes

 Connections established 5; dropped 4
Local host: 2.2.2.1, Local port: 51667
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:14:29, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 3.3.3.3, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.121
  BGP state = Established, up for 00:13:28
  Last read 00:00:21, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 47 messages, 2 notifications, 0 in queue
  Sent 53 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 11, neighbor version 11
  Index 1, Offset 0, Mask 0x2
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
  BGP table version 1, neighbor version 1
  Index 3, Offset 0, Mask 0x8
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  Outbound path policy configured
  Route map for outgoing advertisements is *permit-only-1
  0 accepted prefixes
  1 announced prefixes

 Connections established 5; dropped 4
Local host: 3.3.3.1, Local port: 41732
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 3.3.3.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:13:38, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)
```

 © 2021 IP Infusion Inc. Proprietary

```
R1#
```

R2

```
R2#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.1/32       2.2.2.1            -            24320
R2#
```

R3

```
R3#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop        In Label     Out Label
*>i 1.1.1.1/32       3.3.3.1            -            24320
R3#
```

Peer-group-members inherit the properties of Inbound Policies configured for Peer-group under Address-family ipv4 Labeled-Unicast

Follow the configuration of R1,R2,R3 in the previous section with the following configuration

R2

`#configure terminal`	Enter configure mode.
`(config)# interface lo`	Enter interface mode for Loopback interface
`(config-if)#ip address 100.1.1.1/24 secondary`	Configure IP address for Loopback interaface
`(config-if)#interface eth3`	Enter interface mode for interface eth3
`(config-if)#ip address 22.1.1.1/24`	Configure IP address for interface eth3
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 200`	Enter router bgp mode
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#network 22.1.1.0/24`	Advertise the network of eth3 in BGP
`(config-router-af)#network 100.1.1.0/24`	Advertise the network of Loopback in BGP
`(config-router-af)#exit-address-family`	Exit address-family mode
`(config-router)#allocate-label all`	Allocate labels for all IPv4 prefixes advertised
`(config-router)#exit`	Exit router bgp mode

R3

`#configure terminal`	Enter configure mode.
`(config)# interface lo`	Enter interface mode for Loopback interface
`(config-if)#ip address 100.1.1.2/24 secondary`	Configure IP address for Loopback interaface

(config-if)#interface eth3	Enter interface mode for interface eth3
(config-if)#ip address 22.1.1.2/24	Configure IP address for interface eth3
(config-if)#exit	Exit interface mode
(config)#router bgp 200	Enter router bgp mode
(config-router)#address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#network 22.1.1.0/24	Advertise the network of eth3 in BGP
(config-router-af)#network 100.1.1.0/24	Advertise the network of Loopback in BGP
(config-router-af)#exit-address-family	Exit address-family mode
(config-router)#allocate-label all	Allocate labels for all IPv4 prefixes advertised
(config-router)#exit	Exit router bgp mode

R1

#configure terminal	Enter configure mode.
(config)#ip access-list permit-22	Configure access-list to permit 22.1.1.0/24
(config-ip-acl)# permit any 22.1.1.0/24 any	Configure a permit statement to permit 22.1.1.0/24
(config-ip-acl)#exit	Exit ip access-list mode
(config)#route-map permit-only-22	Configure route-map
(config-route-map)#match ip address permit-22	Configure match statement in route-map to match the access-list permit-22
(config-route-map)#exit	Exit route-map mode
(config)#router bgp 200	Enter BGP router mode
(config-router)#address-family ipv4 labeled-unicast	Enter the address-family ipv4 labeled-unicast mode
(config-router-af)#neighbor ABC route-map permit-only-22 in	Configure the peer-group ABC with route-map in the inbound direction under address-family ipv4 labeled-unicast
(config-router-af)# neighbor ABC activate	Activate PEER-GROUP in the address family
(config-router-af)#exit-address-family	Exit address-family ipv4 labeled-unicast mode
(config-router)#exit	Exit router bgp mode
(config)# exit	Exit configure terminal mode
#clear ip bgp peer-group ABC ipv4 labeled-unicast soft in	Do inbound soft reset for the peer-group ABC for the policy to take affect for the labelled-unicast peer-group members

Validation

R1

```
R1#show ip bgp labeled-unicast

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S - stale
     Network          Next Hop         In Label     Out Label
*>  1.1.1.1/32       0.0.0.0           24320          -
*>  11.11.11.11/32   0.0.0.0           24321          -
*>i 22.1.1.0/24      3.3.3.3           24322         24320
* i                  2.2.2.2            -             24320
```


© 2021 IP Infusion Inc. Proprietary

```
*>i 100.1.1.0/24     3.3.3.3           24323          -
R1#


R1#show bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.123
  BGP state = Established, up for 00:45:38
  Last read 00:00:03, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 123 messages, 2 notifications, 0 in queue
  Sent 126 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 14, neighbor version 14
  Index 0, Offset 0, Mask 0x1
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
  BGP table version 3, neighbor version 3
  Index 2, Offset 0, Mask 0x4
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is *permit-only-22
  Route map for outgoing advertisements is *permit-only-1
  1 accepted prefixes
  1 announced prefixes

 Connections established 5; dropped 4
Local host: 2.2.2.1, Local port: 51667
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:45:43, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 3.3.3.3, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, local router ID 10.12.65.126, remote router ID 10.12.65.121
  BGP state = Established, up for 00:44:42
  Last read 00:00:22, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
```

```
    Address family IPv4 Labeled-Unicast: advertised and received
  Received 124 messages, 2 notifications, 0 in queue
  Sent 127 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 14, neighbor version 14
  Index 1, Offset 0, Mask 0x2
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  2 announced prefixes

 For address family: IPv4 Labeled-Unicast
  BGP table version 3, neighbor version 3
  Index 3, Offset 0, Mask 0x8
  ABC peer-group member
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is *permit-only-22
  Route map for outgoing advertisements is *permit-only-1
  1 accepted prefixes
  1 announced prefixes

 Connections established 5; dropped 4
Local host: 3.3.3.1, Local port: 41732
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 3.3.3.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:44:52, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

R1#
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 11 BGP Graceful Restart Configuration

During a BGP restart, all BGP peers detect that a session had gone down and come back up. OcNOS invalidates the associated portion of the IP forwarding cache, does a BGP route re-computation, and generates BGP routing updates. The forwarding tables become corrupted and unstable.

Graceful restart helps minimize these negative effects on routing caused by a BGP restart by allowing the restarting BGP router to temporarily retain routing information and continue forwarding packets while BGP restarts. In this way, even while a router rebuilds routing and forwarding tables, the router continues to operate across the TCP connection.

Graceful restart allows a restarting router, and its neighbors, to continue forwarding packets, without disrupting network performance. Because neighboring routers assist in the restart, the restarting router can quickly resume full operation.

The graceful restart capability extends to the case when a configuration change forces a peer reset.

Graceful reset is a refinement of graceful restart to help ensure smooth restarts when a configuration change forces BGP peer reset.

Topology

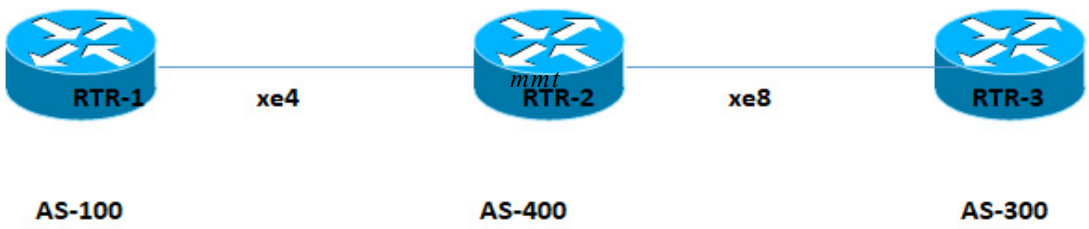


Figure 11: Device topology for BGP in VR/VRF

RTR1

`#configure terminal`	Enter Configuration mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure ip address on loopback.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe4`	Enter interface mode for eth2.
`(config-if)#ip address 10.10.10.1/24`	Configure ip address on eth2.
`(config-if)#exit`	Exit interface mode for eth2.
`(config)# router bgp 100`	Enter router bgp mode.
`(config-router)# bgp router-id 1.1.1.11.1.1.1`	Configure bgp router-id same as loopback ip address.
`(config-router)# bgp graceful-restart`	Configure Graceful Restart for BGP.

`(config-router)# neighbor 10.10.10.2 remote-as 400`	Configure Neighbor for AS-400.
`(config-router)# address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)# neighbor 10.10.10.2 activate`	Activate neighborship
`(config-router-af)#redistribute connected`	Redistributing connected Routes inside BGP.
`(config-router-af)# neighbor 10.10.10.2 capability graceful-restart`	Configure GR capability inside router bgp.
`(config-router-af)#end`	Exit router BGP mode.

RTR2

`#configure terminal`	Enter Configuration mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)# ip address 2.2.2.2/32 secondary`	Configure ip address on loopback.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe4`	Enter interface mode for eth1.
`(config-if)#ip address 10.10.10.2/24`	Configure ip address on eth1.
`(config-if)#exit`	Exit interface mode for eth1.
`(config)#interface xe8`	Enter interface mode for eth2.
`(config-if)#ip address 20.20.20.1/24`	Configure ip address on eth2.
`(config-if)#exit`	Exit interface mode for eth2.
`(config)#router bgp 400`	Enter router BGP mode.
`(config-router)# bgp router-id 2.2.2.22.2.2.2`	Configure bgp router-id same as loopback ip address.
`(config-router)# bgp graceful-restart`	Configure Graceful Restart for BGP.
`(config-router)# neighbor 10.10.10.1 remote-as 100`	Configure Neighbor for AS-100.
`(config-router)# neighbor 20.20.20.2 remote-as 300`	Configure Neighbor for AS-300.
`(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`(config-router-af)#redistribute connected`	Redistributing connected Routes inside BGP.
`(config-router-af)# neighbor 10.10.10.1 activate`	Activate neighbor
`(config-router-af)# neighbor 20.20.20.2 activate`	Activate neighbor
`(config-router-af)# neighbor 10.10.10.1 capability graceful-restart`	Configure GR capability inside router bgp.
`(config-router-af)#end`	Exit router ospf mode.

RTR3

`#configure terminal`	Enter Configuration mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 3.3.3.3/32 secondary`	Configure ip address on loopback.

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit interface mode.
(config)#interface xe8	Enter interface mode for eth2.
(config-if)#ip address 20.20.20.2/24	Configure ip address on eth2.
(config-if)#exit	Exit interface mode for eth2.
(config)# router bgp 300	Enter router BGP mode.
(config-router)# bgp router-id 3.3.3.33.3.3.3	Configure bgp router-id same as loopback ip address.
(config-router)# bgp graceful-restart	Configure Graceful Restart for BGP.
(config-router)# neighbor 20.20.20.1 remote-as 400	Configure Neighbor for AS-400.
(config-router)# address-family ipv4 unicast	Enter address-family ipv4 unicast mode
(config-router-af)#redistribute connected	Redistributing connected Routes inside BGP.
(config-router-af)# neighbor 20.20.20.1 activate	Activate the neighbor.
(config-router-af)# neighbor 20.20.20.1 capability graceful-restart	Configure GR capability inside router bgp.
(config-router-af)#end	Exit router BGP mode.

Validation

RTR1

```
RTR1#show  bgp neighbors
BGP neighbor is 10.10.10.2, remote AS 400, local AS 100, external link
  BGP version 4, local router ID 1.1.1.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:03:31
  Last read 00:00:15, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 13 messages, 1 notifications, 0 in queue
  Sent 13 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  AF-dependant capabilities:
    Graceful restart: advertised, received
     Forwarding states are being preserved
  Community attribute sent to this neighbor (both)
  3 accepted prefixes
  2 announced prefixes

 Connections established 2; dropped 1
 Graceful-restart Status:
  Remote restart-time is 90 sec

Local host: 10.10.10.1, Local port: 179
Foreign host: 10.10.10.2, Foreign port: 60024
Nexthop: 10.10.10.1
```

```
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:03:36, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

#show ip route databaseCodes: K - kernel, C - connected, S - static, R - RIP,
B - BGP O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked
> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
C*>1.1.1.11.1.1.1/32 is directly connected, lo, 00:10:23
B*>2.2.2.22.2.2.2/32 [20/0] via 10.10.10.2, xe4, 00:03:56
B*>3.3.3.33.3.3.3/32 [20/0] via 10.10.10.2, xe4, 00:00:56
C*>10.10.10.0/24 is directly connected, xe4, 00:09:37
B*>20.20.20.0/24 [20/0] via 10.10.10.2, xe4, 00:03:56
C*>127.0.0.0/8 is directly connected, lo, 00:28:58

Gateway of last resort is not set
```

RTR2

```
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA -
OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked
> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
B*>1.1.1.11.1.1.1/32 [20/0] via 10.10.10.1, xe4, 00:03:52
C*>2.2.2.22.2.2.2/32 is directly connected, lo, 00:07:36
B*>3.3.3.33.3.3.3/32 [20/0] via 20.20.20.2, xe8, 00:00:57

C*>10.10.10.0/24 is directly connected, xe4, 00:07:12 C*>20.20.20.0/24 is
directly connected, xe8, 00:06:31
C*>127.0.0.0/8 is directly connected, lo, 00:25:32

Gateway of last resort is not set

RTR2#show bgp neighbors
BGP neighbor is 10.10.10.1, remote AS 100, local AS 400, external link
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 00:04:28
  Last read 00:00:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 43 messages, 1 notifications, 0 in queue
  Sent 41 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
```


© 2021 IP Infusion Inc. Proprietary

```
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  AF-dependant capabilities:
    Graceful restart: advertised, received
     Forwarding states are being preserved
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  3 announced prefixes

 Connections established 4; dropped 3
 Graceful-restart Status:
  Remote restart-time is 90 sec

Local host: 10.10.10.2, Local port: 60050
Foreign host: 10.10.10.1, Foreign port: 179
Nexthop: 10.10.10.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:04:33, due to Administratively Reset (Cease Notification sent)
Notification Error Message: (Cease/Administratively Reset.)

BGP neighbor is 20.20.20.2, remote AS 300, local AS 400, external link
  BGP version 4, local router ID 2.2.2.2, remote router ID 3.3.3.3
  BGP state = Established, up for 00:04:22
  Last read 00:00:03, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 31 messages, 2 notifications, 0 in queue
  Sent 40 messages, 3 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 2, Offset 0, Mask 0x4
  AF-dependant capabilities:
    Graceful restart: advertised, received
     Forwarding states are being preserved
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  4 announced prefixes

 Connections established 4; dropped 3
 Graceful-restart Status:
  Remote restart-time is 90 sec

Local host: 20.20.20.1, Local port: 179
Foreign host: 20.20.20.2, Foreign port: 56342
Nexthop: 20.20.20.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:04:22, due to Administratively Reset (Cease Notification sent)
Notification Error Message: (Cease/Administratively Reset.)
```

```
RTR2#
```

RTR3

```
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA -
OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
B*> 1.1.1.11.1.1.1/32 [20/0] via 20.20.20.1, xe8, 00:01:15
B*> 2.2.2.22.2.2.2/32 [20/0] via 20.20.20.1, xe8, 00:01:15
C*> 3.3.3.3/32 is directly connected, lo
B*> 10.10.10.0/24 [20/0] via 20.20.20.1, xe8, 00:01:15
C*> 20.20.20.0/24 is directly connected, xe8
C*> 127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set
RTR3#show bgp neighbors
BGP neighbor is 20.20.20.1, remote AS 400, local AS 300, external link
  BGP version 4, local router ID 3.3.3.3, remote router ID 2.2.2.2
  BGP state = Established, up for 00:06:47
  Last read 00:00:13, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 45 messages, 1 notifications, 0 in queue
  Sent 38 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  AF-dependant capabilities:
    Graceful restart: advertised, received
     Forwarding states are being preserved
  Community attribute sent to this neighbor (both)
  4 accepted prefixes
  0 announced prefixes

 Connections established 4; dropped 3
 Graceful-restart Status:
  Remote restart-time is 90 sec

Local host: 20.20.20.2, Local port: 56342
Foreign host: 20.20.20.1, Foreign port: 179
Nexthop: 20.20.20.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:06:52, due to Administratively Reset (Cease Notification sent)
Notification Error Message: (Cease/Administratively Reset.)
```

 © 2021 IP Infusion Inc. Proprietary

```
RTR3#
```

Validation After BGP Graceful Restart

RTR2

```
#write
Building configuration... [OK]

#restart bgp graceful
2003 Sep 19 07:20:00.947 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]:
Neighbour
[10.10.10.1] Session down as GR configured/unconfigured
2003 Sep 19 07:20:00.947 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]:
Neighbour
[10.10.10.1] Session down due to config deletion
2003 Sep 19 07:20:00.947 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]:
Neighbour
[20.20.20.2] Session down as GR configured/unconfigured
2003 Sep 19 07:20:00.947 : NOS : BGP : CRITI : [BGP_OPR_NEIGH_STATE_DOWN_2]:
Neighbour
[20.20.20.2] Session down due to config deletion

#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA -
OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN, v - vrf leaked

> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
B*>p 1.1.1.1/32 [20/0] via 10.10.10.1, xe4, 00:19:31
C*>2.2.2.2/32 is directly connected, lo, 00:50:45
B*>p 3.3.3.3/32 [20/0] via 20.20.20.2, xe8, 00:19:32
C*>10.10.10.0/24 is directly connected, xe4, 00:50:21 C*>20.20.20.0/24 is
directly connected, xe8, 00:49:40
C*>127.0.0.0/8 is directly connected, lo, 01:08:41 Gateway of last resort is
not set
#show rib forwarding-timer
Protocol-Name GR-State Time Remaining (sec)Disconnected-time BGPACTIVE572001/
06/07 19:50:38
```

RTR1

```
#show ip bgp
BGP table version is 8, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - Labeled, S Stale
Origin codes: i - IGP, e - EGP,? - incomplete

NetworkNext HopMetricLocPrfWeightPath
*>1.1.1.1/32
0.0.0.0010032768?
S>2.2.2.2/32
10.10.10.201000400?
```

```
S>3.3.3.3/32
10.10.10.201000400300?
*>10.10.10.0/240.0.0.0010032768?
S10.10.10.201000400?
S>20.20.20.0/2410.10.10.201000400?

Total number of prefixes 5
```

RTR3

```
#sh ip bgp
BGP table version is 14, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

NetworkNext HopMetricLocPrfWeightPath
S>1.1.1.1/32
20.20.20.101000400 100?
S>2.2.2.2/32
20.20.20.101000400 ?
*>3.3.3.3/32
0.0.0.0010032768?
S>10.10.10.0/2420.20.20.101000400 ?
*>20.20.20.0/240.0.0.0010032768?
S20.20.20.101000400 ?

Total number of prefixes 5
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 12 Static Route Discard Configuration

This chapter show how to configure the static route discard feature.

Overview

If you identify some routers/attackers distributing invalid/bogus routes just to use the resources of the device or to make the device unstable, you can configure route-map rules, discard all routes, and black hole traffic corresponding to those routes.

To so this, you add “discard” route entries for a prefix in a route map with the “set interface null0” command. You then apply that route map to a BGP neighbor.

IPv4 Route Discard

Figure 12-1 shows the configuration required to enable static route discard for IPv4.

Topology

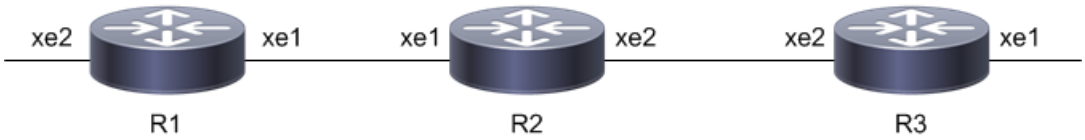


Figure 12-1: Static route discard topology

Configuration

R1

`R1#configure terminal`	Enter configure mode
`R1(config)#interface xe1`	Enter interface mode for xe1
`R1(config-if)#ip address 2.2.2.2/24`	Assign an IP address to the interface
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#interface xe2`	Enter interface mode for xe1
`R1(config-if)#ip address 1.1.1.2/24`	Assign an IP address to the interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#router bgp 2`	Enter BGP router mode
`R1(config-router)#neighbor 2.2.2.3 remote-as 3`	Create static BGP neighbor 2.2.2.3 with remote autonomous system value 3
`R1(config-router)#address-family ipv4`	Enter address-family mode
`R1(config-router-af)#neighbor 2.2.2.3 activate`	Activate neighbor 2.2.2.3
`R1(config-router-af)#redistribute connected`	Advertise the connected network into BGP
`R1(config-router-af)#end`	Exit BGP router mode

R2

`R2#configure terminal`	Enter configure mode
`R2(config)#ip prefix-list p1`	Configure IP prefix list p1
`R2(config-ip-prefix-list)#permit any`	Configure permit any
`R2(config)#route-map r1`	Enter route-map mode
`R2(config-route-map)#match ip address prefix-list p1`	Configure match ip prefix list p1
`R2(config-route-map)#set interface null0`	Set the interface to null0
`R2(config-route-map)#exit`	Exit route-map mode.
`R2(config)#interface xe1`	Enter interface mode for xe1
`R2(config-if)#ip address 2.2.2.3/24`	Assign an IP address to the interface
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe2`	Enter interface mode for xe2
`R2(config-if)#ip address 3.3.3.2/24`	Assign an IP address to the interface
`R2(config-if)#exit`	Exit interface mode
`R2(config)#router bgp 3`	Enter into BGP router mode
`R2(config-router)#neighbor 2.2.2.2 remote-as 2`	Create static BGP neighbor 2.2.2.2 with remote autonomous system value 2
`R2(config-router)#neighbor 3.3.3.3 remote-as 4`	Create static BGP neighbor 3.3.3.3 with remote autonomous system value 4
`R2(config-router)#address-family ipv4`	Enter address-family mode
`R2(config-router-af)#neighbor 2.2.2.2 activate`	Activate neighbor 2.2.2.2
`R2(config-router-af)#neighbor 3.3.3.3 activate`	Activate neighbor 3.3.3.3
`R2(config-router-af)#redistribute connected`	Advertise the connected network into BGP
`R2(config-router-af)#neighbor 2.2.2.2 route-map r1 in`	Attach the route-map with route discard configured for the neighbor 2.2.2.2 in IN direction
`R2(config-router-af)#end`	Exit BGP router mode

R3

`R3#configure terminal`	Enter configure mode.
`R3(config)#interface xe2`	Enter interface mode for xe2
`R3(config-if)#ip address 3.3.3.3/24`	Assign an IP address to the interface
`R3(config-if)#exit`	Exit interface mode
`R3(config)#interface xe1`	Enter interface mode for xe1
`R3(config-if)#ip address 4.4.4.2/24`	Assign an IP address to the interface
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#router bgp 4`	Enter into BGP router mode
`R3(config-router)#neighbor 3.3.3.2 remote-as 3`	Create static BGP neighbor 3.3.3.2 with remote autonomous system value 3
`R2(config-router)#address-family ipv4`	Enter address-family mode

© 2021 IP Infusion Inc. Proprietary

`R2(config-router-af)#neighbor 3.3.3.2 activate`	Activate neighbor 3.3.3.2
`R3(config-router-af)#redistribute connected`	Advertise the connected network into BGP
`R3(config-router-af)#end`	Exit BGP router.

Validation

```
R2#show running-config bgp
!
router bgp 3
 neighbor 2.2.2.2 remote-as 2
 neighbor 3.3.3.3 remote-as 4
 !
 address-family ipv4 unicast
 redistribute connected
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 route-map r1 in
 neighbor 3.3.3.3 activate
 exit-address-family
!

R2#show ip bgp
BGP table version is 3, local router ID is 2.2.2.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
           l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
       Network          Next Hop          Metric  LocPrf     Weight      Path
*>   1.1.1.0/24         2.2.2.2              0    100          0           2 ?
*>   2.2.2.0/24         0.0.0.0              0    100        32768           ?
*                       2.2.2.2              0    100          0           2 ?
*>   3.3.3.0/24         0.0.0.0              0    100        32768            ?
*                       3.3.3.3              0    100          0           4 ?
*>   4.4.4.0/24         3.3.3.3              0    100          0           4 ?
Total number of prefixes 4


R2#show running-config prefix-list
!
ip prefix-list p1
 seq 5 permit any
!

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default
```

```
IP Route Table for VRF "default"
B     1.1.1.0/24 [20/0] is a summary, Null, 00:00:01
C     2.2.2.0/24 is directly connected, xe1, 00:09:57
C     3.3.3.0/24 is directly connected, xe2, 00:09:50
B     4.4.4.0/24 [20/0] via 3.3.3.3, xe2, 00:00:03
C     127.0.0.0/8 is directly connected, lo, 01:18:30

Gateway of last resort is not set

R2#show hsl nh-table
IPv4 FIB 0
0.0.0.0, Null, 00:00:00:00:00:00, Valid  ,
                      1.1.1.0/24, Installed FORWARD
2.2.2.2, xe1, 00:18:23:26:16:45, Valid  , lport:0x8000026, Egress object id:1
00004, refcnt 0, rulecnt 0
3.3.3.3, xe2, 00:18:23:cb:fb:b7, Valid  , lport:0x800002a, Egress object id:1
00003, refcnt 1, rulecnt 0,
                      4.4.4.0/24, Installed FORWARD

IPv4 FIB 1 10.12.29.1, eth0, 00:00:00:00:00:00, Invalid,
                                                , Not Installed TO_CPU

IPv6 FIB 0

IPv6 FIB 1
```

IPv6 Route Discard

Figure 12-1 shows the configuration required to enable static route discard for IPv6.

Configuration

R1

`R1#configure terminal`	Enter configure mode.
`R1(config)#interface lo`	Enter interface mode for loopback
`R1(config-if)#ip address 1.1.1.2/24 secondary`	Assign an IPv4 address to the interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#interface xe1`	Enter interface mode for xe1
`R1(config-if)#ipv6 address 2001::2/64`	Assign an IPv6 address to the interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#interface xe2`	Enter interface mode for xe2
`R1(config-if)#ipv6 address 1001::2/64`	Assign an IPv6 address to the interface
`R1(config-if)#exit`	Exit interface mode

© 2021 IP Infusion Inc. Proprietary

`R1(config)#router bgp 2`	Enter BGP router mode
`R1(config-router)#bgp router-id 1.1.1.1`	Specify router ID
`R1(config-router)#neighbor 2001::3 remote-as 3`	Create static BGP neighbor 2001::3 with remote autonomous system value 3
`R1(config-router)#address-family ipv6 unicast`	Enter address family IPv6 unicast mode
`R1(config-router-af)#neighbor 2001::3 activate`	Activate neighbor in IPv6 address family
`R1(config-router-af)#redistribute connected`	Advertise the connected network into BGP
`R1(config-router)#end`	Exit BGP router mode

R2

`R2#configure terminal`	Enter configure mode
`R2(config)#interface lo`	Enter interface mode for loopback
`R2(config-if)#ip address 2.2.2.2/24 secondary`	Assign an IPV4 address
`R2(config-if)#exit`	Exit interface mode
`R2(config)#ipv6 prefix-list p1 permit any`	Configure IPv6 prefix list.
`R2(config)#route-map r1`	Enter route-map mode.
`R2(config-route-map)#match ipv6 address prefix-list p1`	Configure match IPv6 prefix list p1
`R2(config-route-map)#set interface null0`	Set the interface to null0
`R2(config-route-map)#exit`	Exit route-map mode
`R2(config)#interface xe1`	Enter interface mode for xe1
`R2(config-if)#ipv6 address 2001::3/64`	Assign ipv6 address to the interface
`R2(config-if)#exit`	Exit interface mode
`R2(config)#interface xe2`	Enter interface mode for xe2
`R2(config-if)#ipv6 address 3001::2/64`	Assign an IPv6 address to the interface
`R2(config-if)#exit`	Exit interface mode
`R2(config)#router bgp 3`	Enter BGP router mode
`R2(config-router)#bgp router-id 2.2.2.2`	Specify router ID
`R2(config-router)#neighbor 2001::2 remote-as 2`	Create static BGP neighbor 2001::2 with remote autonomous system value 2
`R2(config-router)#neighbor 3001::3 remote-as 4`	Create static BGP neighbor 3001::3 with remote autonomous system value 4
`R2(config-router)#address-family ipv6 unicast`	Enter address family IPv6 unicast mode
`R2(config-router-af)#redistribute connected`	Advertise the connected network into BGP
`R2(config-router-af)#neighbor 2001::2 activate`	Activate the neighbor in IPv6 address family
`R2(config-router-af)#neighbor 3001::3 activate`	Activate the neighbor in IPv6 address family

`R2(config-router-af)#neighbor 2001::2 route-map r1 in`	Attach the route-map with route discard configured for the neighbor 2001::2 in IN direction
`R2(config-router)#end`	Exit BGP router mode

R3

`R3#configure terminal`	Enter configure mode
`R3(config)#interface lo`	Enter interface mode for loopback
`R3(config-if)#ip address 3.3.3.2/24 secondary`	Assign an IPV4 address to the interface
`R3(config-if)#exit`	Exit interface mode
`R3(config)#interface xe1`	Enter interface mode for xe1
`R3(config-if)#ipv6 address 4001::2/64`	Assign an IPv6 address to the interface
`R3(config-if)#exit`	Exit interface mode
`R3(config)#interface xe2`	Enter interface mode for xe2
`R3(config-if)#ipv6 address 3001::3/64`	Assign an IPv6 address to the interface
`R3(config-if)#exit`	Exit interface mode
`R3(config)#router bgp 4`	Enter into BGP router mode
`R3(config-router)#bgp router-id 3.3.3.3`	Specify router ID
`R3(config-router)#neighbor 3001::2 remote-as 3`	Create static BGP neighbor 3001::2 with remote autonomous system value 3
`R3(config-router)#address-family ipv6 unicast`	Enter address family IPv6 unicast mode
`R3(config-router-af)#neighbor 3001::2 activate`	Activate neighbor in IPv6 address family
`R3(config-router-af)#redistribute connected`	Advertise the connected network into BGP
`R3(config-router)#end`	Exit BGP router mode.

Validation

```
R2#show running-config bgp
!
router bgp 3
 bgp router-id 2.2.2.2
 neighbor 2001::2 remote-as 2
 neighbor 3001::3 remote-as 4
 !
 address-family ipv6 unicast
 redistribute connected
 neighbor 2001::2 activate
 neighbor 2001::2 route-map r1 in
 neighbor 3001::3 activate
 exit-address-family
!
R2#show  bgp ipv6
BGP table version is 3, local router ID is 2.2.2.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```


© 2021 IP Infusion Inc. Proprietary

```
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network    Next Hop                            Metric  LocPrf  Weight  Path
*> 1001::/64 2001::2(fe80::218:23ff:fede:eecf)
                                                    0      100      0        2?
*> 2001::/64  ::                                    0      100    32768       ?
*             2001::2(fe80::218:23ff:fede:eecf)
                                                    0      100      0        2?
*> 3001::/64  ::                                    0      100     32768      ?
*             3001::3(fe80::eef4:bbff:fe84:781b)  0      100       0       4? *> 4001::/
64 3001::3(fe80::eef4:bbff:fe84:781b)  0      100       0       4?

Total number of prefixes 4


R2#show running-config ipv6 prefix-list
!
ipv6 prefix-list p1 seq 5 permit any
!

R2#

R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 00:56:44
B      1001::/64 [20/0] via ::, Null, 00:00:04
C      2001::/64 via ::, xe1, 00:13:03
C      3001::/64 via ::, xe2, 00:12:56
B      4001::/64 [20/0] via fe80::eef4:bbff:fe84:781b, xe50, 00:00:02
C      fe80::/64 via ::, xe50, 00:46:14


R2#show hsl nh-table
IPv4 FIB 0

IPv4 FIB 1
10.12.29.1, eth0, 00:00:00:00:00:00, Invalid,
                      , Not Installed TO_CPU

IPv6 FIB 0
  , Null, 00:00:00:00:00:00, Valid  ,
                      1001::/64, Installed FORWARD
```

```
2001::2, xe1, 00:18:23:de:ee:cf, Valid  , lport:0x8000034, Egress object id:100003,
refcnt 0, rulecnt 0
3001::3, xe2, ec:f4:bb:84:78:1b, Valid  , lport:0x8000032, Egress object id:100004,
refcnt 0, rulecnt 0
fe80::218:23ff:fede:eecf, xe52, 00:18:23:de:ee:cf, Valid  , lport:0x8000034, Egress
object id:100003, refcn
t 0, rulecnt 0
fe80::eef4:bbff:fe84:781b, xe50, ec:f4:bb:84:78:1b, Valid  , lport:0x8000032, Egress
object id:100004, refc
nt 1, rulecnt 0,
                      4001::/64, Installed FORWARD

IPv6 FIB 1
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 13 Route-map Continue Configuration

This section contains Route-map continue configuration with BGP.

Overview

The continue clauses allow you to configure and organize more modular policy definitions to reduce the number of policy configurations that are repeated within the same route map.

Continue clause under a route-map provides the capability to execute additional entries in a route map after an entry is executed with a successful match and set clauses. The continue command allows multiple entries to be evaluated within a single route-map. Continue commands can be assigned optional sequence numbers that indicates the order in which clauses are to be evaluated.

Using Continue with Match Clauses

When a `match` clause exists in a route-map with continue clause then `continue` clause is executed only when a successful match occurs. If a `match` clause does not exist in the route-map and if a `continue` clause exists, the `continue` clause will be evaluated and will go to the specified route-map entry. When a successful match occurs and we have a `continue` clause, the route-map executes the `set` clauses and then goes to the specified route-map entry. If a `continue` clause does not exist in the next route map, then the route-map will behave normally. If a `continue` clause exists in the next route-map but a match is not successful, the route-map will not continue and will “fall through” to the next sequence number if one exists

Using Continue with Set Actions

`Set` clauses are executed after the route-map evaluation is done. The `set` clauses are evaluated and executed in the order in which they were configured. `Set` clauses are only executed after a successful match occurs. The `continue` statement proceeds to the specified route-map entry only after configured `set` actions are performed. If a `set` action is configured in the first route-map and then the same `set` action occurs again but with a different value, in a subsequent route-map entry, then the last `set` action will override the previous `set` actions which were configured with the same set command.

Topology

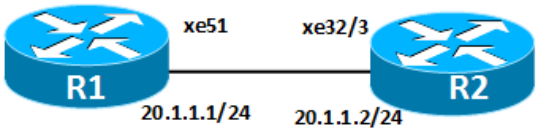


Figure 13-2: Route-map continue

Configure Route-map *continue* on R1

In the below example we will apply route-map `continue` on R1 under BGP 100, with redistributed connected routes from R2 on R1. Here, 10.1.0.0/16 is a superset, while 10.1.1.0/24, 10.1.2.0 /24, 10.1.3.0/24, 10.1.4.0/24, and 10.1.5.0/24 are subsets and will filter PF1, which is a superset and sets several prefixes.

R1

`R1#configure terminal`	Enter configure mode.
`R1(config)#interface xe51`	Enter interface mode.
`R1(config-if)#ip address 20.1.1.1/24`	Configure the IP address of the interface.
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#ip prefix-list PF1`	Configure super set prefix PF1
`R1(config-ip-prefix-list)#seq 5 permit 10.1.0.0/16 le 32`	Permit 10.1.0.0/16 length as 32
`R1(config)#ip prefix-list P1`	Configure subset prefix P1
`R1(config-ip-prefix-list)#seq 5 permit 10.1.1.0/24 le 32`	Permit 10.1.1.0/24 length as 32
`R1(config)#ip prefix-list P2`	Configure subset prefix P2
`R1(config-ip-prefix-list)#seq 5 permit 10.1.2.0/24 le 32`	Permit 10.1.2.0/24 length as 32
`R1(config-ip-prefix-list)#ip prefix-list P3`	Configure subset prefix P3
`R1(config-ip-prefix-list)#seq 5 permit 10.1.3.0/24 le 32`	Permit 10.1.3.0/24 length as 32
`R1(config-ip-prefix-list)#exit`	Exit from prefix-list mode
`R1(config)#route-map myid1 permit 1`	Configure route-map myid1 with sequence number 1
`R1(config-route-map)match ip address prefix-list PF1`	Match for prefix PF1
`R1(config-route-map)continue`	Configure continue command without sequence number
`R1(config-route-map)set metric 10`	Set metric as 10
`R1(config-route-map)set weight 3465789`	Set weight as 3465789
`R1(config-route-map)route-map myid1 permit 2`	Configure route-map myid1 with sequence number 2
`R1(config-route-map)match ip address prefix-list P1`	Match for IP prefix-list P1
`R1(config-route-map)continue 3`	Configure continue with sequence number 3
`R1(config-route-map)set metric 20`	Set metric as 20.
`R1(config-route-map)set origin igp`	Set origin as IGP protocol
`R1(config-route-map)route-map myid1 permit 3`	Configure route-map myid1 with sequence number 3
`R1(config-route-map)match ip address prefix-list P2`	Match for IP prefix-list P2
`R1(config-route-map)continue 4`	Configure continue with sequence number 4
`R1(config-route-map)set metric 30`	Set metric as 30.
`R1(config-route-map)set as-path prepend 600`	Set as-path prepend as 600
`R1(config-route-map)route-map myid1 permit 4`	Configure route-map myid1 with sequence number 4
`R1(config-route-map)match ip address prefix-list P3`	Match for IP prefix-list P3.
`R1(config-route-map)set local-preference 400`	Set local preference as 400
`R1(config-route-map)set weight 400`	Set weight as 400
`R1(config-route-map)end`	End the route-map
`R1(config)#router bgp 100`	Configure bgp process 100
`R1(config-router)#bgp router-id 1.1.1.1`	Configure bgp router id

© 2021 IP Infusion Inc. Proprietary

`R1(config-router)#neighbor 20.1.1.2 remote-as 100`	Configure bgp remote-as 100 with neighbor IP
`R1(config-router)#address-family ipv4`	Enter address-family mode
`R1(config-router-af)#neighbor 20.1.1.2 activate`	Activate neighbor 20.1.1.2
`R1(config-router-af)#neighbor 20.1.1.2 route-map myid1 in`	Configure bgp route-map myid1 as In bound policy with neighbor ip
`R1(config-router-af)#end`	Exit the router bgp mode

R2

`R2#configure terminal`	Enter configure mode.
`R2(config)#interface xe32/1`	Enter interface mode.
`R2(config-if)#ip address 10.1.1.1/24`	Configure the IP address of the interface on an interface which is up and running
`R2(config-if)#interface xe32/2`	Enter interface mode.
`R2(config-if)#ip address 10.1.2.1/24`	Configure the IP address of the interface on an interface which is up and running
`R2(config-if)#interface xe32/4`	Enter interface mode.
`R2(config-if)#ip address 10.1.3.1/24`	Configure the IP address of the interface on an interface which is up and running
`R2(config-if)#interface xe17/1`	Enter interface mode.
`R2(config-if)#ip address 10.1.4.1/24`	Configure the IP address of the interface on an interface which is up and running
`R2(config-if)#interface xe21/1`	Enter interface mode.
`R2(config-if)#ip address 10.1.5.1/24`	Configure the IP address of the interface on an interface which is up and running
`R2(config-if)#interface xe32/3`	Enter interface mode.
`R2(config-if)#ip address 20.1.1.2/24`	Configure the IP address on the connected interface.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#router bgp 100`	Configure BGP process 100
`R2(config-router)#bgp router-id 2.2.2.2`	Configure BGP router id
`R2(config-router)#neighbor 20.1.1.1 remote-as 100`	Configure BGP remote-as 100 with neighbor IP
`R2(config-router)#address-family ipv4`	Enter address-familymode
`R2(config-router-af)#neighbor 20.1.1.1 activate`	Activate neighbor20.1.1.1
`R2(config-router-af)#redistribute connected`	Redistribute the connected routes which are 10 networks here.
`R2(config-router-as)#end`	Exit router BGP mode

© 2021 IP Infusion Inc. Proprietary

Validation

R1

```
R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 5
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
20.1.1.2                 4   100  145        177       5      0      0
00:40:05               5

Total number of neighbors 1

Total number of Established sessions 1

Note: Check the prefixes learnt here are 5.

R1#

R1#show ip bgp
BGP table version is 5, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  10.1.1.0/24      20.1.1.2              20        100           3465789  i
*>i  10.1.2.0/24      20.1.1.2              30        100           3465789 600
?
*>i  10.1.3.0/24      20.1.1.2              10        400           400      ?
*>i  10.1.4.0/24      20.1.1.2              10        100           3465789  ?
*>i  10.1.5.0/24      20.1.1.2              10        100           3465789  ?

Total number of prefixes 5
R1#
```

Note: In the above example, 10.1.4.0/24 and 10.1.5.0/24 prefixes will match only on PF1 which is a super set prefix and metric is set as 10, while the 10.1.1.0/24, 10.1.2.0/24 and 10.1.3.0/24 prefixes will match in P1, P2 and P3 prefix-lists and execute the set clauses respectively.

```
R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default
```


© 2021 IP Infusion Inc. Proprietary

```
IP Route Table for VRF "default"
B     10.1.1.0/24 [200/20] via 20.1.1.2, xe51, 00:45:05
B     10.1.2.0/24 [200/30] via 20.1.1.2, xe51, 00:45:05
B     10.1.3.0/24 [200/10] via 20.1.1.2, xe51, 00:45:05
B     10.1.4.0/24 [200/10] via 20.1.1.2, xe51, 00:25:05
B     10.1.5.0/24 [200/10] via 20.1.1.2, xe51, 00:24:35
C     20.1.1.0/24 is directly connected, xe51, 01:00:40
C     127.0.0.0/8 is directly connected, lo, 02:26:41

Gateway of last resort is not set
R1#

R1#show ip bgp route-map myid1
BGP table version is 5, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>i  10.1.1.0/24      20.1.1.2              20        100           3465789  i
*>i  10.1.2.0/24      20.1.1.2              30        100           3465789 600
?
*>i  10.1.3.0/24      20.1.1.2              10        400           400      ?
*>i  10.1.4.0/24      20.1.1.2              10        100           3465789  ?
*>i  10.1.5.0/24      20.1.1.2              10        100           3465789  ?

Total number of prefixes 5
R1#
R1#
```

R2

```
R2#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
20.1.1.1                 4   100  133        133       3      0      0
00:39:57              0

Total number of neighbors 1

Total number of Established sessions 1
R2#
R2#


R2#show ip bgp
BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop            Metric    LocPrf       Weight Path
*>   10.1.1.0/24      0.0.0.0              0         100            32768    ?
*>   10.1.2.0/24      0.0.0.0              0         100            32768    ?
*>   10.1.3.0/24      0.0.0.0              0         100            32768    ?
*>   10.1.4.0/24      0.0.0.0              0         100            32768    ?
*>   10.1.5.0/24      0.0.0.0              0         100            32768    ?
*>   20.1.1.0/24      0.0.0.0              0         100            32768    ?

Total number of prefixes 6
R2#

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     10.1.1.0/24 is directly connected, xe32/1, 01:02:22
C     10.1.2.0/24 is directly connected, xe32/2, 01:01:46
C     10.1.3.0/24 is directly connected, xe32/4, 01:02:21
C     10.1.4.0/24 is directly connected, xe17/1, 00:26:52
C     10.1.5.0/24 is directly connected, xe21/1, 00:26:32
C     20.1.1.0/24 is directly connected, xe32/3, 01:02:22
C     127.0.0.0/8 is directly connected, lo, 01:34:40

Gateway of last resort is not set
R2#
```

Route-map Show Commands

```
R1#show running-config route-map
    !
    route-map myid1 permit 1
     match ip address prefix-list PF1
     continue
     set metric 10
     set weight 3465789
    !
    route-map myid1 permit 2
     match ip address prefix-list P1
     continue 3
     set metric 20
     set origin igp
    !
    route-map myid1 permit 3
     match ip address prefix-list P2
     continue 4
     set metric 30
     set as-path prepend 600
```


© 2021 IP Infusion Inc. Proprietary

```
    !
    route-map myid1 permit 4
     match ip address prefix-list P3
     set local-preference 400
     set weight 400
    !
    R1#
R1#show route-map
    route-map myid1, permit, sequence 1
      Match clauses:
        ip address prefix-list: PF1
      Continue clause:  next sequence
      Set clauses:
        metric 10
        weight 3465789
    route-map myid1, permit, sequence 2
      Match clauses:
        ip address prefix-list: P1
      Continue clause:  sequence 3:
      Set clauses:
        metric 20
        origin igp
    route-map myid1, permit, sequence 3
      Match clauses:
        ip address prefix-list: P2
      Continue clause:  sequence 4:
      Set clauses:
        metric 30
        as-path prepend 600
    route-map myid1, permit, sequence 4
      Match clauses:
        ip address prefix-list: P3
      Set clauses:
        local-preference 400
        weight 400
    R1#
```

© 2021 IP Infusion Inc. Proprietary

VRF Lite Configuration Guide

Contents

This document contains these chapters and appendices:

- Chapter 1, *VRF Configuration*
- Chapter 2, *OSPF Configuration*
- Chapter 3, *RIP Configuration*
- Chapter 4, *ISIS Configuration*
- Chapter 5, *BGP Configuration*
- Chapter 6, *Inter-VRF Route Leaking Configuration*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 VRF Configuration

Overview

Virtual routing and forwarding (VRF) is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. VRF may be implemented in a network device by distinct routing tables known as forwarding information bases – one per routing instance.

Topology



Figure 1-3: Device topology

Default VRF

`#con t`	Enter the router configuration mode
`(config)#interface eth1`	Switch to interface eth1
`(config-if)#ip address 3.3.3.2/24`	Configure the ip address **`3.3.3.2`** to eth1
`(config-if)#exit`	Exit interface mode.

Adding a Static Route

`#con t`	Enter the router configuration mode
`(config)#ip route  20.20.20.0/24 eth1`	Add static route with eth1 as exit interface

User-Defined VRF

`#con t`	Enter configuration mode.
`(config)#ip vrf vrf1`	Create vrf1
`(config)#exit`	Exit configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf1`	Associate eth1 to vrf1.
`(config-if)#ip address 3.3.3.2/24`	Configure the IP address 3.3.3.2 to eth1
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

Adding a Static Route

`#con t`	Enter the router configuration mode
`(config)# ip route vrf vrf1 20.20.20.0/24 eth1`	Add static route in vrf1 with eth1 as exit interface

Validation

```
#show ip route vrf all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     127.0.0.0/8 is directly connected, lo, 00:14:59
C     192.168.52.0/24 is directly connected, eth0, 00:14:55
IP Route Table for VRF "management"
IP Route Table for VRF "vrf1"
C     3.3.3.0/24 is directly connected, eth1, 00:00:44
S     20.20.20.0/24 [1/0] is directly connected, eth1, 00:00:08

Gateway of last resort is not set
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 OSPF Configuration

Overview

Open Shortest Path First (OSPF) is an interior routing protocol operating within a single autonomous system (AS) that uses a link state routing algorithm. OSPF gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet layer which makes routing decisions based solely on the destination IP address in IP packets.

This chapter covers OSPF configuration in non-default VRF.

Topology



Figure 2-4: OSPF topology for VRF

Configuration IPv4 VRF

R1

`#con t`	Enter the router config mode.
`(config)#ip vrf vrf1`	Create vrf1
`((config-vrf)#exit`	Exit VRF mode
`(config)#router ospf 1 vrf1`	Associate the ospf process with vrf1.
`(config-router)#network 2.2.2.0/24 area 0`	Specify the network type and area 0.
`(config-router)#ex`	Exit the OSPF configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf1`	Associate eth1 to vrf1.
`(config-if)#ip address 2.2.2.1/24`	Assign the IP address 2.2.2.1 to eth1 in vrf1

R2

`#con t`	Enter the router config mode
`(config)#ip vrf vrf1`	Create vrf1
`(config-vrf)#exit`	Exit VRF mode
`(config)#router ospf 1 vrf1`	Associate the ospf process with vrf1
`(config-router)#network 2.2.2.0/24 area 0`	Specify the network type and area 0.
`(config-router)#ex`	Exit router mode.
`(config)#interface eth1`	Enter interface mode.

(config-if)#ip vrf forwarding vrf1	Associate eth1 to vrf1.
(config-if)#ip address 2.2.2.2/24	Assign the IP address 2.2.2.1 to eth1 in vrf1

Validation

R1

```
#show ip ospf neighbor
Total number of full neighbors: 1
OSPF process 1 VRF(vrf1):
Neighbor ID     Pri   State           Dead Time   Address       Interface        Instance
ID
2.2.2.2    1     Full/Backup        00:00:30        2.2.2.2     eth1              0

#show ip route vrf vrf1
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C     2.2.2.0/24 is directly connected, eth1, 00:11:31

Gateway of last resort is not set
```

R2

```
#show ip ospf neighbor
Total number of full neighbors: 1
OSPF process 1 VRF(vrf1):
Neighbor ID     Pri   State         Dead Time   Address       Interface          Instance
ID
2.2.2.1   1       Full/Backup      00:00:35        2.2.2.1        eth1             0

#show ip route vrf vrf1
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C     2.2.2.0/24 is directly connected, eth1, 00:11:31
Gateway of last resort is not set
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 RIP Configuration

The Routing Information Protocol (RIP) is a distance-vector routing protocol which uses the hop count as a routing metric. RIP prevents routing loops by limiting the number of hops allowed — (15) in a path from the source to a destination. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and used to indicate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

Note: This chapter covers RIP configuration in non-default VR and non-default VRF.

Topology

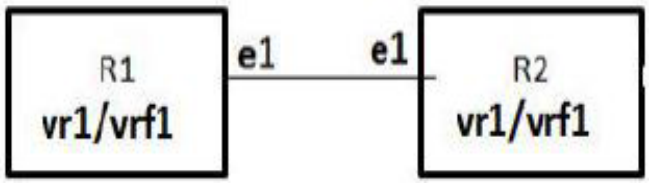


Figure 3-5: RIP topology for VR/VRF

Configuration IPv4 VRF

R1

`#configure terminal`	Enter configure mode.
`(config)#virtual-router VR1`	Create virtual router VR1.
`(config-vr)#load rip`	Load the RIP module in VR1.
`(config)#exit`	Exit VR mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#virtual-router forwarding VR1`	Associate eth1 to VR1.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.
`#login virtual-router VR1`	Log in to virtual-router VR1.
`>en`	Enter privileged exec mode.
`#con t`	Enter configuration mode.
`(config)#ip vrf vrf1`	Create vrf1
`((config-vrf)#exit`	Exit VRF mode
`(config)#router rip`	Enter router mode.
`(config-router)#version 2`	Specify RIP version 2.
`(config-router)#address-family ipv4 vrf  vrf1`	Enter address family mode for vrf1
`(config-router-af)#network 2.2.2.0/24`	Advertise the connected network under rip.
`(config-router-af)#exit`	Exit address-family mode.
`(config-router)#ex`	Exit router mode
`(config)#interface eth1`	Enter interface mode

(config-if)#ip vrf forwarding vrf1	Associate the interface to vrf1
(config-if)#ip address 2.2.2.1/24	Configure the IP address 2.2.2.1 to eth1

R2

#configure terminal	Enter configure mode.
(config)#virtual-router VR1	Create virtual router VR1.
(config-vr)#load rip	Load the rip module in VR1.
(config)#exit	Exit VR mode.
(config)#interface eth1	Enter interface mode.
(config-if)#virtual-router forwarding VR1	Associate eth1 to VR1.
(config-if)#exit	Exit interface mode.
(config)#exit	Exit configure mode.
#login virtual-router VR1	Log in to virtual router VR1.
>en	Enter privileged exec mode.
#con t	Enter configuration mode.
(config)#ip vrf vrf1	Create vrf1
((config-vrf)#exit	Exit VRF mode
(config)#router rip	Enter router mode.
(config-router)#version 2	Specify RIP version 2.
(config-router)#address-family ipv4 vrf vrf1	Enter address family mode for vrf1
(config-router-af)#network 2.2.2.0/24	Advertise the connected network under RIP.
(config-router-af)#exit	Exit address family mode.
(config-router)#ex	Exit router mode
(config)#interface eth1	Enter interface mode
(config-if)#ip vrf forwarding vrf1	Associate the interface to vrf1
(config-if)#ip address 2.2.2.2/24	Configure the IP address 2.2.2.1 to eth1

Validation

Verify the routing table in R1:

```
#show ip route vrf vrf1
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default
IP Route Table for VRF "vrf1"
C       2.2.2.0/24 is directly connected, eth1
Gateway of last resort is not set
```

Verify RIP database in R1:

```
#show ip rip database vrf vrf1
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
```


© 2021 IP Infusion Inc. Proprietary

```
        C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
   Network            Next Hop         Metric  From            If     Time
  Rc 2.2.2.0/24                              1                          eth1
```

Verify the routing table in R2:

```
#show ip route vrf vrf1
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default
IP Route Table for VRF "vrf1"
C       2.2.2.0/24 is directly connected, eth1
Gateway of last resort is not set
```

Verify RIP database in R2:

```
#show ip rip database vrf vrf1
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
   Network            Next Hop         Metric From            If     Time
  Rc 2.2.2.0/24                              1                          eth1
```

Configuration IPv6 VRF

R1

`#configure terminal`	Enter the Configure mode.
`(config)#virtual-router VR1`	Create a virtual router VR1.
`(config-vr)#load ipv6 rip`	Load the RIPng module to be used in VR1.
`(config)#exit`	Exit the VR mode.
`(config)#interface eth1`	Switch to interface eth1.
`(config-if)#virtual-router forwarding VR1`	Associate eth1 to VR1.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit the router config mode.
`#login virtual-router VR1`	Login in to virtual-router VR1.
`>en`	Enable the config mode.
`#con t`	Enter the router configuration mode.
`(config)#ip vrf vrf1`	Create the vrf1
`(config-vrf)#exit`	Exit the vrf
`(config)#router ipv6 rip`	Enable ipv6 rip
`(config-router)#address-family ipv6 vrf vrf1`	Switch to ipv6 rip address family
`(config-router-af)#aggregate-address 2222::/48`	Configure the ipv6 aggregate-address
`(config-router-af)#exit`	Exit the router rip mode.
`(config-router)#ex`	exit.

(config)#interface eth1	Switch to interface eth1
(config-if)#ip vrf forwarding vrf1	Associate eth1 to the vrf1
(config-if)#ip address 2.2.2.1/24	Configure the ip address 2.2.2.2 to interface eth1
(config-if)#ipv6 address 2222::1/48	Configure the ipv6 address.
(config-if)#ipv6 address fe80::1/48	Configure the link local address
(config-if)#ipv6 router rip	Associate interface eth1 to ipv6 rip

R2

#configure terminal	Enter the Configure mode.
(config)#virtual-router VR1	Create a virtual router VR1.
(config-vr)#load ipv6 rip	Load the Ripng module to be used in VR1
(config)#exit	Exit the VR mode.
(config)#interface eth1	Switch to interface eth1.
(config-if)#virtual-router forwarding VR1	Associate eth1 to VR1.
(config-if)#exit	Exit interface mode.
(config)#exit	Exit the router config mode.
#login virtual-router VR1	Login in to virtual-router VR1.
>en	Enable the config mode.
#con t	Enter the router configuration mode.
(config)#ip vrf vrf1	Create the vrf1
(config-vrf)#exit	Exit the vrf
(config)#router ipv6 rip	Switch to the rip ipv6 address family
(config-router)#address-family ipv6 vrf vrf1	Switch to the rip ipv6 address family
(config-router-af)#aggregate-address 2222::/48	Configure the ipv6 aggregate address
(config-router-af)#exit	Exit the address ipv6 rip address family
(config-router)#ex	Exit the router IPV6 rip mode.
(config)#interface eth1	Exit to the router config mode
(config-if)#ip vrf forwarding vrf	Associate eth1 to the vrf1
(config-if)#ip address 2.2.2.2/24	Configure the ip address 2.2.2.1 to eth eth1
(config-if)#ipv6 address 2222::2/48	Configure the ipv6 address.
(config-if)#ipv6 address fe80::2/48	Configure the link local address
(config-if)#ipv6 router rip	Associate interface eth1 to ipv6 rip

Validation

```
rtr1#show ipv6 route vrf vrf1
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, I - IS-IS, B - BGP
Timers: Uptime
IP Route Table for VRF "vrf1"
C      2222::/48 via ::, eth1, 00:06:19
```


© 2021 IP Infusion Inc. Proprietary

```
C      fe80::/48 via ::, eth1, 00:02:33
rtr18#show ipv6 rip database vrf vrf1
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP aggregated,
       Rcx - RIP connect suppressed, Rsx - RIP static suppressed,
       K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
   Network                    Next Hop                  If     Met Tag  Time
Rcx 2222::/48                 ::                        eth1     1   0

rtr2#show ipv6 rip interface
eth1 is up, line protocol is up
  Routing Protocol: RIPng
    VPN Routing/Forwarding: vrf1
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IPv6 interface address:
      2222::1/48
      fe80::1/48
eth2 is up, line protocol is up
  RIPng is not enabled on this interface
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 ISIS Configuration

Overview

Intermediate System to Intermediate System (IS-IS) is an interior routing protocol operating within a single administrative domain.It is a link-state routing protocol, operating by reliably flooding link state information throughout a network of routers. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information. IS-IS uses Dijkstra's algorithm for computing the best path through the network. Packets (datagrams) are then forwarded, based on the computed ideal path, through the network to the destination.

Topology

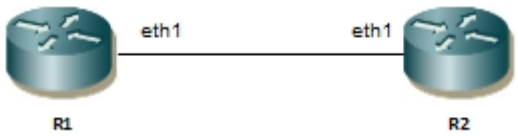


Figure 4-6: ISIS Topology for VRF

Configuration IPv4 VRF

R1

`#con t`	Enter configuration mode.
`(config)#ip vrf vrf1`	Create vrf1
`(config-vrf)#exit`	Exit VRF mode
`(config)#router isis 1 vrf1`	Associate the ISIS process to vrf1
`(config-router)#net 49.0001.0000.0000.0001.00`	Establish a network entity title for this instance, specifying the area address and the system ID.
`(config-router)#is-type level-1`	Configure instance 1 as level-1 routing
`(config-router)#exit`	Exit router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf1`	Associate the interface to vrf1
`(config-if)#ip address 2.2.2.1/24`	Configure the IP address 2.2.2.1 to eth1
`(config-if)#ip router isis 1`	Enable ISIS routing on an instance for area 49
`(config-if)#isis circuit-type level-1`	Configure interface as level-1
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit config mode

R2

#con t	Enter configuration mode.
(config)#ip vrf vrf1	Create vrf1
(config-vrf)#exit	Exit VRF mode
(config)#router isis 1 vrf1	Associate the ISIS process to vrf1
(config-router)#net 49.0001.0000.0000.0002.00	Establish a network entity title for this instance, specifying the area address and the system ID.
(config-router)#is-type level-1	Configure instance 1 as level-1 routing
(config-router)#exit	Exit router mode
(config)#interface eth1	Enter interface mode
(config-if)#ip vrf forwarding vrf1	Associate the interface to vrf1
(config-if)#ip address 2.2.2.2/24	Configure the IP address 2.2.2.1 to eth1
(config-if)#ip router isis 1	Enable ISIS routing on an instance for area 49
(config-if)#isis circuit-type level-1	Configure interface as level-1
(config-if)#exit	Exit interface mode
(config)#exit	Exit config mode

Validation

R1

```
#show clns neighbors
Tag 1:  VRF : vrf1
System Id      Interface   SNPA      State     Holdtime        Type     Protocol
0000.0000.0002      eth1   5254.00d1.5789      Up          9    L1      IS-IS
```

R2

```
#show clns neighbors
Tag 1:  VRF : vrf1
System Id      Interface   SNPA               State  Holdtime  Type Protocol
0000.0000.0001 eth1        5254.0024.4323     Up     26        L1   IS-IS
```

R1

```
#show ip isis route
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric

Tag 1:  VRF : vrf1
     Destination         Metric      Next-Hop            Interface      Tag
C    2.2.2.0/24         10         --                eth1          0            0
```

R2

```
#show ip isis route
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
```


© 2021 IP Infusion Inc. Proprietary

```
Tag 1:  VRF : vrf1
     Destination         Metric      Next-Hop            Interface      Tag
C    2.2.2.0/24         10         --                eth1          0            0
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 BGP Configuration

Overview

Border Gateway Protocol (BGP) makes core routing decisions on the Internet using a table of IP networks or “prefixes” which designate network reachability among autonomous systems (AS). BGP is a path vector protocol or a variant of a distance-vector routing protocol. BGP does not involve traditional Interior Gateway Protocol (IGP) metrics, but routing decisions are made based on path, network policies, and/or rule sets. For this reason, it is more appropriately termed a reachability protocol rather than routing protocol.

Note: This chapter covers BGP configuration in non-default VR and non-default VRF.

Enabling dynamic capability on the specific BGP peer will prevent BGP session to reset.

Topology



Figure 5-7: BGP topology for VRF

Configuration

R1

`#con t`	Enter configuration mode.
`(config)#ip vrf vrf1`	Create vrf1
`(config-vrf)#rd 800:1`	Specify the route distinguisher in the VRF
`(config-vrf)#route-target import 800:1`	Specify the import route target
`(config-vrf)#route-target export 800:1`	Specify the export route target
`(config-vrf)#exit`	Exit VRF mode
`(config)#router bgp 200`	Enter the bgp configuration mode
`(config-router)#address-family ipv4 vrf  vrf1`	Enter address family mode for vrf1
`(config-router-af)#neighbor 2.2.2.2 remote-as 100`	Specify the BGP neighbor and remote-AS.
`(config-router-af)#exit`	Exit address family mode.
`(config-router)#ex`	Exit router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf1`	Associate the interface to vrf1
`(config-if)#ip address 2.2.2.1/24`	Configure the IP address 2.2.2.1 to eth1

© 2021 IP Infusion Inc. Proprietary

R2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrf1`	Create vrf1
`(config-vrf)#rd 800:1`	Specify the route distinguisher in the VRF
`(config-vrf)#route-target import 800:1`	Specify the import route target
`(config-vrf)#route-target export 800:1`	Specify the export route target
`(config-vrf)#exit`	Exit vrf mode
`(config)#router bgp 100`	Enter router mode.
`(config-router)#address-family ipv4 vrf  vrf1`	Enter address family mode for vrf1
`(config-router-af)#neighbour 2.2.2.1 remote-as 200`	Specify the BGP neighbor and remote-as.
`(config-router-af)#exit`	Exit address family mode.
`(config-router)#ex`	Exit router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf1`	Associate the interface to vrf1
`(config-if)#ip address 2.2.2.2/24`	Configure the IP address 2.2.2.1 to eth1

Validation

Verify the routing table in R1

```
#show ip bgp neighbors
BGP neighbor is 2.2.2.2, vrf vrf1, remote AS 100, local AS 200, external link
  BGP version 4, local router ID 2.2.2.1, remote router ID 2.2.2.2
  BGP state = Established, up for 00:00:14
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 3 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 2.2.2.1, Local port: 179
Foreign host: 2.2.2.2, Foreign port: 36200
Nexthop: 2.2.2.1
Nexthop global: ::
Nexthop local: ::
```


© 2021 IP Infusion Inc. Proprietary

```
BGP connection: non shared network
```

Verify the routing table in R2

```
#show ip bgp neighbors
BBGP neighbor is 2.2.2.1, vrf vrf1, remote AS 200, local AS 100, external link
  BGP version 4, local router ID 2.2.2.2, remote router ID 2.2.2.1
  BGP state = Established, up for 00:08:09
  Last read 00:00:09, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 18 messages, 0 notifications, 0 in queue
  Sent 18 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 2.2.2.2, Local port: 36200
Foreign host: 2.2.2.1, Foreign port: 179
Nexthop: 2.2.2.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

R1

```
#show ip route vrf vrf1
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C     2.2.2.0/24 is directly connected, eth1, 00:20:40

Gateway of last resort is not set
```

R2

```
#show ip route vrf vrf1
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "vrf1"
C     2.2.2.0/24 is directly connected, eth1, 00:14:53

Gateway of last resort is not set
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 6 Inter-VRF Route Leaking Configuration

This chapter shows how to configure inter-VRF route leaking.

Overview

Virtual Routing and Forwarding (VRF) provides the ability to have multiple virtual routers on a single physical device. VRFs operate without knowledge of one another unless they are imported or exported into one another using inter-VRF route leaking. Inter-VRF route leaking allows leaking of route prefixes from one VRF instance to another VRF instance on the same physical router which eliminates the need for external routing.This is useful in cases where multiple VRFs share the same path to reach an external domain, while maintaining their internal routing information limited to their own VRF. This feature enables a data center to consolidate multiple VRF services onto a single server.

There are two types of inter-VRF route leaking:

- Static leaking: leaking manually configured static route entries from a source VRF to a global default VRF table.
- Dynamic leaking: leaking connected routes and dynamically learned routes from protocols such as ISIS, OSPF, and BGP from a source VRF to a destination VRF.

Static Leaking

Static route leaking directly between VRFs is not supported. What does work is routing traffic from a VRF to the global default VRF routing table. One advantage of using static route leaking is that you can configure exactly which routes are reachable without configuring BGP.

Topology

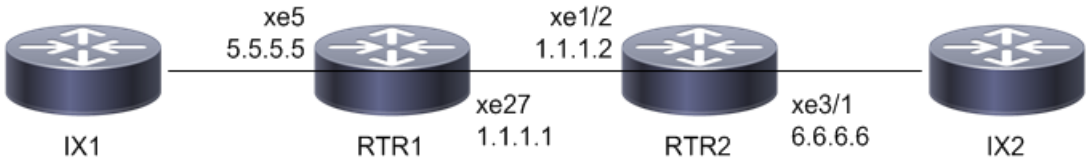


Figure 6-8: Static leaking

Configuration

The following steps describe how to configure static leaking.

RTR1

`RTR1#configure terminal`	Enter configure mode.
`RTR1(config)#interface xe5`	Enter interface mode
`RTR1(config-if)#ip address 5.5.5.5/24`	Assign IP address 5.5.5.5 to interface xe5
`RTR1(config-if)#exit`	Exit interface mode
`RTR1(config)#interface xe27`	Enter interface mode

`RTR1(config-if)#ip address 1.1.1.1/24`	Assign IP address 1.1.1.1 to interface xe27
`RTR1(config-if)#exit`	Exit interface mode

RTR2

`RTR2#configure terminal`	Enter configure mode.
`RTR2(config)#interface xe1/2`	Enter interface mode
`RTR2(config-if)#ip address 1.1.1.2/24`	Assign IP address 1.1.1.2 to interface xe1/2
`RTR2(config-if)#exit`	Exit interface mode
`RTR2(config)#ip vrf vrf1`	Create VRF vrf1
`RTR2(config-vrf)#exit`	Exit VRF mode
`RTR2(config)#interface xe3/1`	Enter interface mode
`RTR2(config-if)#ip vrf forwarding vrf1`	Associate xe3/1 to vrf1
`RTR2(config-if)#ip address 6.6.6.6/24`	Assign IP address 6.6.6.6 to interface xe3/1
`RTR2(config-if)#exit`	Exit interface mode
`RTR2(config)#ip route vrf vrf1 5.5.5.0/24 1.1.1.1 xe1/2 global`	Add static route to reach global default VRF table
`RTR2(config)#exit`	Exit configure mode

Validation

```
RTR2#show ip route vrf all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     1.1.1.0/24 is directly connected, xe1/2, 00:00:05
C     127.0.0.0/8 is directly connected, lo, 00:20:38
IP Route Table for VRF "management"
Gateway of last resort is 10.12.29.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.12.29.1, eth0, 00:20:38
C     10.12.29.0/24 is directly connected, eth0, 00:20:38
C     127.0.0.0/8 is directly connected, lo.management, 00:20:38
IP Route Table for VRF "vrf1"
S    v5.5.5.0/24 [1/0] via 1.1.1.1, xe1/2, 00:05:20
C     6.6.6.0/24 is directly connected, xe3/1, 00:07:06
C     127.0.0.0/8 is directly connected, lo.vrf1, 00:12:25

RTR2#show ip route vrf all database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```


© 2021 IP Infusion Inc. Proprietary

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
C    *>  1.1.1.0/24 is directly connected, xe1/2, 00:00:51
C    *>  127.0.0.0/8 is directly connected, lo, 00:21:24
IP Route Table for VRF "management"
S    *>  0.0.0.0/0 [1/0] via 10.12.29.1, eth0, 00:21:24
C    *>  10.12.29.0/24 is directly connected, eth0, 00:21:24
C    *>  127.0.0.0/8 is directly connected, lo.management, 00:21:24
IP Route Table for VRF "vrf1"
S    *> v5.5.5.0/24 [1/0] via 1.1.1.1, xe1/2, 00:06:06
C    *>  6.6.6.0/24 is directly connected, xe3/1, 00:07:52
C    *>  127.0.0.0/8 is directly connected, lo.vrf1, 00:13:11
```

Dynamic Leaking

Route Leaking enables communication between isolated (virtual) routing domains by segregating and sharing a set of services that are available on one routing domain with other virtual domains. Inter-VRF route leaking enables a VRF to leak or export routes in its router to one or more VRFs. Dynamic route leaking enables a source VRF to share both its connected routes as well as dynamically learned routes from protocols such as ISIS, OSPF, and BGP to destination VRFs.

Topology



Figure 6-9: Dynamic leaking

Configuration

The following steps describe how to configure dynamic leaking.

RTR1

`RTR1#configure terminal`	Enter configure mode.
`RTR1(config)#interface xe5`	Enter interface mode
`RTR1(config-if)#ip address 5.5.5.5/24`	Assign IP address 5.5.5.5 to interface xe5
`RTR1(config-if)#exit`	Exit interface mode
`RTR1(config)#interface xe27`	Enter interface mode
`RTR1(config-if)#ip address 1.1.1.1/24`	Assign IP address 1.1.1.1 to interface xe27

`RTR1(config-if)#exit`	Exit interface mode
`RTR1(config)#router ospf 1`	Enter OSPF router mode
`RTR1(config-router)#network 1.1.1.0/24 area 0`	Specify the network type and area 0
`RTR1(config-router)#redistribute connected`	Redistribute connected route inside ospf
`RTR1(config-router)#exit`	Exit OSPF router mode

RTR2

`RTR2#configure terminal`	Enter configure mode.
`RTR2(config)#ip vrf vrf1`	Create VRF vrf1
`RTR2(config-vrf)#rd 100:1`	Configure route distinguisher in the VRF
`RTR2(config-vrf)#route-target export 100:1`	Configure export route target
`RTR2(config-vrf)#route-target import 200:1`	Configure import route target
`RTR2(config-vrf)#exit`	Exit VRF mode
`RTR2(config)#ip vrf vrf2`	Create VRF vrf2
`RTR2(config-vrf)#rd 200:1`	Configure route distinguisher in the VRF
`RTR2(config-vrf)#route-target export 200:1`	Configure export route target
`RTR2(config-vrf)#route-target import 100:1`	Configure import route target
`RTR2(config-vrf)#exit`	Exit VRF mode
`RTR2(config)#interface xe1/2`	Enter interface mode
`RTR2(config-if)#ip vrf forwarding vrf1`	Associate vrf1 to interface xe1/2
`RTR2(config-if)#ip address 1.1.1.2/24`	Assign IP address 1.1.1.2 to interface xe1/2
`RTR2(config-if)#exit`	Exit interface mode
`RTR2(config)#interface xe3/3`	Enter interface mode
`RTR2(config-if)#ip vrf forwarding vrf2`	Associate vrf2 to interface xe3/3
`RTR2(config-if)#ip address 2.2.2.2/24`	Assign IP address 2.2.2.2 to interface xe3/3
`RTR2(config-if)#exit`	Exit interface mode
`RTR2(config)#router ospf 1 vrf1`	Associate the OSPF process with vrf1
`RTR2(config-router)#network 1.1.1.0/24 area 0`	Specify the network type and area 0
`RTR2(config-router)#redistribute bgp`	Redistribute BGP routes inside OSPF
`RTR2(config-router)#exit`	Exit router mode
`RTR2(config)#router ospf 2 vrf2`	Associate the OSPF process with vrf2
`RTR2(config-router)#network 2.2.2.0/24 area 0`	Specify the network type and area 0
`RTR2(config-router)#redistribute bgp`	Redistribute BGP routes inside OSPF
`RTR2(config-router)#exit`	Exit router mode
`RTR2(config)#router bgp 100`	Enter BGP router mode
`RTR2(config-router)#address-family ipv4 vrf vrf1`	Enter address family mode for vrf1
`RTR2(config-router-af)#redistribute ospf 1`	Redistribute OSPF routes inside BGP
`RTR2(config-router-af)#exit-address-family`	Exit address family mode

© 2021 IP Infusion Inc. Proprietary

`RTR2(config-router)#address-family ipv4 vrf vrf2`	Enter address family mode for vrf2
`RTR2(config-router-af)#redistribute ospf 2`	Redistribute OSPF routes inside BGP
`RTR2(config-router-af)#exit-address-family`	Exit address family mode
`RTR2(config-router)#exit`	Exit router mode

RTR3

`RTR3#configure terminal`	Enter configure mode.
`RTR3(config)#interface xe1`	Enter interface mode
`RTR3(config-if)#ip address 6.6.6.6/24`	Assign IP address 6.6.6.6 to interface xe1
`RTR3(config-if)#exit`	Exit from config mode
`RTR3(config)#interface xe33`	Enter interface mode
`RTR3(config-if)#ip address 2.2.2.3/24`	Assign IP address 2.2.2.3 to interface xe33
`RTR3(config-if)#exit`	Exit interface mode
`RTR3(config)#router ospf 2`	Enter OSPF router mode
`RTR3(config-router)#network 2.2.2.0/24 area 0`	Specify the network type and area 0
`RTR3(config-router)#redistribute connected`	Redistribute connected route inside ospf
`RTR3(config-router)#exit`	Exit OSPF router mode

Validation

RTR1

```
RTR1#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
       Instance ID
1.1.1.2           1   Full/Backup     00:00:39    1.1.1.2         xe27

RTR1#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     1.1.1.0/24 is directly connected, xe27, 01:51:47
O E2  2.2.2.0/24 [110/1] via 1.1.1.2, xe27, 00:22:51
C     5.5.5.0/24 is directly connected, xe5, 02:16:39
O E2  6.6.6.0/24 [110/1] via 1.1.1.2, xe27, 00:22:51
```

```
C     127.0.0.0/8 is directly connected, lo, 02:25:23
```

RTR2

```
RTR2#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(vrf1):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
5.5.5.5           1   Full/DR         00:00:34    1.1.1.1         xe1/2                 0

Total number of full neighbors: 1
OSPF process 2 VRF(vrf2):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
6.6.6.6           1   Full/DR         00:00:36    2.2.2.3         xe3/3                 0

RTR2#sh ip route vrf all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     127.0.0.0/8 is directly connected, lo, 02:06:03
IP Route Table for VRF "management"
Gateway of last resort is 10.12.29.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.12.29.1, eth0, 02:06:03
C     10.12.29.0/24 is directly connected, eth0, 02:06:03
C     127.0.0.0/8 is directly connected, lo.management, 02:06:03
IP Route Table for VRF "vrf1"
C     1.1.1.0/24 is directly connected, xe1/2, 01:31:20
B    v2.2.2.0/24 [20/1] is directly connected, xe3/3, 00:02:35
O E2  5.5.5.0/24 [110/20] via 1.1.1.1, xe1/2, 00:07:12
B    v6.6.6.0/24 [20/20] via 2.2.2.3, xe3/3, 00:02:35
C     127.0.0.0/8 is directly connected, lo.vrf1, 01:40:49
IP Route Table for VRF "vrf2"
B    v1.1.1.0/24 [20/1] is directly connected, xe1/2, 00:03:35
C     2.2.2.0/24 is directly connected, xe3/3, 01:31:02
B    v5.5.5.0/24 [20/20] via 1.1.1.1, xe1/2, 00:03:35
O E2  6.6.6.0/24 [110/20] via 2.2.2.3, xe3/3, 00:06:52
C     127.0.0.0/8 is directly connected, lo.vrf2, 01:32:22

RTR2#sh ip route vrf all database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```


© 2021 IP Infusion Inc. Proprietary

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
C    *>  127.0.0.0/8 is directly connected, lo, 02:07:34
IP Route Table for VRF "management"
S    *>  0.0.0.0/0 [1/0] via 10.12.29.1, eth0, 02:07:34
C    *>  10.12.29.0/24 is directly connected, eth0, 02:07:34
C    *>  127.0.0.0/8 is directly connected, lo.management, 02:07:34
IP Route Table for VRF "vrf1"
C    *>  1.1.1.0/24 is directly connected, xe1/2, 01:32:51
O        1.1.1.0/24 [110/1] is directly connected, xe1/2, 00:09:13
B    *> v2.2.2.0/24 [20/1] is directly connected, xe3/3, 00:04:06
O E2 *>  5.5.5.0/24 [110/20] via 1.1.1.1, xe1/2, 00:08:43
B    *> v6.6.6.0/24 [20/20] via 2.2.2.3, xe3/3, 00:04:06
C    *>  127.0.0.0/8 is directly connected, lo.vrf1, 01:42:20
IP Route Table for VRF "vrf2"
B    *> v1.1.1.0/24 [20/1] is directly connected, xe1/2, 00:05:06
C    *>  2.2.2.0/24 is directly connected, xe3/3, 01:32:33
O        2.2.2.0/24 [110/1] is directly connected, xe3/3, 00:08:42
B    *> v5.5.5.0/24 [20/20] via 1.1.1.1, xe1/2, 00:05:06
O E2 *>  6.6.6.0/24 [110/20] via 2.2.2.3, xe3/3, 00:08:23
C    *>  127.0.0.0/8 is directly connected, lo.vrf2, 01:33:53
```

RTR3

```
RTR3#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 2 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
2.2.2.2           1   Full/Backup     00:00:37    2.2.2.2         xe33                    0

RTR3#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
O E2  1.1.1.0/24 [110/1] via 2.2.2.2, xe33, 00:20:12
C     2.2.2.0/24 is directly connected, xe33, 01:47:45
O E2  5.5.5.0/24 [110/1] via 2.2.2.2, xe33, 00:20:12
C     6.6.6.0/24 is directly connected, xe1, 02:00:13
C     127.0.0.0/8 is directly connected, lo, 02:21:14
```

© 2021 IP Infusion Inc. Proprietary

Fundamental Layer 3 Command Reference

Contents

This document contains this chapter:

- Chapter 1, *Fundamental Layer 3 Commands*
- Chapter 2, *Route-Map Commands*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Fundamental Layer 3 Commands

This chapter describes the fundamental Layer 3 commands:

- automatic-router-id-selection enable
- clear ip route kernel
- clear ip route
- clear ip route vrf NAME
- clear router-id
- debug rib
- description
- fib retain
- ip route
- ip urpf enable
- ip urpf allow-default
- ip vrf
- maximum-paths
- max-static-routes
- router-id
- show debugging rib
- show ip rpf
- show ipv6 rpf
- show router-id
- show running-config router
- show running-config router-id
- show running-config urpf
- show running-config vrf
- snmp restart rib
- subscriber urpf enable

© 2021 IP Infusion Inc. Proprietary

automatic-router-id-selection enable

Use this command to assure that OcNOS selects the loopback IP address as the router-id each time the device is rebooted.

Use the `no` form of this command to remove this constraint.

Command Syntax

```
automatic-router-id-selection enable
```

```
no automatic-router-id-selection enable
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#automatic-router-id-selection enable
(config)#
```


© 2021 IP Infusion Inc. Proprietary

clear ip route kernel

Use this command to clear stale IPv4 routes from the RIB (Routing Information Base) and FIB (Forwarding Information Base).

Command Syntax

```
clear ip route kernel
clear ip kernel route
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip route kernel
```

clear ip route

Use this command to clear an all IPv4 routes or any specific prefix routes.

Command Syntax

```
clear ip route (*|A.B.C.D/M)
```

Parameters

`*`	Clears all routes
`A.B.C.D/M`	Prefix to be cleared

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip route *
#clear ip route 1.1.1.0/24
```


© 2021 IP Infusion Inc. Proprietary

clear ip route vrf NAME

Use this command to clear all IPv4 VRF route or any specific prefix VRF route of any particular VRF name.

Command Syntax

```
clear ip route vrf NAME (*|A.B.C.D/M)
```

Parameters

NAME	VPN Routing or Forwarding instance name
*	Clears all routes
A.B.C.D/M	Prefix to be cleared

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip route vrf myVRF *
```

clear router-id

Use this command to clear the current Router-Id and trigger the Router-Id calculation again. The new Router-id is sent to all protocol modules.

- To clear only the router-id for the default VRF, enter `clear router-id`.
- To clear the router-id for a particular VRF, enter `clear router-id vrf VRFNAME`.
- To clear the router-id for all VRFs, enter `clear router-id vrf`.

Command Syntax

```
clear router-id (vrf (VRFNAME|))
```

Parameters

`VRFNAME`	VPN routing/forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#clear router-id
(config)#
```

```
#configure terminal
(config)#clear router-id vrf
(config)#
```


© 2021 IP Infusion Inc. Proprietary

debug rib

Use this command to debug the `ribd` process.

Use the `no` form of this command or the `undebug` command to stop debugging.

Command Syntax

```
debug rib (all|)
debug rib events
debug rib packet (recv|send|) (detail|)
debug rib nsm
debug rib bfd
debug rib kernel
debug rib monitor
debug ip routing (add-route|delete-route|mod-route|
no debug all
no debug rib (all|)
no debug all rib
no debug rib events
no debug rib packet (recv|send|) (detail|)
no debug rib nsm
no debug rib bfd
no debug rib kernel
no debug rib monitor
no debug ip routing (add-route|delete-route|mod-route|)
undebug all
undebug rib (all|)
undebug all rib
undebug rib events
undebug rib packet (recv|send|) (detail|)
undebug rib nsm
undebug rib bfd
undebug rib kernel
```

Parameters

`all`	All debugging functions
`events`	Events
`packet`	Packet events
`recv`	Received packets
`send`	Sent packets

`detail`	Detailed information
`nsm`	NSM events
`kernel`	RIB kernel
`monitor`	Enable Monitor route netlink
`bfd`	BFD (Bidirectional Forwarding Detection) events
`ip routing`	IPv4 routing events
`add-route`	Add route events
`delete-route`	Delete route events
`mod-route`	Modify route events

Disabled

By default, debug command is disabled.

Command Mode

Privileged Exec mod

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug rib all
```


© 2021 IP Infusion Inc. Proprietary

description

Use this command to assign a description to a Virtual Router instance.

Use the `no` parameter to remove a description.

Command Syntax

```
description LINE
no description
```

Parameters

`LINE`	Virtual Router description maximum 80 characters

Disabled

By default, description command is disabled

Command Mode

VR mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#virtual-router VR1
(config-vr)#description VR1 has been created for CLI testing
(config-vr)#exit

(config)#virtual-router VR1
(config-vr)#no description
(config-vr)#exit
```

fib retain

Use this command to set the retention time for stale routes in the Forwarding Information Base (FIB) when `ribd` restarts. The `ribd` process reads the FIB and treats previously self-installed routes as stale.

You can display stale routes by running the `show ip route database` command. All routes preceded by the symbol `p` are stale routes. When protocol modules restart, `ribd` overrides these stale routes with routes updated by the protocol modules.

Table 1-116 show the behavior of routes when `ribd` stops.

Table 1-116: FIB retention

Command	Behavior
`fib retain`	Does not clear routes from the FIB and retains stale routes for 60 seconds when restarted.
`fib retain forever`	Does not clear routes and retains stale routes forever.
`fib retain time <1-65535>`	Does not clear routes and retains stale routes for the specified seconds.
`no fib retain` (default)	Cleans up routes in the FIB, but retains stale routes for 60 seconds when restarted.

You can remove stale routes at any time with the clear ip route kernel command.

Use the `no` form of this command to revert to default; that is, do not retain routes in the FIB when `ribd` stops.

Command Syntax

```
fib retain (forever|time <1-65535>|)
no fib retain (forever|time <1-65535>|)
```

Parameters

`forever`	Retain FIB forever
`time`	Retain FIB for a time after `ribd` restarts
`<1-65535>`	Retention time in seconds; if you omit this value, the default is 60 seconds

Default

Routes are cleared from the FIB when `ribd` stops. However, when `ribd` restarts, stale routes are retained for 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#fib retain time 180
```


© 2021 IP Infusion Inc. Proprietary

ip route

Use this command to create an IPv4 static route.

Use the `no` form of this command to delete a static route.

Command Syntax

```
ip route A.B.C.D/M (A.B.C.D|IFNAME)
ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME)
ip route A.B.C.D/M (A.B.C.D|IFNAME){<1-255>|tag <0-4294967295>|description WORD}
ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME){<1-255>|tag <0-4294967295>|description
  WORD}
ip route vrf NAME A.B.C.D/M IFNAME
ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME
ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME global
ip route vrf NAME A.B.C.D/M IFNAME {<1-255>|tag <0-4294967295>|description WORD}
ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME {<1-255>|tag <0-4294967295>|description
  WORD}
no ip route A.B.C.D/M (A.B.C.D|IFNAME|)
no ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME)
no ip route A.B.C.D/M (A.B.C.D|IFNAME){<1-255>|tag <0-4294967295>|description WORD}
no ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME){<1-255>|tag <0-4294967295>|description
  WORD}
no ip route vrf NAME A.B.C.D/M IFNAME
no ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME
no ip route vrf NAME A.B.C.D/M IFNAME {<1-225>|tag <0-4294967295>|description WORD}
no ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME {<1-255>|tag <0-
  4294967295>|description WORD}
```

Parameters

`A.B.C.D/M`	Subnet: IP destination prefix and a mask length
`A.B.C.D A.B.C.D`	Subnet: IP destination address and mask
`A.B.C.D`	Gateway nexthop IPv4 address
`global`	Global table lookup (to support inter-VRF static route leaking)
`<1-255>`	Administrative distance
`IFNAME`	Gateway nexthop interface name
`description`	Description of the static route maximum 80 character
`tag`	Tag used as a “match” value to control redistribution via route maps
`<0-4294967295>`	Tag value

`vrf`	VRF (Virtual Routing and Forwarding) instance
`NAME`	VRF name

Default

By default, no static IPv4 route configured

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and was updated in OcNOS version 1.3.4.

Examples

```
#configure terminal
(config)#ip route 192.168.3.0 255.255.255.0 2.2.2.2 128
(config)#ip route 1.1.1.0/24 eth0 32
(config)#ip route vrf new 1.1.1.1/1 1.1.1.1 eth1 description new tag 1
```

This example creates VRF static routes with the nexthops belonging to the default VRF. The nexthop gateway address can be the IFNAME network address or any other IP address reachable via IFNAME.

```
#show ip route vrf
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     10.12.19.0/24 is directly connected, eth0, 4d23h06m
C     11.1.1.0/24 is directly connected, eth4, 4d23h01m
C     13.13.13.0/31 is directly connected, eth3, 4d23h06m
C     50.5.5.0/24 is directly connected, eth3, 4d23h06m
C     100.100.100.0/24 is directly connected, lo, 4d23h06m
O     101.1.1.1/32 [110/11] via 11.1.1.2, eth4, 19:20:39
C     127.0.0.0/8 is directly connected, lo, 4d23h06m
Gateway of last resort is not set

(config)#ip route vrf vrf1 201.201.201.201/32 11.1.1.11 eth4 global
(config)#ip route vrf vrf1 202.202.202.202/32 101.1.1.1 eth4 global

#show ip route vrf vrf1 static
IP Route Table for VRF "vrf1"
S    v201.201.201.201/32 [1/0] via 11.1.1.11, eth4, 00:00:44
S    v202.202.202.202/32 [1/0] via 101.1.1.1, eth4 (recursive via 11.1.1.2), 00:00:17
Gateway of last resort is not set
```


© 2021 IP Infusion Inc. Proprietary

ip urpf enable

Use this command to enable uRPF mode on the system.

Use the `no` form of the command to disable uRPF mode on this system.

Note: The configuration is applied only after a reboot.

Command Syntax

```
ip urpf enable
no ip urpf enable
```

Parameter

None

Default

By default, uRPF mode on the system is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip urpf enable
% System Reboot is required for new URPF configurations to take effect

(config)#no ip urpf enable
% System Reboot is required for new URPF configurations to take effect
```

ip urpf allow-default

Use this command to enable default route check for uRPF mode.

Use `no` form of this command to disable default route check for uRPF mode.

Command Syntax

This command applies only to Qumran platforms.

```
ip urpf allow-default
no ip urpf allow-default
```

Parameter

None

Default

By default, uRPF mode on the system is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip urpf allow-default

(config)#no ip urpf allow-default
```


© 2021 IP Infusion Inc. Proprietary

ip vrf

This command creates a user-defined VRF (Virtual Routing and Forwarding) RIB (Routing Information Base), assigns a VRF identifier, and switches to VRF mode.

Use the `no` parameter with command to remove a VRF RIB.

Command Syntax

```
ip vrf WORD
no ip vrf WORD
```

Parameter

`WORD`	VRF identifier

Default

By default, no user-defined VRFs exist, only the default VRF.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf myVRF
(config-vrf)#
```

maximum-paths

Use this command to set the maximum number of paths to install in the FIB (Forwarding Information Base) for the ECMP (Equal-Cost MultiPath) feature.

Use the `no` parameter with this command to revert to default.

Note: If you change the number of paths from the default (8), you must save the running configuration and perform a reboot.

Command Syntax

```
maximum-paths <1-64>
no maximum-paths
```

Parameter

`<1-64>`	Maximum number of paths to install in the FIB

Default

By default, the maximum number of paths is 8.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#maximum-paths 5
```


© 2021 IP Infusion Inc. Proprietary

max-static-routes

Use this command to set the maximum number of static routes.

Use the `no` parameter to disable this command.

Command Syntax

```
max-static-routes <1-4294967294>
no max-static-routes
```

Parameters

`<1-4294967294>` Maximum number of static routes

Default

By default, max static routes value is 4294967294

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#max-static-routes 123

(config)#no max-static-routes
```

router-id

Use this command to add a router identifier for this system.

Use the `no` form of this command to disable this function.

Command Syntax

```
router-id A.B.C.D
no router-id (A.B.C.D)
```

Parameters

`A.B.C.D`	Router identifier in IP address format for this system.

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router-id 123.12.3.123
(config)#
```


© 2021 IP Infusion Inc. Proprietary

show debugging rib

Use this command to display debug settings.

Command Syntax

```
show debugging rib
```

Parameters

None

Command Mode

Privileged Exec Mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging rib
```

show ip rpf

Use this command to display reverse path forwarding (RPF) information for the specified source address.

Command Syntax

```
show ip rpf A.B.C.D
show ip rpf (vrf NAME|) A.B.C.D
```

Parameters

A.B.C.D	IP address of multicast source.
NAME	Virtual Routing and Forwarding name.

Default

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip rpf 10.10.10.50

RPF information for 10.10.10.50
  RPF interface: eth0
  RPF neighbor: 10.1.2.1
  RPF route: 0.0.0.0/0
  RPF type: unicast (kernel)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 0
  Metric: 0
#
```

Table 1-117 explains the output fields.

Table 1-117: show ip rpf output fields

Field	Description
RPF Interface	Name of the RPF interface.
RPF neighbor	Upstream RPF neighbor.
RPF route	Route table in which the logical interface address is located.
RPF type	Different type of RPF like multicast, unicast, MBGP, DVMRP, or static mroutes.

© 2021 IP Infusion Inc. Proprietary

Table 1-117: show ip rpf output fields

Field	Description
RPF recursion count	Number of times that the router lookups its routing table more than once to find out the immediate next-hop and exiting interface.
Distance	IP address of the remote side of the connection. Doing distance-preferred lookups across tables.
Metric	Metrics are informational units that can be measured and compared.

show ipv6 rpf

Use this command to display reverse path forwarding (RPF) information for the specified source address.

Command Syntax

```
show ipv6 rpf X:X::X:X
show ipv6 rpf (vrf NAME|) X:X::X:X
```

Parameters

`X:X::X:X`	IP address of multicast source.
`NAME`	Virtual Routing and Forwarding name.

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 rpf 10:10::10:50

RPF information for 10.10.10.50
  RPF interface: eth0
  RPF neighbor: 10.1.2.1
  RPF route: 0.0.0.0/0
  RPF type: unicast (kernel)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 0
  Metric: 0
#
```

Table 1-118 explains the output fields.

Table 1-118: show ipv6 rpf output fields

Field	Description
RPF Interface	Name of the RPF interface.
RPF neighbor	Upstream RPF neighbor.
RPF route	Route table in which the logical interface address is located.
RPF type	Different type of RPF like multicast, unicast, MBGP, DVMRP, or static mroutes.

© 2021 IP Infusion Inc. Proprietary

Table 1-118: show ipv6 rpf output fields

Field	Description
RPF recursion count	Number of times that the router lookups its routing table more than once to find out the immediate next-hop and exiting interface.
Distance	IPv6 address of the remote side of the connection. Doing distance-preferred lookups across tables.
Metric	Metrics are informational units that can be measured and compared.

show router-id

Use this command to display the Router ID of the current system.

Command Syntax

```
show router-id
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show router-id
Router ID: 10.55.0.2 (automatic)
```


© 2021 IP Infusion Inc. Proprietary

show running-config router

Use this command to display the running system router configuration.

Command Syntax

```
show running-config router bgp
show running-config router isis
show running-config router ldp
show running-config router ospf
show running-config router rip
show running-config router rsvp
show running-config router vrrp
```

Parameters

`bgp`	Display Border Gateway Protocol (BGP) information.
`isis`	Display Intermediate System to Intermediate System (IS-IS) information.
`ldp`	Display Label Distribution Protocol (LDP) information.
`ospf`	Display Open Shortest Path First (OSPF) information.
`rip`	Display Routing Information Protocol (RIP) information.
`rsvp`	Display Resource Reservation Protocol (RSVP) information.
`vrrp`	Display Virtual Router Redundancy Protocol (VRRP) information.

Default

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config router vrrp
!
router-id 3.3.3.3
!
```

show running-config router-id

Use this command to show the running system global router ID configuration.

Command Syntax

```
show running-config router-id
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config router-id
!
router-id 3.3.3.3
!
```


© 2021 IP Infusion Inc. Proprietary

show running-config urpf

Use this command to check uRPF status for this system.

Command Syntax

```
show running-config urpf
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config urpf
ip urpf enable

(config)#show running-config urpf
ip urpf enable
```

show running-config vrf

Use this command to show the running system status and configuration details for a specified VRF instance name.

Command Syntax

```
show running-config vrf WORD
```

Parameters

WORD	Virtual Routing and Forwarding name

Command Mode

Privileged exec mode, configure mode, router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config vrf xyz
!
ip vrf xyz
 description vrf
 router-id 11.11.11.11
```


© 2021 IP Infusion Inc. Proprietary

snmp restart rib

Use this command to restart SNMP in Routing Information Base (RIB)

Command Syntax

```
snmp restart rib
```

Parameters

None

Default

By default, snmp restart command is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#snmp restart rib
```

subscriber urpf enable

Use this command to enable uRPF for a subscriber interface.

Use the `no` form of this command to disable enable uRPF for a subscriber interface.

Note: The configuration is applied only after a reboot.

Command Syntax

```
subscriber urpf enable
```

Parameters

None

Default

By default, uRPF is disabled for a subscriber interface.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Examples

```
#config terminal
(config)#subscriber urpf enable
%% System Reboot is required for new URPF configurations to take effect
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Route-Map Commands

This chapter describes route-map commands.

- continue
- match as-path
- match community
- match extcommunity
- match interface
- match ip address
- match ip address prefix-list
- match ip next-hop
- match ip next-hop prefix-list
- match ip peer
- match ipv6 address
- match ipv6 address prefix-list
- match ipv6 next-hop
- match ipv6 next-hop prefix-list
- match ipv6 peer
- match metric
- match origin
- match route-type
- match tag
- route-map
- set aggregator
- set as-path
- set atomic-aggregate
- set comm-list
- set community
- set dampening
- set extcommunity
- set interface null0
- set ip next-hop
- set ipv6 next-hop
- set level
- set local-preference
- set metric
- set metric-type
- set origin

© 2021 IP Infusion Inc. Proprietary

- set originator-id
- set tag
- set vpnv4 next-hop
- set weight
- show route-map
- show running-config route-map

© 2021 IP Infusion Inc. Proprietary

continue

The continue clause provides the capability to execute additional entries in a route map after an entry is executed with a successful match and set clauses (i.e), the continue command allows multiple entries to be evaluated within a single route-map. Continue commands can be assigned optional sequence numbers that indicate the order in which clauses are to be evaluated.

Use the no form of the command (specifying a particular sequence number if desired), to remove individual or all continue clauses from a route-map.

Continue clause with match Clauses

When a match clause exists in a route map with continue clause, then the continue clause is executed only when a successful match occurs. If a match clause does not exist in the route-map and if a continue clause does exist, the continue clause will be evaluated and then go to the specified route-map entry. When a successful match occurs and we have a continue clause, the route-map executes the set clauses and then goes to the specified route-map entry. If continue clause does not exist in the next route map, then the route-map will behave normally. If a continue clause exists in the next route-map but a match is not successful, the route-map will not continue and will *fall through* to the next sequence number if one exists.

Continue clause with set Clauses

Set clauses are executed after the route-map evaluation is done. The set clauses are evaluated and executed in the order in which they were configured. Set clauses are only executed after a successful match occurs. The continue statement proceeds to the specified route-map entry only after configured set actions are performed. If a set action is configured in the first route-map and then the same set action occurs again, but with a different value in a subsequent route-map entry, then the last set action will override the previous set actions, which were configured with the same set command.

Command Syntax

```
continue <2-65535>|)
no continue <2-65535>|)
```

Parameter

<2-65535>	Continue sequence number.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#route-map Rmap1
(config-route-map)#continue ?
  <2-65535>  Route-map entry sequence number
  <cr>
(config-route-map)#continue 10
```

```
(config-route-map)#continue 30
```


© 2021 IP Infusion Inc. Proprietary

match as-path

Use this command to match an autonomous system path access list. This command specifies the autonomous system path to be matched. If there is a match for the specified AS path, and `permit` is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are `not` met then the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to remove a path list entry.

Command Syntax

```
match as-path WORD
no match as-path (WORD|)
```

Parameter

`WORD`	Autonomous system path access list name.

Default

Enabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map myroute deny 34
(config-route-map)#match as-path myaccesslist
```

match community

Use this command to specify the community to be matched.

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes. This command allows the matching based on community lists.

The values set by the `match community` command overrides the global values. The route that does not match at least one match clause is ignored.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to remove the community list entry.

Command Syntax

```
match community (<1-99>|<100-199>|WORD) (exact-match|)
no match community (<1-99>|<100-199>|WORD|) (exact-match|)
```

Parameters

`<1-99>`	Community-list number (standard).
`<100-199>`	Community-list number (expanded).
`WORD`	Community-list name.
`exact-match`	Do exact matching of communities.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match community mylist
```


© 2021 IP Infusion Inc. Proprietary

match extcommunity

Use this command to match BGP external community list

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes. This command allows the matching based on community lists.

The values set by this command overrides the global values. The route that does not match at least one match clause is ignored.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to remove the community list entry.

Command Syntax

```
match extcommunity (<1-99>|<100-199>|WORD) (exact-match|)
no match extcommunity (<1-99>|<100-199>|WORD|) (exact-match|)
```

Parameters

`<1-99>`	Community-list number (standard).
`<100-199>`	Community-list number (expanded).
`WORD`	Name of the community-list.
`exact-match`	Do exact matching of communities.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match extcommunity mylist
```

match interface

Use this command to define the interface match criterion. This command specifies the next-hop interface name of a route to be matched.

Use the `no` parameter with this command to remove the specified match criterion.

Command Syntax

```
match interface IFNAME
no match interface (IFNAME|)
```

Parameter

`IFNAME`	Interface name.

Default

By default, match interface is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map mymap1 permit 10
(config-route-map)#match interface eth0
```


© 2021 IP Infusion Inc. Proprietary

match ip address

Use this command to specify the match address of route. If there is a match for the specified IP address, and `permit` is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and `deny` is specified then the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the `no` parameter with this command to remove the `match ip address` entry.

Command Syntax

```
match ip address (<1-199>|<1300-2699>|WORD)
no match ip address (<1-199>|<1300-2699>|WORD|)
```

Parameters

`WORD`	IP access-list name.
`<1-199>`	IP access-list number (standard range).
`<1300-2699>`	IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match ip address List1
```

match ip address prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the `no` parameter with this command too disable this function

Command Syntax

```
match ip address prefix-list WORD
no match ip address prefix-list (WORD|)
```

Parameter

`WORD`	IP prefix list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ip address prefix-list mylist
```


© 2021 IP Infusion Inc. Proprietary

match ip next-hop

Use this command to specify a next-hop address to be matched in a route-map. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
match ip next-hop (<1-199>|<1300-2699>|WORD)
no match ip next-hop (<1-199>|<1300-2699>|WORD|)
```

Parameters

`WORD`	Specify the IP access-list name.
`<1-199>`	Specify the IP access-list number (standard range).
`<1300-2699>`	Specify the IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ip next-hop mylist
```

match ip next-hop prefix-list

Use this command to specify the next-hop IP address match criterion using the prefix-list. This command matches the next-hop IP address of a route.

Use the `no` parameter with this command to remove the specified match criterion.

Command Syntax

```
match ip next-hop prefix-list WORD
no match ip next-hop prefix-list (WORD|)
```

Parameter

`WORD`	Prefix-list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#match ip next-hop prefix-list list1
```


© 2021 IP Infusion Inc. Proprietary

match ip peer

Use this command to specify the match peer IPv4 address of a route.

Use the `no` parameter with this command to remove the specified match criterion.

Command Syntax

```
match ip peer (<1-199>|<1300-2699>|WORD)
no match ip peer (<1-199>|<1300-2699>|WORD|)
```

Parameter

`WORD`	IP access-list name.
`<1-199>`	IP access-list number (standard range).
`<1300-2699>`	IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#match ip peer 123

(config-route-map)#no match ip peer 123
```

match ipv6 address

Use this command to specify the match address of route. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the `no` parameter with this command to remove the `match ip address` entry.

Note: This command is valid for BGP, OSPFv3, and RIPng only.

Command Syntax

```
match ipv6 address WORD
no match ipv6 address (WORD|)
```

Parameter

`WORD`	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myRM deny 1
(config-route-map)#match ipv6 address myRM
```


© 2021 IP Infusion Inc. Proprietary

match ipv6 address prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP, OSPFv3, and RIPng only.

Use the `no` parameter with this command to disable this function

Command Syntax

```
match ipv6 address prefix-list WORD
no match ipv6 address prefix-list (WORD|)
```

Parameter

`WORD`	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ipv6 address prefix-list mylist
```

match ipv6 next-hop

Use this command to specify the next-hop address to be matched. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP and IS-IS only.

Use the `no` parameter with this command to disable this function

Command Syntax

```
match ipv6 next-hop (X:X::X:X|WORD)
no match ipv6 next-hop (X:X::X:X|WORD|)
```

Parameters

`X:X::X:X`	IPv6 address of the next-hop.
`WORD`	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ipv6 next-hop 3ffe::1
```


© 2021 IP Infusion Inc. Proprietary

match ipv6 next-hop prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP and IS-IS only.

Use the `no` parameter with this command to disable this function

Command Syntax

```
match ipv6 next-hop prefix-list WORD
no match ipv6 next-hop prefix-list WORD
```

Parameters

`WORD`	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ipv6 next-hop prefix-list new
```

match ipv6 peer

Use this command to specify the match peer IPv6 address of a route.

Use the `no` parameter with this command to remove the specified match criterion.

Command Syntax

```
match ipv6 peer (<1-199>|<1300-2699>|WORD)
no match ipv6 peer (<1-199>|<1300-2699>|WORD|)
```

Parameter

`WORD`	IP access-list name.
`<1-199>`	IP access-list number (standard range).
`<1300-2699>`	IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#match ipv6 peer 123

(config-route-map)#no match ipv6 peer 123
```


© 2021 IP Infusion Inc. Proprietary

match metric

Use this command to match a metric of a route. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP, OSPF, RIP, and IS-IS only.

Use the `no` parameter with this command to disable this function

Command Syntax

```
match metric <0-4294967295>
no match metric (<0-4294967295>|)
```

Parameters

`<0-4261412864>` Metric value.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match metric 888999
```

match origin

Use this command to match origin code. The origin attribute defines the origin of the path information. The `egp` parameter is indicated as an `e` in the routing table, and it indicates that the origin of the information is learned via EGP (Exterior Gateway Protocol). The `igp` parameter is indicated as an `i` in the routing table, and it indicates the origin of the path information is interior to the originating AS. The `incomplete` parameter is indicated as a `?` in the routing table, and indicates that the origin of the path information is unknown or learned through other means. If a static route is redistributed into BGP, the origin of the route is incomplete.

This command specifies the origin to be matched. If there is a match for the specified origin, and `permit` is specified when you created the route-map, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to disable this matching.

Command Syntax

```
match origin (egp|igp|incomplete)
no match origin (egp|igp|incomplete|)
```

Parameters

`egp`	Remote exterior gateway protocol.
`igp`	Local internal gateway protocol.
`incomplete`	Unknown heritage.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map myroute deny 34
(config-route-map)#match origin egp
```


© 2021 IP Infusion Inc. Proprietary

match route-type

Use this command to match an external route type. AS-external LSA is either Type-1 or Type-2. External type-1 matches only Type 1 external routes and external type-2 matches only Type 2 external routes.

Use the `no` parameter with this command to turn off the matching.

Command Syntax

```
match route-type external (type-1|type-2)
no match route-type external (type-1|type-2|)
```

Parameters

`type-1`	Match OSPF External Type 1 metric.
`type-2`	Match OSPF External Type 2 metric.

Default

By default, match route type external is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap1 permit 10
(config-route-map)#match route-type external type-1
```

match tag

Use this command to match the specified tag value.

Use the `no` parameter with this command to turn off the declaration.

Command Syntax

```
match tag <0-4294967295>
no match tag (<0-4294967295>|)
```

Parameters

`<0-4294967295>` Tag value.

Default

By default, match tag is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap1 permit 10
(config-route-map)#match tag 100
```


© 2021 IP Infusion Inc. Proprietary

route-map

Use this command to enter route-map mode and to permit or deny match/set operations.

This command controls and modifies routing information to allow redistribution of routes. It has a list of `match` and `set` commands associated with it. The `match` commands specify the conditions under which redistribution is allowed, and the `set` commands specify the particular redistribution actions to be performed if the criteria enforced by match commands are met. Route maps are used for detailed control over route distribution between routing processes.

Route maps also allow policy routing, and might route packets to a different route than the obvious shortest path.

Use the `no` parameter with this command to turn off the declaration.

Command Syntax

```
route-map WORD (deny|permit) <1-65535>
no route-map WORD ((deny|permit) <1-65535>|)
```

Parameters

`WORD`	Route-map name (maximum size 63 characters).
`deny`	Route map deny set operations. If this parameter is specified, and the match criteria are met, the route is not redistributed, and any other route maps with the same map tag are not examined.
`permit`	Route map permit set operations. If this parameter is specified, and the match criteria are met, the route is redistributed as specified by the set actions. If the `match` criteria are not met, the next route map with the same tag is tested.
`<1-65535>`	Sequence to insert into or delete from an existing route-map.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map route1 permit 1
(config-route-map)#
```

set aggregator

Use this command to set the AS number for the route map and router ID. An Autonomous System (AS) is a collection of networks under a common administration sharing a common routing strategy. It is subdivided by areas, and is assigned a unique 16-bit number. Use the `set aggregator` command to assign an AS number for the aggregator.

To use the `set aggregator` command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function

Command Syntax

```
set aggregator as <1-65535> A.B.C.D
no set aggregator as (<1-65535> A.B.C.D|)
```

Parameters

`<1-65535>`	AS number of aggregator.
`A.B.C.D`	IP address of aggregator.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#set aggregator as 43 10.10.0.3
```


© 2021 IP Infusion Inc. Proprietary

set as-path

Use this command to modify an autonomous system path for a route. By specifying the length of the AS-Path, the router influences the best path selection by a neighbor. Use this command to prepend an AS path string to routes increasing the AS path length.

To use this command, you must first give the `match` and `set` commands configure the conditions for redistributing routes from one routing protocol to another:

- The `match` command specifies the match criteria under which redistribution is allowed for the current route-map.
- The `set` command specifies the set redistribution actions to be performed if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set as-path prepend .<1-65535>
set as-path prepend .<1-4294967295>
no set as-path prepend (.<1-65535>|)
no set as-path prepend (.<1-4294967295>|)
```

Parameters

`<1-65535>`	OcNOS prepends this number to the AS path.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#set as-path prepend 8 24
```

set atomic-aggregate

Use this command to set an atomic aggregate attribute.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function

Command Syntax

```
set atomic-aggregate
```

```
no set atomic-aggregate
```

Parameters

No default value is specified

Default

None

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set atomic-aggregate
```


© 2021 IP Infusion Inc. Proprietary

set comm-list

Use this command to delete the matched communities from the community attribute of an inbound or outbound update when applying route-map.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
set comm-list (<1-99>|<100-199>|WORD) delete
no set comm-list (<1-99>|<100-199>|WORD) delete
```

Parameters

`<1-99>`	Standard community-list number.
`<100-199>`	Expanded community-list number.
`WORD`	Name of the community-list.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map myRM permit 3
(config-route-map)#set comm-list 34 delete
```

set community

Use this command to set the communities attribute. and group destinations in a certain community, as well as apply routing decisions according to those communities.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to delete the entry.

Command Syntax

```
set community [<65536-4294901759>|AA:NN|internet|local-AS|no-advertise|no-
  export|none] (additive|)
no set community [AA:NN|internet|local-AS|no-advertise|no-export|none] (additive|)
```

Parameters

`<65536-4294901759>`	Community number
`AA:NN`	The community number in aa:nn format.
`internet`	Internet.
`local-AS`	Do not send outside the local AS (well-known community).
`no-advertise`	Do not advertise this route to eBGP peers
`no-export`	Do not advertise this route to any peer.
`none`	Remove the community attribute from the prefixes that pass the route-map.
`additive`	Add to the existing community.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following examples show the use of the `set community` command with different parameters.

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set community no-export no-advertise

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set community no-advertise
```


© 2021 IP Infusion Inc. Proprietary

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set community 10:01 23:34 12:14 no-export
```

set dampening

Use this command to enable route-flap dampening and set parameters. Set the unreachability half-life time to be equal to, or greater than, reachability half-life time. The suppress-limit value must be greater than or equal to the reuse limit value.

Use the `no` parameter with this command to delete the entry.

Command Syntax

```
set dampening <1-45> <1-20000> <1-20000> <1-255> (<1-45>|)
no set dampening <1-45> <1-20000> <1-20000> <1-255> (<1-45>|)
```

Parameters

`<1-45>`	Reachability half-life time in minutes. The time for the penalty to decrease to one-half of its current value.
`<1-20000>`	Reuse-limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed.
`<1-20000>`	Suppress-limit value. When the penalty for a route exceeds the suppress value, the route is suppressed.
`<1-255>`	Max-suppress-time. Maximum time that a dampened route is suppressed.
`<1-45>`	Unreachability half-life time for penalty, in minutes.

Default

Default reachability half-life time: 15 minutes

Default reuse limit value: 750

Default suppress limit value: 2000

Default max-suppress value is 4 times the half-life time (60 minutes)

Default unreachability half-life time value: 15 minutes

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map R1 permit 24
(config-route-map)#set dampening 20 333 534 30
```


© 2021 IP Infusion Inc. Proprietary

set extcommunity

Use this command to set an extended community attribute.

To use this command you must first have a match clause. The `match` and `set` commands define the conditions for redistributing routes from one routing protocol to another:

- The `match` command defines the match criteria under which redistribution is allowed for the current route-map.
- The `set` command defines the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set extcommunity rt .AA:NN (additive|)
set extcommunity soo .AA:NN
set extcommunity cost (igp|pre-bestpath|) <0-255> <0-4294967295>
no set extcommunity rt (.AA:NN|) (additive|)
no set extcommunity soo (.AA:NN|)
no set extcommunity cost (igp|pre-bestpath|) <0-255> <0-4294967295>
```

Parameters

`rt`	Route target extended community.
`.AA:NN`	VPN extended community
`additive`	Add to the exsisting community.
`soo`	Site-of-origin extended community.
`cost`	Extended cost community.
`igp`	Compare following IGP cost comparison.
`pre-bestpath`	Compare following IGP cost comparison.
`<0-255>`	Community ID.
`<0-4294967295>`	Cost.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
```

```
(config)#route-map rmap1 permit 3
(config-route-map)#set extcommunity rt 06:01

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set extcommunity rt 0.0.0.6:01

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set extcommunity soo 06:01

#configure terminal
(config-route-map)#route-map rmap1 permit 3
(config-route-map)#set extcommunity soo 0.0.0.6:01
```


© 2021 IP Infusion Inc. Proprietary

set interface null0

Use this command to discard routes based on policy/rules configured for a route map.

Route maps can be applied to BGP neighbors. When this command is given for a route map and that route map is applied to a BGP neighbor, the discard route entries are added by BGP for the prefix permitted by the route map.

Use the `no` form of this command to not discard routes based on policy/rules configured for a route map.

Command Syntax

```
set interface null0
no set interface null0
```

Parameters

None

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

To discard 1.1.1.1/24 from BGP neighbor 30.1.1.1:

```
#configure terminal
(config)#ip prefix-list myPrefixList seq 5 permit 1.1.1.1/24 eq 24
(config)#route-map myRM permit 1
(config-route-map)#match ip address prefix-list myPrefixList
(config-route-map)#set interface null0
(config-route-map)#exit
(config)#router bgp 200
(config-router)#neighbor 30.1.1.1 remote-as 200
(config-router)#neighbor 30.1.1.1 route-map myRM in
```

set ip next-hop

Use this command to set the specified next-hop value.

Use the `no` parameter with this command to turn off the setting.

Note: This command is valid for BGP, OSPF, and RIP only.

Command Syntax

```
set ip next-hop A.B.C.D
no set ip next-hop (A.B.C.D|)
```

Parameter

`A.B.C.D`	IP address of the next-hop.

Default

By default, set ip next hop A.B.C.D is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#set ip next-hop 10.10.0.67
```


© 2021 IP Infusion Inc. Proprietary

set ipv6 next-hop

Use this command to set a next hop-address.

Use the `no` parameter with this command to delete an entry.

Note: This command is valid for BGP and OSPFv3 only.

Command Syntax

```
set ipv6 next-hop X:X::X:X
set ipv6 next-hop local X:X::X:X
no set ipv6 next-hop (X:X::X:X|)
no set ipv6 next-hop local (X:X::X:X|)
```

Parameters

`X:X::X:X`	Global IPv6 address of the nexthop.
`local`	Local IPv6 address of the nexthop.

Default

By default, set ipv6 next hop X:X::X:X is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set ipv6 next-hop local fe80::203:47ff:fe97:66dc
```

set level

Use this command to set the IS-IS level to export a route.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set level (level-1|level-2|level-1-2)
no set level (level-1|level-2|level-1-2|)
```

Parameters

`level-1`	Export into a level-1 area.
`level-2`	Export into a level-2 sub-domain.
`level-1-2`	Export into level-1 and level-2.

Default

By default, set level is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set level level-1
```


© 2021 IP Infusion Inc. Proprietary

set local-preference

Use this command to set the BGP local preference path attribute.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set local-preference <0-4294967295>
no set local-preference (<0-4294967295>|)
```

Parameters

`<0-4294967295>` Tag value for destination routing protocol.

Default

By default, set local preference is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set local-preference 12
```

set metric

Use this command to set a metric value for a route and influence external neighbors about the preferred path into an Autonomous System (AS). The preferred path is the one with a lower metric value. A router compares metrics for paths from neighbors in the same ASs. To compare metrics from neighbors coming from different ASs, use the `bgp always-compare-med` command.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set metric WORD
no set metric (WORD|)
```

Parameters

`WORD`	Metric value [+/-] <1-4294967295>

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set metric 600
```


© 2021 IP Infusion Inc. Proprietary

set metric-type

Use this command to set the metric type for the destination routing protocol. Select a type to be either Type-1 or Type-2 in the AS-external-LSA when the route-map matches the condition.

Note: This command is for OSPF, OSPFv3, or IS-IS only.

Use the `no` parameter with this command to return to the default.

Command Syntax

```
set metric-type (internal|external)
set metric-type (type-1|type-2)
no set metric-type (internal|external|)
no set metric-type (type-1|type-2|)
```

Parameters

`external`	IS-IS external metric type.
`internal`	IS-IS internal metric type.
`type-1`	OSPF external type 1 metric.
`type-2`	OSPF external type 2 metric

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In this example the metric type of the destination protocol is set to OSPF external Type 1.

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set metric-type 1
```

set origin

Use this command to set the BGP origin code. The origin attribute defines the origin of the path information.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to delete an entry.

Command Syntax

```
set origin (egp|igp|incomplete)
no set origin (egp|igp|incomplete|)
```

Parameters

`egp`	Learned through an Exterior Gateway Protocol.
`igp`	Interior to the originating AS. This happens when an Internal Gateway Protocol is redistributed into BGP.
`incomplete`	Unknown or learned through some other means. This happens when a static route is redistributed in BGP and the origin of the route is incomplete.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set origin egp
```


© 2021 IP Infusion Inc. Proprietary

set originator-id

Use this command to set the originator ID attribute.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function

Command Syntax

```
set originator-id A.B.C.D
no set originator-id (A.B.C.D|)
```

Parameter

`A.B.C.D`	IP address of originator.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set originator-id 1.1.1.1
```

set tag

Use this command to set a tag value. The parameter is the route tag that is labeled by another routing protocol (BGP or other IGP when redistributing), because AS-external-LSA has a route-tag field in its LSAs. In addition, when using route-map, OcNOS can tag the LSAs with the appropriate tag value. Sometimes the tag matches with using route-map, and sometimes, the value may be used by another application.

Use the `no` parameter with this command to unset a tag value.

Command Syntax

```
set tag <0-4294967295>
no set tag (<0-4294967295>|)
```

Parameter

`<0-4294967295>` Tag value for destination routing protocol.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example the tag value of the destination routing protocol is set to 6:

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set tag 6
```


© 2021 IP Infusion Inc. Proprietary

set vpnv4 next-hop

Use this command to set a VPNv4 next-hop address.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Note: This command is valid for BGP only.

Use the `no` parameter with this command to disable this function

Command Syntax

```
set vpnv4 next-hop A.B.C.D
no set vpnv4 next-hop (A.B.C.D|)
```

Parameter

`A.B.C.D`	IP address of originator.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set vpnv4 next-hop 6.6.6.6
```

set weight

Use this command to set weights for the routing table.

The weight value is used to assist in best path selection. It is assigned locally to a router. When there are several routes with a common destination, the routes with a higher weight value are preferred.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to delete an entry.

Command Syntax

```
set weight <0-4294967295>
no set weight (<0-4294967295>|)
```

Parameter

`<0-4294967295>` Weight value.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following configuration, all routes that apply to access-list 10 will have the weight set at 400. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match as-path 10
(config-route-map)#set weight 400
```


© 2021 IP Infusion Inc. Proprietary

show route-map

Use this command to display route-map information.

Command Syntax

```
show route-map (|WORD)
```

Parameters

WORD	Route-map name (maximum size 63 characters)

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show route-map` command.

```
#show route-map
route-map myRM, permit, sequence 1
  Match clauses:
    metric 200
  Set clauses:
    metric 60
#
```

Table 2-119 explains the output fields.

Table 2-119: show route-map details

Field	Description
route-map	Name of a route map.
permit	Routes that match the match clauses are redistributed according to the conditions defined by the set clauses.
sequence	Position of this route map in sequence of route-maps with the same name.
Match clauses	Routes that match the conditions defined by the match clause are redistributed according to the conditions defined by the set clauses.
Set clauses	Routes that pass the match clause are redistributed according to the conditions defined by the set clauses.

show running-config route-map

Use this command to display the running system status and configuration details for route-maps.

Command Syntax

```
show running-config route-map
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config route-map
!
route-map abc deny 2
 match community 2
!
route-map abc permit 3
 match route-type external type-2
 set metric-type type-1
!
```


© 2021 IP Infusion Inc. Proprietary

Open Shortest Path First Command Reference

Contents

This document contains these chapters and appendices:

- Chapter 1, *OSPFv2 Commands*
- Chapter 2, *OSPFv3 Commands*
- Chapter 3, *OSPF VPN Commands*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 OSPFv2 Commands

This chapter provides an alphabetized reference for each of the OSPFv2 commands. It includes the following commands:

- area authentication
- area default-cost
- area interface
- area interface authentication
- area interface network-type
- area interface passive
- area filter-list
- area nssa
- area range
-
- area shortcut
- area stub
- area virtual-link
- auto-cost reference bandwidth
- bfd all-interfaces
- capability cspf
- capability lls
- capability opaque
- capability restart
- capability traffic-engineering
- capability vrf-lite
- clear ip ospf
- compatible rfc1583
- debug ospf
- debug ospf database-timer rate-limit
- debug ospf events
- debug ospf ifsm
- debug ip ospf graceful-restart
- debug ip ospf lfa
- debug ip ospf redist
- debug ip ospf retransmission
- debug ospf lsa
- debug ospf nfsm
- debug ospf nsm
- debug ospf packet

© 2021 IP Infusion Inc. Proprietary

- debug ospf rib
- debug ospf route
- default-information originate
- default-metric
- distance
- distribute-list
- enable db-summary-opt
- fast-reroute keep-all-paths
- fast-reroute tie-break
- host area
- ip ospf authentication
- ip ospf authentication-key
- ip ospf bfd
- ip ospf cost
- ip ospf database-filter
- ip ospf dead-interval
- ip ospf disable
- ip ospf fast-reroute per-prefix candidate disable
- ip ospf flood-reduction
- ip ospf hello-interval
- ip ospf multi-area
- ip ospf message-digest-key
- ip ospf mtu
- ip ospf mtu-ignore
- ip ospf network
- ip ospf priority
- ip ospf retransmit-interval
- ip ospf transmit-delay
- log-adjacency-changes
- max-concurrent-dd
- maximum-area
- neighbor
- network
- ospf abr-type
- ospf area-interface-config-mode
- ospf flood-reduction
- ospf restart helper
- ospf router-id
- overflow database

© 2021 IP Infusion Inc. Proprietary

- overflow database external
- passive-interface
- redistribute
- restart ospf graceful
- router ospf
- show cspf rsvp forwarding-timer
- show debugging ospf
- show ip ospf
- show ip ospf border-routers
- show ip ospf database brief
- show ip ospf database detail
- show ip ospf igp-shortcut-lsp
- show ip ospf igp-shortcut-route
- show ip ospf interface
- show ip ospf multi-area-adjacencies
- show ip ospf neighbor
- show ip ospf route
- show ip ospf valid
- show ip ospf virtual-links
- show ip protocols
- show ip route fast-reroute
- shutdown
- snmp restart ospf
- summary-address
- timers lsa arrival
- timers spf exp
- timers throttle lsa

© 2021 IP Infusion Inc. Proprietary

area authentication

Use this command to enable authentication for an OSPF area. Specifying the area authentication sets the authentication to Type 1 authentication or simple text password authentication (details in RFC 2328). Setting up a Type 1 authentication configures a 64-bit field for that particular network. All packets sent on this network must have this configured value in their OSPF header. This allows only routers that have the same passwords to join the routing domain. Give all routers that are to communicate with each other through OSPF the same authentication password.

Use the ip ospf authentication-key command to specify a simple text password.

Use the ip ospf message-digest-key command to specify an MD5 password.

Use the `no` parameter to remove the authentication specification for an area.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) authentication
area (A.B.C.D|<0-4294967295>) authentication message-digest
no area (A.B.C.D|<0-4294967295>) authentication
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as 4-octet unsigned integer value.
`message-digest`	Enables MD5 authentication in the specified area ID.

Default

Null authentication

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 authentication message-digest

(config)#router ospf 100
(config-router)#no area 1 authentication
```


© 2021 IP Infusion Inc. Proprietary

area default-cost

Use this command to specify a cost for the default summary route sent into a stub or NSSA area. This command provides the metric for the summary default route, generated by the area border router, into the NSSA or stub area. Use this option only on an area border router that is attached to the NSSA or stub area. Refer to the RFC 3101 for information on NSSA.

Use the `no` form of this command to remove the assigned default-route cost.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) default-cost <0-16777215>
no area (A.B.C.D|<0-4294967295>) default-cost
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`default-cost`	Indicates the cost for the default summary route used for a stub or NSSA area.
`<0-16777215>`	Stub's advertised default summary cost. The default is 1.

Default

By default, route cost is 1

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example sets the default-cost to 10 for area 1.

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 default-cost 10

(config)#router ospf 100
(config-router)#no area 1 default-cost
```

area interface

Use this command to enable OSPF routing on the current interface.

Use no form of this command to disable OSPF routing on the current interface.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) interface IFNAME
no area (A.B.C.D|<0-4294967295>) interface IFNAME
```

Parameters

A.B.C.D	OSPF area ID as an IPv4 address.
<0-4294967295>	OSPF area ID as a decimal value.
IFNAME	Specify the interface name.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced in OcNOS-OTN version 4.2.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 interface xe1
```


© 2021 IP Infusion Inc. Proprietary

area interface authentication

Use this command to send and receive OSPF packets with the specified authentication method on the current interface.

Use no form of this command to stop sending and receiving OSPF packets with the specified authentication method on the current interface.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) interface IFNAME authentication (null|message-
  digest|)
no area (A.B.C.D|<0-4294967295>) interface IFNAME authentication
```

Parameters

`A.B.C.D`	OSPF area ID as an IPv4 address.
`<0-4294967295>`	OSPF area ID as a decimal value.
`IFNAME`	Specify the interface name.
`null`	Use no authentication.
`message-digest`	Use message digest authentication.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced in OcNOS-OTN version 4.2.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 interface xe1 authentication null
```

area interface network-type

Use this command to set the OSPF network type on the current interface.

Use no form of this command to unset the OSPF network type on the current interface.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) interface IFNAME network-type (broadcast|non-
  broadcast|point-to-multipoint (non-broadcast|)|point-to-point)
no area (A.B.C.D|<0-4294967295>) interface IFNAME network-type
```

Parameters

`A.B.C.D`	OSPF area ID as an IPv4 address.
`<0-4294967295>`	OSPF area ID as a decimal value.
`IFNAME`	Specify the interface name.
`broadcast`	Sets the network type to broadcast.
`non-broadcast`	Sets the network type to NBMA.
`point-to-multipoint`	Sets the network type to point-to-multipoint..
`non-broadcast`	Sets the network type to NBMA.
`point-to-point`	Sets the network type to point-to-point.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced in OcNOS-OTN version 4.2.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 interface xe1 network-type point-to-point
```


© 2021 IP Infusion Inc. Proprietary

area interface passive

Use this command to suppress sending hello packets on the current interface.

Use no form of this command to unsuppress sending Hello packets on the current interface.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) interface IFNAME passive
no area (A.B.C.D|<0-4294967295>) interface IFNAME passive
```

Parameters

A.B.C.D	OSPF area ID as an IPv4 address.
<0-4294967295>	OSPF area ID as a decimal value.
IFNAME	Specify the interface name.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced in OcNOS-OTN version 4.2.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 interface xe1 passive
```

area filter-list

Use this command to configure a filter to advertise summary routes on an Area Border Router (ABR).

This command suppresses incoming and outgoing summary routes between this area and other areas. You use this command in conjunction with the `prefix-list` and `access-list` commands.

Use the `no` form of this command to remove a filter.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) filter-list prefix WORD (in|out)
area (A.B.C.D|<0-4294967295>) filter-list access WORD (in|out)
no area (A.B.C.D|<0-4294967295>) filter-list prefix WORD
no area (A.B.C.D|<0-4294967295>) filter-list prefix WORD (in|out)
no area (A.B.C.D|<0-4294967295>) filter-list access WORD (in|out)
```

Parameters

`A.B.C.D`	OSPF area ID as an IPv4 address.
`<0-4294967295>`	OSPF area ID as a decimal value.
`prefix`	Use prefix list to filter summary.
`WORD`	Name of the prefix list.
`access`	Use access list to filter summary.
`WORD`	Name of the access list.
`in`	Filter routes from other areas into this area.
`out`	Filter routes from this area into other areas.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#access-list 1 deny 172.22.0.0
(config)#router ospf 100
(config-router)#area 1 filter-list access 1 in
```


© 2021 IP Infusion Inc. Proprietary

area nssa

Use this command to set an area as a Not-So-Stubby-Area (NSSA). There are no external routes in an OSPF stub area, so you cannot redistribute from another protocol into a stub area. An NSSA allows external routes to be flooded within the area. These routes are then leaked into other areas. However, the external routes from other areas still do not enter the NSSA. You can configure an area to be a stub area or an NSSA, but not both.

This command simplifies administration when connecting a central site using OSPF to a remote site that is using a different routing protocol. You can extend OSPF to cover the remote connection by defining the area between the central router and the remote router as a NSSA.

Use the `no` form of this command to remove this designation.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) nssa {translator-role (candidate|always)|
  stabilityinterval < 0-2147483647>|no-redistribution|default-information-originate
  (metric < 0-16777214>|metric-type <1-2>|metric <0-16777214> metric-type <1-
  2>|metric-type< 1-2> metric <0-16777214>|)|no-summary}

area (A.B.C.D|<0-4294967295>) nssa {translator-role (candidate|always|never)|
  stabilityinterval < 0-2147483647>|no-redistribution|default-information-originate
  (metric < 0-16777214>|metric-type <1-2>|metric <0-16777214> metric-type <1-
  2>|metric-type< 1-2> metric <0-16777214>|)|no-summary}

no area (A.B.C.D|<0-4294967295>) nssa

no area (A.B.C.D|<0-4294967295>) nssa {translator-role|stability-interval|no-
  redistribution |default-information-originate (route-map |) |no-summary}
```

Parameters

`A.B.C.D` OSPF Area ID in IPv4 address format.

`<0-4294967295>` OSPF Area ID as a decimal value.

`translator-role`

NSSA-ABR translator role

- `candidate` Translate NSSA-LSA to Type-5 LSA if router is elected.
- `never` Do not translate NSSA-LSA to Type-5 LSA.
- `always` Always translate NSSA-LSA to Type-5 LSA.

`stability-interval`

Stability timer for a NSSA area. If an elected translator determines its services are no longer required, it continues to perform its duties for this time interval. This minimizes excess flushing of translated Type-7 LSAs and provides a more stable translator transition.

- `<0-2147483647>`

  Stability interval in seconds.

`no-redistribution`

Do not redistribute into the NSSA.

`default-information-originate`

Originate Type-7 default LSA into the NSSA.

`metric`	Specify metric for default routes.
`<0-16777214>`	Specify metric value.
`metric-type`	Specify metric type (see RFC 3101).
`<1-2>`	Specify metric type: 1: Type 1 external route 2: Type 2 external route
`route-map`	OSPF default Route map reference.
`WORD`	Pointer to route-map entries.
`no-summary`	Do not inject inter-area routes into the NSSA.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router ospf 100
(config-router)#area 3 nssa translator-role candidate no-redistribution
default-information-originate metric 34 metric-type 2
```


© 2021 IP Infusion Inc. Proprietary

area range

Use this command to summarize OSPF routes at an area boundary. A single summary route is then advertised to other areas by the Area Border Routers (ABRs). Routing information is condensed at area boundaries and outside the area. If the network numbers in an area are assigned in a way such that they are contiguous, the ABRs can be configured to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D)
area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D) non-advertise
area (A.B.C.D|<0-4294967295>) range A.B.C.D A.B.C.D non-advertise
no area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D)
no area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D) not-advertise
```

Parameters

`A.B.C.D`	Area range prefix or length e.g. X.X.X.X/length
`A.B.C.D`	Area range prefix e.g. A.B.C.D
`<0-4294967295>`	OSPF Area ID as a decimal value.
`A.B.C.D/M`	The area range prefix and length.
`not-advertise`	Does not advertise this range.

Default

Range is advertised by default.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 range 192.16.0.0/24

(config)#router ospf 100
(config-router)#no area 1 range 192.16.0.0/24
```

area shortcut

Use this command to configure the short-cutting mode of an area. An area shortcut enables traffic to go through the non-backbone area with a lower metric whether or not an ABR router is attached to the backbone area.

Use the no form of this command to disable this function.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) shortcut (default|enable|disable)
no area (A.B.C.D|<0-4294967295>) shortcut
```

Parameters

A.B.C.D	OSPF Area ID in IPv4 address format.
<0-4294967295>	OSPF Area ID as a decimal value.
default	Sets default short-cutting behavior.
enable	Forces short-cutting through the area.
disable	Disables short-cutting through the area.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 shortcut default
(config)#router ospf 100
(config-router)#area 52 shortcut disable
(config)#router ospf 100
(config-router)#no area 42 shortcut
```


© 2021 IP Infusion Inc. Proprietary

area stub

Use this command to define an area as a stub area. There are two stub area router configuration commands: the `stub` and `default-cost` commands. In all routers attached to the stub area, configure the area by using the `stub` option of the area command. For an area border router (ABR) attached to the stub area, use the `area default-cost` command.

Use the `no-summary` parameter with this command to define a totally stubby area. Define an area as a totally stubby area when routers in the area do not need to learn about summary LSAs from other areas.

Use the `no` form of this command to disable this function.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) stub
area (A.B.C.D|<0-4294967295>) stub no-summary
no area (A.B.C.D|<0-4294967295>) stub
no area (A.B.C.D|<0-4294967295>) stub no-summary
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`no-summary`	Stops an ABR from sending summary link advertisements into the stub area.

Default

By default, no stub area is defined.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 stub no-summary
```

area virtual-link

Use this command to configure a link between two backbone areas that are physically separated through other non-backbone area.

In OSPF, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection. Configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these routers joined by a virtual link as if they were connected by an unnumbered point-to-point network.

Configure the hello-interval to be the same for all routers attached to a common network. A short hello-interval results in the router detecting topological changes faster but also an increase in the routing traffic. The retransmit-interval is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The transmit-delay is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet, are incremented by this amount. Set the transmit-delay to be greater than zero. Also, take into account the transmission and propagation delays for the interface. Include the transit area ID and the corresponding virtual link neighbor's router ID in each virtual link neighbor to properly configure a virtual link.

Use the `no` parameter with this command to remove a virtual link.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D authentication (message-
  digest|null|)
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D authentication-key LINE
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D message-digest-key <1-255> md5
  LINE
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {dead-interval <1-65535>|hello-
  interval <1-65535>|retransmit-interval <1-3600>|transmit-delay <1-3600>}
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D authentication
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D authentication-key
no message-digest-key <1-255>
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {dead-interval |hello-
  interval |retransmit-interval |transmit-delay }
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`A.B.C.D`	Specify IP address of the virtual link neighbor.
`authentication`	Enable authentication on this virtual link
`message-digest`	Cryptographic authentication.

© 2021 IP Infusion Inc. Proprietary

`null`	Null authentication.
`authentication-key`	
	Set authentication key.
`LINE`	Authentication key ID of 8 characters.
`message-digest-key`	
	Set message digest key.
`<1-255>`	Set message digest key.
`md5`	Specify the MD5 key.
`LINE`	MD5 key.
`dead-interval`	The interval during which no packets are received and after which the router acknowledges a neighboring router as off-line.
`<1-65535>`	The interval in seconds. The default is 40 seconds.
`hello-interval`	The interval the router waits before it sends a hello packet.
`<1-65535>`	The interval in seconds. The default is 10 seconds.
`retransmit-interval`	
	The interval the router waits before it retransmits a packet.
`<1-3600>`	The interval in seconds. The default is 5 seconds.
`transmit-delay`	The interval the router waits before it transmits a packet.
`<1-3600>`	The interval in seconds. The default is 1 second
`fall-over`	Specify fall-over detection.
`bfd`	Bidirectional Forwarding Detection (BFD)

Default

Default intervals:

Dead interval : 40 seconds

Hello interval: 10 seconds

Retransmit interval: 5 seconds

Transmit delay: 1 second

Command Mode

Router mode

OcNOS version 1.3

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 virtual-link 10.10.11.50 hello 5 dead 10
```

The below example shows the differences between with and without encrypted passwords.

0x - Already encrypted password

WORD - Authentication key (without encryption, ie doesn’t begin with 0x)

```
(config-router)#area 0.0.0.1 virtual-link 2.2.2.2 authentication
authentication-key 0x1234567891234567

(config-router)#area 0.0.0.1 virtual-link 2.2.2.2 authentication
authentication-key test
```


© 2021 IP Infusion Inc. Proprietary

auto-cost reference bandwidth

Use this command to control how OSPF calculates the default metric for the interface.

Use the `no` form of this command to assign cost based only on the interface bandwidth.

Command Syntax

```
auto-cost reference-bandwidth <1-4294967>
no auto-cost reference-bandwidth
```

Parameters

`<1-4294967>`	The reference bandwidth in Mbps per second. The default is 100 Mbps.

Default

By default, OSPF calculates the OSPF metric for an interface by dividing the reference bandwidth by the interface bandwidth. The default value for the reference bandwidth is 100Mbps. The auto-cost command is used to differentiate high bandwidth links. For multiple links with high bandwidth, specify a larger reference bandwidth value to differentiate cost on those links.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#auto-cost reference-bandwidth 50

(config)#router ospf 100
(config-router)#no auto-cost reference-bandwidth
```

bfd all-interfaces

Use this command to enable Bidirectional Forwarding Detection (BFD) on all interfaces.

Use the `no` form of this command to disable BFD.

Command Syntax

```
bfd all-interfaces
no bfd all-interfaces
```

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#bfd all-interfaces

(config)#router ospf 100
(config-router)#no bfd all-interfaces
```


© 2021 IP Infusion Inc. Proprietary

capability cspf

Use this command to enable the CSPF (Constrained Shortest Path First) feature for an OSPFv2 or OSPFv3 instance.

Use the `no` parameter with this command to disable CSPF functionality for the OSPFv2 or OSPFv3 instance.

Command Syntax

```
capability cspf
no capability cspf
```

Parameters

None

Default

By default, CSPF functionality for the OSPFv2 or OSPFv3 instance is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability cspf

(config)#router ospf 100
(config-router)#no capability cspf
```

capability lls

Use this command to enable link-local signaling feature on OSPF router.

Use no parameter to disable link-local signaling feature on OSPF router.

Command Syntax

```
capability lls
no capability lls
```

Parameters

None

Default

By default, capability lls is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability lls

(config-router)#no capability lls
```


© 2021 IP Infusion Inc. Proprietary

capability opaque

Use this command to enable opaque-LSAs which are Type 9, 10 and 11 LSAs that deliver information used by external applications.

Use the `no` form of this command to disable the feature.

Command Syntax

```
capability opaque
```

```
no capability opaque
```

Parameters

None

Default

By default, opaque-LSA is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability opaque

(config)#router ospf 100
(config-router)#no capability opaque
```

capability restart

Use this command to enable OSPF graceful restart or restart signaling. If a router is not restart-enabled, it cannot enter graceful restart mode and act as a helper.

Use the `no` parameter with this command to disable the features.

Command Syntax

```
capability restart graceful
no capability restart graceful
```

Parameters

`graceful`	Specify enabling OSPF graceful restart feature.

Default

By default, OSPF graceful restart or restart signaling is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability restart graceful

(config)#router ospf 100
(config-router)#no capability restart graceful
```


© 2021 IP Infusion Inc. Proprietary

capability traffic-engineering

Use this command to enable traffic engineering feature on OSPF router.

Use `no` parameter to disable traffic engineering feature on OSPF router.

Command Syntax

```
capability traffic-engineering
no capability traffic-engineering
```

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf
(config-router)#capability traffic-engineering

(config-router)#no capability traffic-engineering
```

capability vrf-lite

Use this command to apply multi-VRF capability to OSPF process or to decouple the PE router from the VPN backbone.

Use `no` parameter to deny multi-VRF capability to OSPF process or to avoid decoupling the PE router from the VPN backbone.

Command Syntax

```
capability vrf-lite
```

```
no capability vrf-lite
```

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf
(config-router)#capability vrf-lite

(config-router)#no capability vrf-lite
```


© 2021 IP Infusion Inc. Proprietary

clear ip ospf

Use this command to clear and restart all OSPF routing processes or a given OSPF routing process.

Command Syntax

```
clear ip ospf (<0-65535>|) process
```

Parameter

<0-65535>	Specify the process ID.

Command Mode

Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip ospf process
#clear ip ospf 555 process
```

compatible rfc1583

Use this command to restore the method used to calculate summary route costs per RFC.

RFC 1583 specified a method for calculating the metrics for summary routes based on the minimum metric of the component paths available. RFC 2328 specifies a method for calculating metrics based on maximum cost. With this change, it is possible that all of the ABRs in an area might not be upgraded to the new code at the same time. This command addresses this issue and allows the selective disabling of RFC 2328 compatibility.

Use the `no` parameter with this command to disable RFC 1583 compatibility.

Command Syntax

```
compatible rfc1583
```

```
no compatible rfc1583
```

Parameters

None

Default

By default, OSPF is RFC 2328 compatible

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#compatible rfc1583

(config)#router ospf 100
(config-router)#no compatible rfc1583
```


© 2021 IP Infusion Inc. Proprietary

debug ospf

Use this command to specify debugging options for OSPF.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ospf (all|bfd|database-timer|events|ifsm|lsa|nfsm|nsm| packet|route|sr|)
debug ospf rib ({interface|redistribute}|)
no debug ospf (all|bfd|database-timer|events|ifsm|lsa|nfsm|nsm| packet|route|sr|)
undebug ospf (all|bfd|database-timer|events|ifsm|lsa|nfsm|nsm| packet|route|)
no debug all ospf
undebug all ospf
no debug all
no debug ospf rib ({interface|redistribute}|)
undebug all
```

Parameters

`all`	Enable or disable debugging for `ifsm`, `nsfm`, `lsa`, `nsm`, `events`, and `route`.
`bfd`	Debug Bidirectional Forwarding Detection (BFD)
`database-timer`	Debug OSPF rate-limiting values for LSA throttling (see debug ospf database-timer rate-limit)
`events`	Debug OSPF events information (see debug ospf events)
`ifsm`	Debug OSPF Interface State Machine (see debug ospf ifsm)
`lsa`	Debug OSPF Link State Advertisement (see debug ospf lsa)
`nfsm`	Debug OSPF Neighbor State Machine (see debug ospf nfsm)
`nsm`	Debug OSPF NSM information (see debug ospf nsm)
`packet`	Debug OSPF packets (see debug ospf packet)
`route`	Debug OSPF route information (see debug ospf route)
`rib`	Debug OSPF RIB information
`sr`	Debug OSPF segment routing information
`interface`	Debug OSPF RIB interface
`redistribute`	Debug OSPF RIB redistribute

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ospf all

#debug ospf bfd
#no debug ospf bfd
```


© 2021 IP Infusion Inc. Proprietary

debug ospf database-timer rate-limit

Use this command to log when link-state advertisement (LSA) rate-limiting timers will expire. These messages are logged only when debug ospf lsa `generate` or debug ospf lsa `refresh` is enabled

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ospf database-timer rate-limit


no debug ospf database-timer rate-limit
undebug ospf database-timer rate-limit
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ospf database-timer rate-limit

#undebug ospf database-timer rate-limit
```

debug ospf events

Use this command to specify debugging options for OSPF event troubleshooting. Use this command without parameters to turn on all the options.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ospf events ({abr|asbr|lsa|nssa|os|router|vlink}|)


no debug ospf events ({abr|asbr|lsa|nssa|os|router|vlink}|)
undebug ospf events ({abr|asbr|lsa|nssa|os|router|vlink}|)
```

Parameters

`abr`	Debug OSPF ABR events.
`asbr`	Debug ASBR events.
`lsa`	Debug LSA events.
`nssa`	Debug NSSA events.
`os`	Debug OS interaction events.
`router`	Debug other router events.
`vlink`	Debug virtual link events.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#no debug ospf event abr
#debug ospf event asbr
#debug ospf event lsa
#no debug ospf event nssa
#debug ospf event os
#debug ospf event router
#debug ospf event vl
```


© 2021 IP Infusion Inc. Proprietary

debug ospf ifsm

Use this command to specify debugging options for OSPF Interface Finite State Machine (IFSM) troubleshooting.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ospf ifsm ({events|status|timers}|)

no debug ospf ifsm ({events|status|timers}|)
undebug ospf ifsm ({events|status|timers}|)
```

Parameters

`events`	Debug IFSM event information
`status`	Debug IFSM status information
`timers`	Debug IFSM timer information

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#no debug ospf ifsm events
#debug ospf ifsm status
#debug ospf ifsm timers
```

debug ip ospf graceful-restart

Use this command to specify debugging option for OSPF graceful restart.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ip ospf graceful-restart (detail|terse|)
no debug ip ospf graceful-restart (detail|terse|)
```

Parameters

`detail`	Debug OSPF graceful restart detail information
`terse`	Debug OSPF graceful restart summary information

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ip ospf graceful-restart detail
```


© 2021 IP Infusion Inc. Proprietary

debug ip ospf lfa

Use this command to specify the debugging options for OSPFv2 Loop-free Alternate path

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ip ospf lfa
no debug ip ospf lfa
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ip ospf lfa
```

debug ip ospf redist

Use this command to display debugging option for OSPF redistribute information

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ip ospf redist (detail|terse|)
no debug ip ospf redist (detail|terse|)
```

Parameters

`detail`	Debug OSPF redistribute detail information
`terse`	Debug OSPF redistribute summary information

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ip ospf redistribute detail
```


© 2021 IP Infusion Inc. Proprietary

debug ip ospf retransmission

Use this command to display debug logs of OSPF retransmission information.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ip ospf retransmission
no debug ip ospf retransmission
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ip ospf retransmission
```

debug ospf lsa

Use this command to specify debugging options for OSPF Link State Advertisements (LSA) troubleshooting.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ospf lsa ({flooding|generate|install|maxage|refresh}|)

no debug ospf lsa ({flooding|generate|install|maxage|refresh}|)
undebug ospf lsa ({flooding|generate|install|maxage|refresh}|)
```

Parameters

`flooding`	Debug LSA flooding.
`generate`	Debug LSA generation.
`install`	Debug LSA installation.
`maxage`	Debug the maximum age processing.
`refresh`	Debug LSA refresh.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#no debug ospf lsa refresh
#debug ospf lsa flooding
#debug ospf lsa install
#debug ospf lsa maxage
#debug ospf lsa generate
```


© 2021 IP Infusion Inc. Proprietary

debug ospf nfsm

Use this command to specify debugging options for OSPF Neighbor Finite State Machines (NFSMs).

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ospf nfsm ({events|status|timers}|)

no debug ospf nfsm ({events|status|timers}|)
undebug ospf nfsm ({events|status|timers}|)
```

Parameters

`events`	Debug NFSM event information
`status`	Debug NFSM status information
`timers`	Debug NFSM timer information

Command Mode

Privileged Exec mode Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ospf nfsm events
#no debug ospf nfsm timers
```

debug ospf nsm

Use this command to specify debugging options for OSPF NSM information.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ospf nsm ({interface|redistribute}|)

no debug ospf nsm ({interface|redistribute}|)
undebug ospf nsm ({interface|redistribute}|)
```

Parameters

`interface`	Debug NSM interface information.
`redistribute`	Debug NSM redistribute information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The `debug ospf nsm` command enables the display of debug information related to NSM.

```
#debug ospf nsm interface
#no debug ospf nsm redistribute
```


© 2021 IP Infusion Inc. Proprietary

debug ospf packet

Use this command to specify debugging options for OSPF packets.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)

no debug ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)
undebug ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)
```

Parameters

`hello`	Debug OSPF hello packets.
`dd`	Debug OSPF database.
`ls-request`	Debug OSPF link state requests.
`ls-update`	Debug OSPF link state updates.
`ls-ack`	Debug OSPF link state acknowledgments.
`send`	Debug OSPF sent packets.
`recv`	Debug OSPF received packets.
`detail`	Debug OSPF detailed information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ospf packet detail
#debug ospf packet dd send detail
#no debug ospf packet ls-request recv detail
```

debug ospf rib

Use this command to display debug information about the interaction between the OSPF process and the Routing Information Base (RIB).

Use `no` parameter of this command to disable debugging output.

Command Syntax

```
debug ospf rib ({interface|redistribute}|)
no debug ospf rib ({interface|redistribute}|)
debug ip ospf ({client|redistribute}|)
no debug ip ospf ({client|redistribute}|)
undebug ospf rib ({interface|redistribute}|)
```

Parameters

`interface`	Debug RIB interface information.
`redistribute`	Debug RIB redistribute information.
`client`	Debug RIB client information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ospf rib interface
#no debug ospf rib redistribute
```


© 2021 IP Infusion Inc. Proprietary

debug ospf route

Use this command to debug route calculation. Use this command without parameters to turn on all the options.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ospf route ({ase|ia|install|spf}|)
no debug ospf route ({ase|ia|install|spf}|)
undebug ospf route ({ase|ia|install|spf}|)
```

Parameters

`ase`	Debug OSPF external route calculation.
`ia`	Debug OSPF Inter-Area route calculation.
`install`	Debug OSPF route installation.
`spf`	Debug OSPF SPF calculation.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ospf route
#no debug ospf route ia
#debug ospf route install
```

default-information originate

Use this command to create a default external route into an OSPF routing domain.

Use the `no` parameter with this command to disable this feature.

The system acts like an Autonomous System Boundary Router (ASBR) when you use the `default-information originate` command to redistribute routes into an OSPF routing domain. An ASBR does not by default generate a default route into the OSPF routing domain.

When you give the `default-information originate` command, also specify a `route-map` to avoid a dependency on the default network in the routing table.

Command Syntax

```
default-information originate
default-information originate {metric <0-16777214>|metric-type (1|2)|?route-map
  WORD|always}
no default-information originate
no default-information originate {metric|metric-type|?route-map|always}
```

Parameters

`always`	Used to advertise the default route regardless of whether there is a default route.
`metric`	Sets the OSPF metric used in creating the default route.
`<0-16777214>`	Sets the OSPF metric used in creating the default route. The default metric value is 10. The value used is specific to the protocol.
`metric-type`	The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).
`1`	Sets OSPF External Type 1 metric.
`2`	Sets OSPF External Type 2 metric (default).
`route-map`	Route map.
`WORD`	Specify the name of route map.

Default

Sets the OSPF metric used in creating the default route. The default metric value is 10.

The value used is specific to the protocol. metric-type The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).

By default, 2 Sets OSPF External Type 2 metric.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

© 2021 IP Infusion Inc. Proprietary

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#default-information originate always metric 23 metric-type 2
route-map myinfo

(config)#router ospf 100
(config-router)#no default-information originate metric metric-type route-map
```

default-metric

Use this command to set a default metric for OSPF.

A default metric facilitates redistributing routes with incompatible metrics. If the metrics do not convert, the default metric provides an alternative. Use this command to use the same metric value for all redistributed routes. Use this command in conjunction with the redistribute command.

Use the `no` parameter with this command to return to the default state.

Command Syntax

```
default-metric <1-16777214>
no default-metric
```

Parameters

`<1-16777214>`	Default metric value.

Default

Built-in, automatic metric translations, as appropriate for each routing protocol.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#default-metric 100
```


© 2021 IP Infusion Inc. Proprietary

distance

Use this command to set OSPF administrative distances.

The administrative distance rates the trustworthiness of a routing information source. A higher distance value means a lower trust rating. For example, an administrative distance of 255 means that the routing information source cannot be trusted and should be ignored.

Use the `no` form of this command to restore the default value (110).

Command Syntax

```
distance <1-255>
distance <1-255> A.B.C.D/M (WORD|)
distance ospf {intra-area <1-255>|inter-area <1-255>|external <1-255>}
no distance <1-255>
no distance <1-255> A.B.C.D/M (WORD|)
no distance ospf {intra-area |inter-area |external}
```

Parameters

`<1-255>`	Used alone, this parameter specifies a default administrative distance used when no other specification exists for a routing information source.
`intra-area`	Routes within an area.
`<1-255>`	Distance for all routes within an area
`inter-area`	Routes from one area to another area.
`<1-255>`	Distance for all routes from one area to another area.
`external`	Routes from other routing domains learned by redistribution.
`<1-255>`	Distance for routes from other routing domains learned by redistribution.
`A.B.C.D/M`	Distance for routes to prefixes whose nexthop matches this address.
`WORD`	Name of access list to apply to route updates.

Default

By default, distance for each type of route (intra-, inter-, or external) is 110

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#distance ospf inter-area 20 intra-area 10 external 40
```

distribute-list

Use this command to filter networks in routing updates. This command redistributes other routing protocols into the OSPF routing table.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
distribute-list WORD out (kernel|connected|static|rip|bgp|isis|ospf (<0-65535>|))
distribute-list WORD in
no distribute-list WORD out (kernel|connected|static|rip|bgp|isis|ospf (<0-
  65535>|))
no distribute-list WORD in
```

Parameters

`WORD`	Specify the name of the access list.
`in`	Filter incoming routing updates.
`out`	Filter outgoing routing updates.
`kernel`	Specify kernel routes.
`connected`	Specify connected routes.
`static`	Specify static routes.
`rip`	Specify RIP routes.
`bgp`	Specify BGP routes.
`isis`	Specify IS-IS routes.
`ospf`	Specify OSPF process.
`<0-65535>`	Specify OSPF process ID <1-65535>. If not specified, this command redistribute OSPF instance with process ID 0.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the distribution of BGP routing updates based on the access list `list1` (network 172.10.0.0).

```
#configure terminal
(config)#access-list list1 permit 172.10.0.0
(config)#router ospf 100
(config-router)#distribute-list list1 out bgp
```


© 2021 IP Infusion Inc. Proprietary

```
(config-router)#redistribute bgp
```

enable db-summary-opt

Use this command to enable the database summary list optimization for OSPFv2.

When this feature is enabled, the database exchange process is optimized by removing the LSA from the database summary list for the neighbor, if the LSA instance in database summary list is the same as or less recent than the listed LSA in the database description packet received from the neighbor.

Use the `no` form of this command to disable database summary list optimization.

Command Syntax

```
enable db-summary-opt
```

```
no enable db-summary-opt
```

Parameters

None

Default

By default, database summary list optimization for OSPFv2 is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf
(config-router)#enable db-summary-opt
(config-router)#no enable db-summary-opt
```


© 2021 IP Infusion Inc. Proprietary

fast-reroute keep-all-paths

Use this command to enable fast rerouting on all OSPF interfaces.

Use the `no` parameter with this command to disable fast rerouting.

Command Syntax

```
fast-reroute keep-all-paths
no fast-reroute keep-all-paths
```

Parameters

None

Defaults

By default, fast rerouting is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 200
(config-router)#fast-reroute keep-all-paths
```

fast-reroute tie-break

Use this command to set the tie-breaking policy for selecting a fast reroute repair path. You assign a priority to each type of repair path.

Use the `no` parameter with this command to set the tie-breaking policy for a specific type of repair path to its default priority. To set all types of repair paths to their default priorities, do not specify a repair path with the `no` form of this command.

Command Syntax

```
fast-reroute tie-break (primary-path|interface-disjoint|node-protecting|broadcast-
  interface-disjoint) index <1-10>
no fast-reroute tie-break
no fast-reroute tie-break (primary-path|interface-disjoint|node-
  protecting|broadcast-interface-disjoint) index <1-10>
```

Parameters

`primary-path` Use a path from the Equal-Cost Multipath Path (ECMP) set. An ECMP found during the primary shortest path first (SPF) repair might not be desirable in networks where traffic exceeds the capacity of any single link.

`interface-disjoint`

Do not select point-to-point interfaces that have no alternate next hop for rerouting if the primary gateway fails, thus protecting the interface.

`node-protecting`

Bypass the `primary-path` gateway router which might not protect the router that is the next hop in the primary path.

`broadcast-interface-disjoint`

Do not use the interface if connected to a broadcast network. Repair paths protect links when a repair path and a protected primary path use *different* next-hop interfaces. However, on broadcast interfaces, if the repair path is computed via the same interface as the primary path, but their next-hop gateways are different, the router is protected but the link might not be.

`index` Tie break priority. A lower value has higher preference.

`<1-10>` Range of priority values.

Defaults

By default, LFA backup path is calculated based on interface-disjoint.

The default priority scheme is:

1. primary-path
2. interface-disjoint
3. node-protecting
4. broadcast-interface-disjoint

© 2021 IP Infusion Inc. Proprietary

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 200
(config-router)#fast-reroute tie-break interface-disjoint index 1
```

host area

Use this command to configure a stub host entry belonging to a particular area.

Using this command, you can advertise specific host routes in the router-LSA as stub link. Since stub host belongs to the specified router, specifying cost is not important.

Use the `no` form of this command to remove the host area configuration.

Command Syntax

```
host A.B.C.D area (A.B.C.D|<0-4294967295>)
host A.B.C.D area (A.B.C.D|<0-4294967295>) cost <0-65535>
no host A.B.C.D area (A.B.C.D|<0-4294967295>)
no host A.B.C.D area (A.B.C.D|<0-4294967295>) cost
```

Parameters

`A.B.C.D`	Specify IP address of the host.
`area`	Set the OSPF area ID
`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`cost`	Specify cost for stub host entry.
`<0-65535>`	Specify cost for stub host entry.

Default

No host entry is configured

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#host 172.16.10.100 area 1
(config-router)#host 172.16.10.101 area 2 cost 10
```


© 2021 IP Infusion Inc. Proprietary

ip ospf authentication

Use this command to send and receive OSPF packets with the specified authentication method on the current interface.

Use the `no` parameter with this command to disable the authentication.

Command Syntax

```
ip ospf authentication (null|message-digest|)
ip ospf A.B.C.D authentication (null|message-digest|)
no ip ospf (A.B.C.D|) authentication
```

Parameters

`A.B.C.D`	The IP address of the interface.
`null`	Use no authentication.
`message-digest`	Use message digest authentication.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In this example, interface `eth0` is configured to have no authentication. This will override any `text` or `MD5` authentication configured on this interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf authentication null
```

ip ospf authentication-key

Use this command to specify an OSPF authentication password for neighboring routers.

This command creates a password (key) that is inserted into the OSPF header when OcNOS originates packets. Assign a separate password to each network for different interfaces. All neighboring routers on the same network with the same password exchange OSPF routing data.

The key can be used only when authentication is enabled for an area with the `area authentication` command.

Simple password authentication allows a password to be configured for each area. Configure the routers in the same routing domain with the same password.

Use the `no` parameter with this command to remove an OSPF authentication password.

Command Syntax

```
ip ospf (A.B.C.D|) authentication-key WORD
no ip ospf (A.B.C.D|) authentication-key
```

Parameters

`A.B.C.D`	The IP address of the interface.
`authentication-key`	Specify the authentication password.
`WORD`	Specify the OSPF Encrypted password (key) of 8 bytes.

Default

By default, no password used when exchanging OSPF routing data

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, an authentication key `test` is created on interface `eth0` in area `0`. Note that first authentication is enabled for area `0`.

```
#configure terminal
(config)#router ospf 100
(config-router)#network 10.10.10.0/24 area 0
(config-router)#area 0 authentication
(config-router)#exit
(config)#interface eth0
(config-if)#ip ospf 3.3.3.3 authentication-key test

OcNOS#sh run int xe1
!
interface xe1
ip ospf authentication
ip ospf authentication-key 0x94eebee8c349a4b0
```

 © 2021 IP Infusion Inc. Proprietary

```
!
(config)#int xe1
(config-if)#ip ospf authentication-key 0x94eebee8c349a4b0 -
```
encrypted password of 16 characters which can be obtained from sh run <int>

ip ospf bfd

Use this command to enable Bidirectional Forwarding Detection (BFD).

Use this command with either the `no` or `disable` parameter to disable BFD.

Command Syntax

```
ip ospf bfd (disable|)
no ip ospf bfd (disable|)
```

Parameters

`disable`	Specify to disable BFD.

Default

By default, ip ospf bfd is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf bfd
```


© 2021 IP Infusion Inc. Proprietary

ip ospf cost

Use this command to explicitly specify the cost of the link-state metric in a router-LSA.

The interface cost indicates the overhead required to send packets across an interface. This cost is stated in the Router-LSA's link. The cost is inversely proportional to the bandwidth of an interface. By default, the cost of an interface is calculated based on the bandwidth (10^8/ bandwidth). Use this command to set the cost manually.

Use the `no` parameter with this command to reset the cost to its default value.

Command Syntax

```
ip ospf (A.B.C.D|) cost <1-65535>
no ip ospf (A.B.C.D|) cost
```

Parameters

`A.B.C.D`	The IP address of the interface.
`<1-65535>`	Specify the link-state metric.

Default

By default, the cost of an interface is calculated based on the bandwidth (10^8/ bandwidth). The default cost value is 10.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the cost as 10 on interface `eth0` for IP address 10.10.10.50.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf 10.10.10.50 cost 10
```

ip ospf database-filter

Use this command to turn on the LSA database-filter for a particular interface.

OSPF floods new LSAs over all interfaces in an area, except the interface on which the LSA arrives. This redundancy ensures robust flooding. However, too much redundancy can waste bandwidth and might lead to excessive link and CPU usage in certain topologies, resulting in destabilizing the network. To avoid this, use this command to block flooding of LSAs over specified interfaces.

Use the `no` parameter with this command to turn off the filter.

Command Syntax

```
ip ospf (A.B.C.D|) database-filter all out
no ip ospf (A.B.C.D|) database-filter
```

Parameters

`A.B.C.D`	The IP address of the interface.

Default

Disabled, all outgoing LSAs are flooded to the interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf database-filter all out
```


© 2021 IP Infusion Inc. Proprietary

ip ospf dead-interval

Use this command to set the interval during which the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down. This value is advertised in the router's hello packets. It must be a multiple of hello-interval and be the same for all routers on a specific network.

Use the `no` parameter with this command to return to the default time. If you have configured this command specifying the IP address of the interface and want to remove the configuration, use the `no` parameter with the specified IP address (`no ip ospf dead-interval A.B.C.D`).

Command Syntax

```
ip ospf (A.B.C.D|) dead-interval <1-65535>
no ip ospf (A.B.C.D|) dead-interval
```

Parameters

`A.B.C.D`	The IP address of the interface.
`dead-interval`	Specify the interval.
`<1-65535>`	Specify the interval in seconds.

Default

By default, dead interval is 40 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows configuring dead-interval for 10 seconds on eth0 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf dead-interval 10
```

ip ospf disable

Use this command to completely disable OSPF packet processing on an interface.

This command overrides the network command.

Use the `no` option with this command to return to the default setting.

Command Syntax

```
ip ospf disable all
no ip ospf disable all
```

Parameters

None

Default

By default, this feature is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf disable all
```


© 2021 IP Infusion Inc. Proprietary

ip ospf fast-reroute per-prefix candidate disable

Use this command to prohibit the interface from being used as the next hop in a repair path.

Use the `no` option with this command to use the interface as the next hop in a repair path.

Command Syntax

```
ip ospf fast-reroute per-prefix candidate disable
no ip ospf fast-reroute per-prefix candidate disable
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf fast-reroute per-prefix candidate disable
```

ip ospf flood-reduction

Use this command to enable flood reduction on an interface. When this command is configured, an LSA sent out on the interface is set with the DNA bit in the LSA age field. The LSA is not refreshed every refresh interval if there is no change in LSA. Only changed LSAs are sent out on the interface

Use the `no` option with this command to disable flood reduction on an interface.

Command Syntax

```
ip ospf flood-reduction
```

```
no ip ospf flood-reduction
```

Parameters

None

Default

By default, flood reduction on an interface is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip ospf flood-reduction

(config-if)#no ip ospf flood-reduction
```


© 2021 IP Infusion Inc. Proprietary

ip ospf hello-interval

Use this command to specify the interval between hello packets.

The hello-interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter hello interval ensures faster detection of topological changes but results in more routing traffic.

Use the `no` parameter with this command to return to the default time.

Command Syntax

```
ip ospf (A.B.C.D|) hello-interval <1-65535>
no ip ospf (A.B.C.D|) hello-interval
```

Parameters

`A.B.C.D`	The IP address of the interface.
`hello-interval`	Specify the interval.
`<1-65535>`	Specify the interval in seconds.

Default

By default, hello interval is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the hello-interval for 3 seconds on interface eth0.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf hello-interval 3
```

ip ospf multi-area

Use this command to enable multi-area adjacency on point-to-point network and other network types. Multi-area adjacency establishes adjacency between the Area Border Routers (ABRs). The interface of the ABR where this command is configured, shall be associated with multiple areas.

Use the `no` parameter to disable multi-area adjacency on the given interface on point-to-point network.

Command Syntax

```
ip ospf <0-65535> multi-area (A.B.C.D|<0-4294967295>)(neighbor A.B.C.D |)
no ip ospf <0-65535> multi-area (A.B.C.D|<0-4294967295>)
no ip ospf <0-65535> multi-area (A.B.C.D|<0-4294967295>) neighbor
```

Parameters

`<0-65535>`	OSPF process ID.
`A.B.C.D`	OSPF area ID in IP address format.
`<0-4294967295>`	OSPF area ID as a decimal value.
`A.B.C.D`	Neighbor IP address.

Default

By default, multi-area adjacency is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ip ospf 0 multi-area 1

(config-if)#no ip ospf 0 multi-area 1
```


© 2021 IP Infusion Inc. Proprietary

ip ospf message-digest-key

Use this command to register an MD5 key for OSPF authentication.

Use the `no` parameter with this command to remove an MD5 key.

Message Digest Authentication is cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a message digest that is appended to the packet.

Use this command for uninterrupted transitions between passwords. This is helpful for administrators who want to change the OSPF password without disrupting communication. The system begins a rollover process until all the neighbors have adopted the new password. This allows neighboring routers to continue communication while the network administrator is updating them with a new password. The router will stop sending duplicate packets once it detects that all of its neighbors have adopted the new password.

Maintain only one password per interface, removing the old password whenever you add a new one. This prevents the local system from continuing to communicate with the system that is using the old password. Removing the old password also reduces overhead during rollover. All neighboring routers on the same network must have the same password value to enable exchange of OSPF routing data.

Command Syntax

```
ip ospf (A.B.C.D|) message-digest-key <1-255> md5 WORD
no ip ospf (A.B.C.D|) message-digest-key <1-255>
```

Parameters

`A.B.C.D`	IPv4 address of the interface.
`message-digest-key`	Specify a key ID.
`<1-255>`	Specify a key ID.
`md5`	Specify a key (password).
`WORD`	Specify an encrypted password (key).

Default

By default, MD5 key for OSPF authentication is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows OSPF authentication on the interface eth0 when IP address has not been specified.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf authentication message-digest
(config-if)#ip ospf message-digest-key 1 md5 yourpass
```

```
(config-if)#sh run int xe1

!

interface xe1

 ip ospf authentication

 ip ospf authentication-key 0x94eebee8c349a4b0

 ip ospf message-digest-key 1 md5 0x94eebee8c349a4b0

!

(config-if)#ip ospf message-digest-key 1 md5 0x94eebee8c349a4b0 - encrypted password of 16 characters which can be obtained from sh run <int>
```

The following example shows OSPF authentication on the interface eth0 for the IP address 1.1.1.1. (If the interface has two IP addresses assigned-- 1.1.1.1 & 2.2.2.2, OSPF authentication will be enabled only for the IP address 1.1.1.1)

```
(config)#interface eth0
(config-if)#ip ospf 1.1.1.1 authentication message-digest
(config-if)#ip ospf 1.1.1.1 message-digest-key 2 md5 yourpass
```


© 2021 IP Infusion Inc. Proprietary

ip ospf mtu

Use this command to set MTU size for OSPF to construct packets based on this value. Whenever OSPF constructs packets, it uses interface MTU size as Maximum IP packet size. This command forces OSPF to use the specified value overriding the actual interface MTU size.

This command does not configure the MTU settings in the kernel. OSPF does not recognize MTU size changes made in the kernel until the MTU size is updated through this command.

Use the `no` parameter with this command to return to the default value.

Command Syntax

```
ip ospf mtu <576-65535>
no ip ospf mtu
```

Parameters

`mtu`	Specify an MTU size.
`<576-65535>`	Specify an MTU size.

Default

By default, OSPF uses interface MTU derived from the kernel.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf mtu 1480
```

ip ospf mtu-ignore

Use this command to configure OSPF so that it does not check the MTU size during DD (Database Description) exchange.

Use the `no` form of this command to make OSPF check the MTU size during DD exchange.

Command syntax

```
ip ospf (A.B.C.D|) mtu-ignore
no ip ospf (A.B.C.D|) mtu-ignore
```

Parameters

`A.B.C.D`	IP address of the interface.

Default

By default, during the DD exchange process, OSPF checks the MTU size described in DD packets received from its neighbor. If the MTU size does not match the interface MTU, the neighbor adjacency is not established. Using this command makes OSPF ignore this check and allows establishing of adjacency regardless of MTU size in the DD packet.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-router)#ip ospf mtu-ignore
```


© 2021 IP Infusion Inc. Proprietary

ip ospf network

Use this command to set the OSPF network type.

Use the `no` parameter with this command to return to the default value.

Command Syntax

```
ip ospf network (broadcast|non-broadcast|point-to-multipoint|point-to-point)
ip ospf network point-to-multipoint non-broadcast
no ip ospf network
```

Parameters

`broadcast`	Sets the network type to broadcast.
`non-broadcast`	Sets the network type to NBMA.
`point-to-multipoint`	Sets the network type to point-to-multipoint.
`non-broadcast`	Sets the network type to NBMA.
`point-to-point`	Sets the network type to point-to-point.

Default

By default, OSPF network type is broadcast

Command Mode

interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the network to `point-to-point` type on the `eth0` interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf network point-to-point
```

ip ospf priority

Use this command to set the router priority to determine the designated router (DR) for the network.

A router with the higher router priority becomes the DR. If the priority is the same for two routers, the router with the higher router ID takes precedence.

Only routers with a nonzero priority value are eligible to become the designated or backup designated router. Configure router priority for broadcast or NBMA networks only and not for point-to-point networks.

Use the `no` parameter with this command to return to the default value.

Command Syntax

```
ip ospf (A.B.C.D|) priority <0-255>
no ip ospf (A.B.C.D|) priority
```

Parameters

`A.B.C.D`	The IP address of the interface.
`priority`	Specify the router priority of the interface.
`<0-255>`	Specify the router priority of the interface. The default value is 1.

Default

By default, ip ospf priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the OSPF priority value to 3 on the `eth0` interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf priority 3
```


© 2021 IP Infusion Inc. Proprietary

ip ospf retransmit-interval

Use this command to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.

After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgement. If the router does not receive an acknowledgement during the retransmit interval, it retransmits the LSA. Set the retransmission interval value conservatively to avoid needless retransmission. The interval should be greater than the expected round-trip delay between two routers.

Use the `no` parameter with this command to return to the default value.

Command Syntax

```
ip ospf (A.B.C.D|) retransmit-interval <1-3600>
no ip ospf (A.B.C.D|) retransmit-interval
```

Parameters

`A.B.C.D`	The IPv4 address of the interface.
`retransmit-interval`	Specify the interval.
`<1-3600>`	Specify the interval in seconds.

Default

By default, retransmit interval is 5 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the `ospf retransmit interval` to 6 seconds on the eth0 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf retransmit-interval 6
```

ip ospf transmit-delay

Use this command to set the estimated time it takes to transmit a link-state-update packet on the interface.

The transmit delay value adds a specified time to the age field of an update. If the delay is not added, the time in which the LSA transmits over the link is not considered. This command is especially useful for low speed links. Add transmission and propagation delays when setting the transmit delay value.

Use the `no` parameter with this command to return to the default value.

Command Syntax

```
ip ospf (A.B.C.D|) transmit-delay <1-65535>
no ip ospf (A.B.C.D|) transmit-delay
```

Parameters

`A.B.C.D`	The IPv4 address of the interface.
`transmit-delay`	Specify the time to transmit a link-state update.
`<1-65535>`	Specify the time in seconds to transmit a link-state update.

Default

By default, transmit delay is 1 second

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the OSPF transmit delay time to 3 seconds on the `eth0` interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf transmit-delay 3
```


© 2021 IP Infusion Inc. Proprietary

log-adjacency-changes

Use this command for the router to send a SYSLOG message when an OSPF neighbor goes up or down.

Use `no` parameter of this command to stop sending SYSLOG message.

Command Syntax

```
log-adjacency-changes (brief|detail|)
no log-adjacency-changes
```

Parameters

`brief`	Sends a SYSLOG message for each state change, not just when a neighbor goes up or down.
`detail`	Sends a SYSLOG message for each state change, not just when a neighbor goes up or down.

Default

Default option is brief.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#log-adjacency-changes
(config-router)#log-adjacency-changes detail

(config-router)#no log-adjacency-changes
(config-router)#no log-adjacency-changes detail
```

© 2021 IP Infusion Inc. Proprietary

max-concurrent-dd

Use this command to limit the number of Database Descriptors (DD) that can be processed concurrently.

This command is useful when a router's performance is affected from simultaneously bringing up several OSPF adjacencies. This command limits the maximum number of DD exchanges that can occur concurrently per OSPF instance, thus allowing for all of the adjacencies to come up.

Use the `no` option with this command to remove the limit.

Command Syntax

```
max-concurrent-dd <1-65535>
no max-concurrent-dd
```

Parameters

`<1-65535>`	Specify the number of DD processes.

Default

By default, max concurrent dd value is 64

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example set the `max-concurrent-dd` value to 4.

```
#configure terminal
(config)#router ospf 100
(config-router)#max-concurrent-dd 4
```


© 2021 IP Infusion Inc. Proprietary

maximum-area

Use this command to configure the maximum number of OSPF areas.

Use the `no` parameter with this command to disable the limit.

Command Syntax

```
maximum-area <1-4294967294>
no maximum-area
```

Parameters

`<1-4294967294>` Specify the maximum number of OSPF areas.

Default

By default, ospf maximum area is 4294967294

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#maximum-area 5
```

neighbor

Use this command to configure OSPF routers interconnecting to NBMA (Non-Broadcast Multi-Access) networks. Include one neighbor entry for each known non-broadcast network neighbor. Configure the neighbor address on the primary address of the interface.

Use the `no` parameter with this command to remove a configuration.

Command Syntax

```
neighbor A.B.C.D {cost <1-65535> | priority <0-255>| poll-interval <1-2147483647>}
no neighbor A.B.C.D { cost | priority | poll-interval}
no neighbor A.B.C.D
```

Parameters

`A.B.C.D`	Specify the interface IP address of the neighbor.
`priority`	Specify the router priority of the non-broadcast neighbor associated with the specified IP address.This parameter does not apply to point-to-multipoint interfaces.
`<0-255>`	Specify the router priority value of the non-broadcast neighbor associated with the specified IP address.
`poll-interval`	The reduced rate at which routers continue to send hello packets when a neighboring router has become inactive.
`<1-2147483647>`	Dead neighbor polling interval in seconds. Set this value much larger than hello interval.

Default

The default priority is 0 and polling interval is 120 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows neighbor configured with a priority value and poll interval time.

```
#configure terminal
(config)#router ospf 100
(config-router)#neighbor 1.2.3.4 priority 1 poll-interval 90
```


© 2021 IP Infusion Inc. Proprietary

network

Use this command to enable OSPF routing with a specified area ID (and optionally an instance ID) on interfaces with IP addresses that match the specified network address.

OSPF routing is enabled per IPv4 subnet basis. You define the network address using the prefix length or a subnet mask.

Use the `no` parameter with this command to disable OSPF routing on the interfaces.

Command Syntax

Network address defined using the prefix length:

```
network A.B.C.D/M area (A.B.C.D|<0-4294967295>) (instance-id <0-255>|)
no network A.B.C.D/M area (A.B.C.D|<0-4294967295>) (instance-id)
```

Network address defined using subnet mask:

```
network A.B.C.D A.B.C.D area (A.B.C.D|<0-4294967295>) (instance-id <0-255>|)
no network A.B.C.D A.B.C.D area (A.B.C.D|<0-4294967295>) (instance-id)
```

Parameters

`A.B.C.D/M`	IPv4 network address with prefix length.
`A.B.C.D`	IPv4 network address.
`A.B.C.D`	Subnet mask where the bits on left side are set to 1 to represent the network part and the bits on the right side are set to 0 to represent the host part.
`area`	OSPF area ID
`A.B.C.D`	OSPF area ID in IPv4 address format.
`<0-4294967295>`	OSPF area ID as a decimal value.
`instance-id`	Instance ID
`<0-255>`	Instance ID value.

Default

No network area is configured

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following the use of the `network` command with OSPF multiple-instance support disabled.

```
#configure terminal
(config-router)#network 10.0.0.0/8 area 3
(config-router)#network 10.0.0.0/8 area 1.1.1.1
```

The following shows the use of the `network` command with OSPF multiple-instance support enabled.

```
(config)#router ospf 100
(config-router)#network 10.0.0.0/8 area 3 instance-id 4
```


© 2021 IP Infusion Inc. Proprietary

ospf abr-type

Use this command to set an OSPF Area Border Router (ABR) type.

Use the `no` parameter with this command to revert the ABR type to the default setting (`cisco`).

Specifying the ABR type allows better functioning in a multi-vendor environment. The ABR types are:

- Cisco (RFC 3509): A router is considered an ABR if it has more than one area actively attached and one of them is the backbone area.
- IBM (RFC 3509): A router is considered an ABR if it has more than one area actively attached and the backbone area is configured. In this case the configured backbone need not be actively connected.
- Standard (RFC 2328): A router is considered an ABR if it has more than one area actively attached to it.

Command Syntax

```
ospf abr-type (cisco|ibm|standard|shortcut)
no ospf abr-type
```

Parameters

`cisco`	Specify an alternative ABR using Cisco implementation. This is the default ABR type.
`ibm`	Specify an alternative ABR using IBM implementation.
`standard`	Specify a standard ABR.
`shortcut`	Shortcut ABR.

Default

By default, ABR type is Cisco

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#ospf abr-type ibm
```

ospf area-interface-config-mode

Use this command to attach the interface to the router OSPF area. When this is enabled, any existing configuration of `router ospf` attached to the interface is erased.

Use no form of this command to disable. When this is disabled, any existing configuration of interface attached to the `router ospf` is erased.

Command Syntax

```
ospf area-interface-config-mode
```

```
no ospf area-interface-config-mode
```

Parameters

None

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS-OTN version 4.2.

Examples

```
#configure terminal
(config)#ospf area-interface-config-mode
```


© 2021 IP Infusion Inc. Proprietary

ospf flood-reduction

Use this command to Enable flood reduction on all OSPF interface. When this command is configured, an LSA sent out on the OSPF interface is set with the DNA bit in the LSA age field. If there is no change in LSA, it is not refreshed every refresh interval. LSAs are sent out on the interface only if there is a change in an LSA

Use the `no` option with this command to disable flood reduction on all OSPF interfaces.

Command Syntax

```
ospf flood-reduction
```

```
no ospf flood-reduction
```

Parameters

None

Default

By default, flood reduction on all OSPF interfaces is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#ospf flood-reduction

(config-router)#no ospf flood-reduction
```

ospf restart grace-period

Use this command to set the grace period for restarting the router.

If graceful restart is enabled, NSM is notified about the grace period. If the OSPF daemon unexpectedly shuts down, NSM sends this value to the OSPF daemon when it comes up again which uses this value to end the graceful state.

Use the `no` parameter with this command to revert to the default.

Command Syntax

```
ospf restart grace-period <1-1800>
no ospf restart grace-period
```

Parameters

`grace-period`	Specify the grace period.
`<1-1800>`	Specify the grace period in seconds.

Default

The default grace period for restarting the OSPF router is 120 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ospf restart grace-period 250
```


© 2021 IP Infusion Inc. Proprietary

ospf restart helper

Use this command to configure the helper behavior for graceful restart.

Use the `no` parameter with this command to revert to default.

Command Syntax

```
ospf restart helper max-grace-period <2-1800>
ospf restart helper never (router-id A.B.C.D|)
no ospf restart helper never
no ospf restart helper (never router-id (A.B.C.D | all) | max-grace-period|)
```

Parameters

`max-grace-period`	
	Help only if received grace-period is less than this value.
`<2-1800>`	
	Help only if received grace-period is less than this value.
`never`	Prevent the neighbor from entering helper mode.
`router-id`	Neighbor to never to act as helper.
`A.B.C.D`	Router ID of neighbor to never to act as helper.
`all`	All neighbors to never to act as helper.

Default

By default, router behave as helper. To disable it as helper, `ospf restart helper never` command should be configured. `ospf restart helper max-grace-period` – Max-grace-period to function as helper. If not configured, value will be the grace-period in restarting node.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ospf restart helper never router-id 1.1.1.1

#configure terminal
(config)#ospf restart helper only-reload max-grace-period 200

#configure terminal
(config)#no ospf restart helper never router-id all
```

ospf router-id

Use this command to specify a router ID for the OSPF process.

Configure each router with a unique router ID. In an OSPF router process which has active neighbors, a new router ID is used at the next reload or when you start the OSPF manually.

Use the `no` parameter with this command to force OSPF to use the previous router ID.

Command Syntax

```
ospf router-id A.B.C.D
router-id A.B.C.D


no ospf router-id
no router-id (A.B.C.D|)
```

Parameters

`A.B.C.D`	Specify the router ID in IPv4 address format.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows a specified router ID 2.3.4.5.

```
#configure terminal
(config)#router ospf 100
(config-router)#ospf router-id 2.3.4.5
```


© 2021 IP Infusion Inc. Proprietary

overflow database

Use this command to limit the maximum number of LSAs that can be supported by the OSPF instance.

Use the `no` parameter with this command to have an unlimited number of LSAs.

Command Syntax

```
overflow database <0-4294967294> (hard|soft|)
no overflow database
```

Parameters

`<0-4294967294>`	The maximum number of LSAs
`hard`	Shutdown occurs if the number of LSAs exceeds the specified value.
`soft`	Warning message appears if the number of LSAs exceeds the specified value.

Default

No default value is specified. unlimited number of LSAs.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the database overflow to 5 and shutting down in that event.

```
#configure terminal
(config)#router ospf 100
(config-router)#overflow database 5 hard
```

overflow database external

Use this command to limits the number of AS-external-LSAs a router can receive once it is in the wait state.

Use the `no` parameter with this command to revert to default.

Command Syntax

```
overflow database external <0-2147483647> <0-65535>
no overflow database external
```

Parameters

`<0-2147483647>`	The maximum number of LSAs. This value should be the same on all routers in the AS.
`<0-65535>`	The number of seconds the router waits before trying to exit the database overflow state. If this parameter is 0, the router exits the overflow state only after an explicit administrator command.

Default

The default OSPF exit overflow interval is 0 second and number of external LSDB limit is unlimited.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the maximum number of LSAs to 5 and the time to recover from overflow state to be 3.

```
#configure terminal
(config)#router ospf 100
(config-router)#overflow database external 5 3
```


© 2021 IP Infusion Inc. Proprietary

passive-interface

Use this command to suppress sending Hello packets on all interfaces or on a specified interface.

This command configures OSPF on simplex Ethernet interfaces. Since a simplex interface represents only one network segment between two devices, configure the transmitting interface as a passive interface. This ensures that OSPF does not send hello packets for the transmitting interface. Both the devices can see each other via the hello packet generated for the receiving interface.

Use the `no` form with this command to resume sending `hello` packets on all interfaces, or on a specified interface.

Note: The command `passive-interface` alone configures all interfaces as non-passive.

Command Syntax

```
passive-interface
passive-interface IFNAME ((disable|enable)|)
passive-interface IFNAME A.B.C.D ((disable|enable)|)
no passive-interface
no passive-interface IFNAME
no passive-interface IFNAME A.B.C.D
```

Parameters

`enable`	Enable passive interface
`disable`	Disable passive interface
`IFNAME`	The name of the interface.
`A.B.C.D`	IPv4 address of the interface.

Default

The default OSPF exit overflow interval is 0 second and number of external LSDB limit is 100000.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router ospf 100
(config-router)#passive-interface eth0 enable
```

redistribute

This command redistributes routes from a routing protocol, static route, and kernel route into an OSPF routing table.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
redistribute (kernel|connected|static|rip|bgp|isis|ospf (<1-65535>|)) {metric <0-
  16777214>|metric-type (1|2)|?route-map WORD|tag <0-4294967295>}
no redistribute (kernel|connected|static|rip|bgp|isis|ospf (<1-65535>|))
  metric|metric-type|?route-map|tag}
```

Parameters

`kernel`	Specify kernel routes.
`connected`	Specify connected routes.
`static`	Specify static routes.
`rip`	Specify RIP routes.
`bgp`	Specify BGP routes.
`isis`	Specify IS-IS routes.
`ospf`	Specify OSPF process.
`<1-65535>`	Specify an OSPF process ID to redistribute a particular OSPF instance into another OSPF instance. If not specified, this command redistribute OSPF instance with process ID 0.
`metric`	Specify the external metric.
`<0-16777214>`	Specify the external metric.
`metric-type`	Specify the external metric-type (see RFC 3101):
`1`	Set OSPF External Type 1 metrics.
`2`	Set OSPF External Type 2 metrics.
`route-map`	Specify a route map reference.
`WORD`	Specify name of the route-map.
`tag`	Tag value to use as a “match” value for controlling redistribution via route maps
`<0-4294967295>`	Specify the route tag.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

© 2021 IP Infusion Inc. Proprietary

Examples

```
(config)#router ospf 100
(config-router)#redistribute bgp metric 12
```

The following example shows redistributing OSPF instance 2 into OSPF instance 1.

```
#configure terminal
(config)#router ospf 1
(config-router)#redistribute ospf 2
```

The following example shows redistributing OSPF instance `2` into OSPF instance `1`, with an external metric of `10`, metric type `1`, a route-map named `rmp1`, and an external route tag of `3`.

```
#configure terminal
(config)#router ospf 1
(config-router)#redistribute ospf 2 metric 10 metric-type 1 route-map rmp1 tag
3
```

restart ospf graceful

Use this command to restart OSPF gracefully.

After this command is executed, the router immediately shuts down. NSM is notified that OSPF has shut down gracefully. NSM preserves routes installed by OSPF until the grace period expires.

Command Syntax

```
restart ospf graceful (grace-period <1-1800>|)
```

Parameters

`grace-period`	Specify a grace period.
`<1-1800>`	Specify a grace period in seconds.

Default

By default, restart ospf graceful is disabled. Default value of grace-period is 120 seconds.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#restart ospf graceful grace-period 200
```


© 2021 IP Infusion Inc. Proprietary

router ospf

Use this command to enter router mode and to configure an OSPF routing process.

Specify the process ID to configure multiple instances of OSPF. When running a single instance of OSPF, you do not need to specify a process ID.

Use the `no` parameter with this command to terminate an OSPF routing process.

Command Syntax

```
router ospf
router ospf <1-65535>


no router ospf
no router ospf <1-65535>
```

Parameters

`<1-65535>`	Process ID; should be unique for each routing process.

Default

No routing process defined

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows the use of the `router ospf` command to enter router mode. Note the change in the prompt.

```
#configure terminal
(config)#router ospf 100
(config-router)#
```

show cspf rsvp forwarding-timer

This command displays the information of Graceful Restart capable RSVP client to ISIS or OSPF, CSPF that are currently shutdown.

Command Syntax

```
show cspf rsvp forwarding-timer
```

Parameters

None

Command Mode

Privileged Exec modes

Applicability

This command was introduced before OcNOS-SP version 5.0.

Example

```
OcNOS#show cspf rsvp forwarding-timer
CSPF Server      Protocol-Name   GR-State        Time Remaining (sec)
Disconnected-time
OSPF             RSVP            ACTIVE          88                      2021/
08/18 04:49:23
OcNOS#
```


© 2021 IP Infusion Inc. Proprietary

show debugging ospf

Use this command to display the set OSPF debugging option.

Command Syntax

```
show debugging ospf
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the `show debugging ospf` command. Some lines in this output wrap around, they might not wrap around in the actual display.

```
#show debugging ospf
OSPF debugging status:
  OSPF packet Link State Update debugging is on
  OSPF all events debugging is on
```

show ip ospf

Use this command to display general information about all OSPF routing processes.

Command Syntax

```
show ip ospf (<0-65535>|)
```

Parameters

<0-65535>	The ID of the router process for which information will be displayed. If this parameter is specified, only the information for the specified routing process is displayed.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip ospf 1
 Routing Process "ospf 1" with ID 4.1.1.1
 Process uptime is 1 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 This router is an ASBR (injecting external routing information)
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Initial LSA throttle delay 10 secs 0 msecs
 Minimum hold time for LSA throttle 20 secs 0 msecs
 Maximum wait time for LSA throttle 45 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 5. Checksum 0x010632
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 5
 External LSA database is unlimited.
 Number of LSA originated 6
 Number of LSA received 0
 Number of areas attached to this router: 1
    Area 0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 0
        Area has no authentication
        SPF algorithm last executed 00:00:47.558 ago
```


© 2021 IP Infusion Inc. Proprietary

```
SPF algorithm executed 2 times
Number of LSA 1. Checksum 0x0041e0
```

OSPF Routing Process Fields

Table 1-120 explains the routing process fields.

Table 1-120: show ip ospf output details

Field	Description
Routing Process with ID	OSPF process identifier and router identifier.
Process is not up	OSPF process is not running.
Process uptime is	OSPF process running time.
Process bound to VRF	VRF name
Router is in Graceful Restart	When in graceful restart.
Router is in Restart Signaling	When in restart signalling.
Bidirectional Forwarding Detection is configured	When BFD is enabled.
Conforms to RFC2328, and RFC1583 Compatibility flag is enabled	RFC compatibility.
Supports only single TOS (TOS0) routes	OSPF TOS-based routing was never deployed.
Supports opaque LSA	When opaque LSAs are supported.
Do not support Restarting	When restart is not supported.
Supports Graceful Restart	Method of restart in process.
Supports Restart Signaling	Method of restart in signaling process.
Connected to MPLS VPN Super backbone	VRF is enabled and the process is connected to the MPLS VPN backbone.
This router is an ABR, ABR Type is	Type of ABR: Standard (RFC2328) Alternative Cisco (RFC3509) Alternative IBM (RFC3509) Alternative Shortcut
This router is an ASBR (injecting external routing information)	Type of router function in the process.
SPF schedule delay initial	Initial SPF schedule delay.
SPF schedule delay min	Minimum delay between receiving a change to SPF calculation.
SPF schedule delay max	Maximum delay between receiving a change to SPF calculation.
Refresh timer	LSA refresh interval.
Number of incoming current DD exchange neighbors	Incoming neighbor Database Descriptors and maximum concurrent DDs.

Table 1-120: show ip ospf output details (Continued)

Field	Description
Number of outgoing current DD exchange neighbors	Outgoing neighbor Database Descriptors and maximum concurrent DDs.
Initial LSA throttle delay	Initial delay for the generation of LSAs.
Minimum hold time for LSA throttle	Minimum hold time between generation of the same LSA.
Maximum wait time for LSA throttle	Maximum wait time between generation of the same LSA.
Minimum LSA arrival	Minimum time between reception of new LSAs during flooding.
Number of external LSA	Number of AS external LSAs and checksum.
Number of opaque AS LSA	Number of AS opaque LSAs and checksum.
Number of non-default external LSA	For database overflow, number of non-default external LSAs.
External LSA database is unlimited	When the external LSA database is unlimited.
External LSA database limit	Maximum number of LSAs in database.
Exit database overflow state interval is	Exit database overflow state interval.
Exit database overflow state interval is not configured	When the exit database overflow state interval is not set.
OSPF is [not] in database overflow state now	Whether OSPF is in database overflow state now.
Next attempt to exit database overflow state in	How long until OSPF tries to exit the database overflow state.
LSDB database overflow limit	Maximum number of LSAs that can be supported by the OSPF instance.
LSDB exceed overflow limit	Whether OSPF is exceeding the maximum number of LSAs.
Number of LSA originated	LSAs originated by the OSPF instance.
Number of LSA received	LSAs received by the OSPF instance.
Number of areas attached to this router	As stated
Next fields are repeated for each area	As stated
Area	Area identifier.
(BACKBONE)	Area is a backbone.
no-summary	Area is a stub and does no import summaries.
(Inactive)	Area is not active.
Number of interfaces in this area is	Number of interfaces in this area.
Number of fully adjacent neighbors in this area	As stated.
Number of fully adjacent virtual neighbors through this area	As stated.

© 2021 IP Infusion Inc. Proprietary

Table 1-120: show ip ospf output details (Continued)

Field	Description
Area has no authentication	Area does not use authentication.
Area has simple password authentication	Area uses password authentication.
Area has message digest authentication	Area uses MD5 authentication.
SPF algorithm last executed	As stated.
SPF algorithm executed	As stated.
Number of LSA	Number of LSAs in area link-state database and checksum.
End of area field	As stated.
NSSA Translator Role is	candidate: Translate Type-7 LSAs to Type-5 if router is elected. never: Do not translate Type-7 LSAs to Type-5. always: Always translate Type-7 LSAs to Type-5.
NSSA Translator State is	disabled: Router is not a border router. enabled: Router is a border router. elected: Router has been elected to be an NSSA translator.
Stability Interval	If an elected translator determines its services are no longer required, how long it continues to perform its services.
Number of NSSA Translator Events	As stated.
Shortcutting mode	Shortcut ABR that installs inter-area routes through non-backbone areas if non-backbone paths are really better: Default Enabled Disabled
S-bit consensus	Whether other ABR agrees on S-bit: ok no
Dste Status	Whether DSTE is enabled or disabled.

show ip ospf border-routers

Use this command to display the ABRs and ASBRs for OSPF instances.

Command Syntax

```
show ip ospf (<0-65535>|) border-routers
```

Parameters

`<0-65535>`	The ID of the router process for which information will be displayed.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the `show ip ospf border-routers` command.

```
#show ip ospf border-routers
OSPF process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.15.0.1 [10] via 10.10.0.1, eth0, ASBR, Area 0.0.0.0
i 172.16.10.1 [10] via 10.10.11.50, eth1, ABR, ASBR, Area 0.0.0.0
```

Border Router Fields

Table 1-121 explains the border router fields.

Table 1-121: border router output details

Field	Description
Code	i: Intra-area route I: Inter-area route
Router ID	Router identifier of the destination
Cost	Cost of using this route.
via	Next hop IP address toward the destination.
is directly connected	Destination is directly connected.
Interface	Outgoing interface name.
Type	Router type of the destination: ABR or ASBR.
through Transit Area	Next hop is an area that carries traffic that neither originates nor terminates in the area itself.
Area	Area identifier from which this route was learned.
Transit	Area is a transit area.

© 2021 IP Infusion Inc. Proprietary

show ip ospf database brief

Use this command to display a summary of the OSPF database.

Command Syntax

```
show ip ospf database (self-originate|max-age|adv-router A.B.C.D|)
show ip ospf <0-65535> database(self-originate|max-age|adv-router A.B.C.D|)
```

Parameters

`self-originate`	Self-originated link states.
`max-age`	LSAs which have reached the maximum age (3600 seconds).
`A.B.C.D`	IPv4 address of the advertising router.
`<0-65535>`	ID of the router process

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip ospf database
       OSPF Router process 100 with ID (100.100.100.72)
                Router Link States (Area 0.0.0.0)
Link ID         ADV Router      Age   Seq#       CkSum  Link count
10.100.12.57    10.100.12.57     930  0x80000003 0x90de 2
100.100.100.72  100.100.100.72   933  0x80000004 0x7592 2
                Net Link States (Area 0.0.0.0)
Link ID         ADV Router      Age   Seq#       CkSum
10.100.10.72    100.100.100.72   933  0x80000001 0x0bef
                Summary Link States (Area 0.0.0.0)
Link ID         ADV Router      Age   Seq#       CkSum  Route
10.60.0.0       10.100.12.57     928  0x80000001 0x5108 10.60.0.0/24
71.87.120.0     10.100.12.57     928  0x80000001 0xc2c5 71.87.120.0/24
127.0.0.1       10.100.12.57     928  0x80000001 0x23fb 127.0.0.1/32
```

OSPF Database Fields

Table 1-122 explains the fields for each database entry.

Table 1-122: ospf database output details

Field	Description
Link ID	The meaning of this field depends on the type of Link-State Advertisement (LSA). Type 1: Router LSA (depends on the type of network to which the router connects): Point-to-point network: neighbor's router ID. Transit network: IP address of the designated router's interface. Stub network: IP network or subnet address Virtual link: Neighbor's Router ID. Type 2: Network LSA: The IP address of the designated router's interface. Type 3: Summary LSA: The IP address of the network or subnet being advertised.
ADV Router	The ID of the router advertising the LSA.
Age	The age of the LSA.
Seq#	The sequence number of the LSA. This number increments each time a new instance of the LSA originates. This update helps other routers identify the most recent instance of the LSA.
CkSum	The fetch checksum of the complete LSA except the Age field.
Link count	Total number of links.
Route	Summary prefix address.

© 2021 IP Infusion Inc. Proprietary

show ip ospf database detail

Use this command to display details of the OSPF database.

Command Syntax

```
show ip ospf database (asbr-summary|external|network|router|summary|nssa-
  external|opaque-link|opaque-area|opaque-as) (self-originate|adv-router A.B.C.D|)
show ip ospf <0-65535> database (asbr-summary|external|network|router|summary)
  (self-originate|adv-router A.B.C.D|)
show ip ospf database (asbr-summary|external|network|router|summary|nssa-
  external|opaque-link|opaque-area|opaque-as) A.B.C.D (self-originate|adv-router
  A.B.C.D|)
show ip ospf <0-65535> database (asbr-summary|external|network|router|summary|nssa-
  external|opaque-link|opaque-area|opaque-as) A.B.C.D (self-originate|adv-router
  A.B.C.D|)
```

Parameters

`<0-65535>`	The ID of the router process for which information should be displayed.
`asbr-summary`	Type 4 ASBR summary LSAs.
`external`	Type 5 external LSAs.
`network`	Type 2 network LSAs.
`router`	Type 1 router LSAs.
`summary`	Type 3 summary LSAs.
`nssa-external`	Type 7 NSSA external LSAs.
`opaque-link`	Type 9 LSAs which are not flooded beyond the local network.
`opaque-area`	Type 10 LSAs which are not flooded beyond the borders of their area.
`opaque-as`	Type 11 LSAs which are flooded throughout the AS.
`A.B.C.D`	Link state ID as an IP address.
`self-originate`	Display self-originated link states.
`adv-router`	Advertising router link states.
`A.B.C.D`	IPv4 address of advertising router.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example: external and self-originate Parameters

This is sample output with the `external` and `self-originate` parameters.

```
#show ip ospf database external self-originate

 OSPF Router process 100 with ID (10.10.11.50)
```

```
 AS External Link States
  LS age: 298
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 10.10.100.0 (External Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x7033
  Length: 36
  Network Mask: /24
 Metric Type: 2 (Larger than any link state path)
 TOS: 0
 Metric: 20
 Forward Address: 10.10.11.50
 External Route Tag: 0
```

Example: opaque-as and self-originate Parameters

This is sample output with the `opaque-as` and `self-originate` parameters.

```
#show ip ospf database opaque-as self-originate
 OSPF Router process 100 with ID (10.10.11.50)
 AS-Global Opaque-LSA
  LS age: 325
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external Opaque-LSA
  Link State ID: 11.10.9.23 (AS-external Opaque-Type/ID)
  Opaque Type: 11
  Opaque ID: 657687
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0xb018
 Length: 25
```

Example: adv-router Parameter

This is a sample output with the `adv-router` parameter.

```
#show ip ospf database nssa-external adv-router 10.10.11.50
 OSPF Router process 100 with ID (10.10.11.50)
 NSSA-external Link States (Area 0.0.0.0)
 NSSA-external Link States (Area 0.0.0.1 [NSSA])
  LS age: 78
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 0.0.0.0 (External Network Number For NSSA)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0xc9b6
  Length: 36
  Network Mask: /0
 Metric Type: 2 (Larger than any link state path)
 TOS: 0
 Metric: 1
 NSSA: Forward Address: 0.0.0.0
OSPF Router process 100 with ID (10.10.11.50)
 NSSA-external Link States (Area 0.0.0.0)
 NSSA-external Link States (Area 0.0.0.1 [NSSA])
```


© 2021 IP Infusion Inc. Proprietary

```
  LS age: 78
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
 Link State ID: 0.0.0.0 (External Network Number For NSSA)
```

Example: router and Link State ID Parameters

This is sample output with the `router` and link state ID parameters.

```
#show ip ospf database router 10.10.11.50
 OSPF Router process 100 with ID (10.10.11.50)
 Router Link States (Area 0.0.0.0)
  LS age: 878
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.10.11.50
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000004
  Checksum: 0xe39e
  Length: 36
Number of Links: 1
 Link connected to: Stub Network
 (Link ID) Network/subnet number: 10.10.10.0
 (Link Data) Network Mask: 255.255.255.0
Number of TOS metrics: 0
 TOS 0 Metric: 10
 Router Link States (Area 0.0.0.1)
  LS age: 877
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.10.11.50
  Advertising Router: 10.10.11.50
 LS Seq Number: 80000003
```

Example: adv-router Parameter

This is sample output using the `adv-router` parameter for flood reduction.

```
#show ip ospf database summary adv-router 10.10.11.50

 OSPF Router process 100 with ID (10.10.11.50)
 Summary Link States (Area 0.0.0.0)
  LS age: 1(DoNotAge)
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
 TOS: 0 Metric: 10
Summary Link States (Area 0.0.0.1)
  LS age: 989
  Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
```

```
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
 TOS: 0 Metric: 10

#show ip ospf database external self-originate

 OSPF Router process 100 with ID (10.10.11.50)

 AS External Link States
  LS age: 298
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 10.10.100.0 (External Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x7033
  Length: 36
  Network Mask: /24
 Metric Type: 2 (Larger than any link state path)
 TOS: 0
 Metric: 20
 Forward Address: 10.10.11.50
 External Route Tag: 0
```

Database Detail Header Fields

Table 1-123 explains the fields for each database entry.

Table 1-123: ospf database detail header fields

Field	Description
LS age	Age of the LSA in seconds. “Do Not Age” is displayed if the DNA bit is set.
Options	LSA options as explained in Table 1-124.
Flags	ABR: Area border router ASBR: AS boundary router VL-endpoint: Endpoint of an active virtual link that is using the described area as a transit area Shortcut: shortcut ABR NSSA-Translator: NSSA border router with NSSA Translate or State enabled
LS Type	Type of LSA: Router-LSA Network-LSA Summary-LSA ASBR-summary-LSA AS-external-LSA AS-NSSA-LSA Link-Local Opaque-LSA Area-Local Opaque-LSA AS-external Opaque-LSA

© 2021 IP Infusion Inc. Proprietary

Table 1-123: ospf database detail header fields

Field	Description
Link State ID	Identifier of the router described by the LSA.
Opaque Type	Opaque type used to identify the application type of the LSA: 9: link-local scope 10: area-local scope 11: LSA flooded throughout the AS
Opaque ID	Identifier used to differentiate LSAs of the same type.
Advertising Router	Identifier of the router that originated the LSA.
LS Seq Number	Sequence number of the LSA. This number increments each time a new instance of the LSA originates. This update helps other routers identify the most recent instance of the LSA.
Checksum	Checksum of the entire LSA, except the LS age field.
Length	Length of the LSA
I LSA	Indication LSA: ASBR set the infinity metric to tell all routers in the backbone not to originate DNA LSAs.

OSPF LSA Option Bits

Table 1-124 explains the fields for each database entry.

Table 1-124: ospf LSA option bits output details

Bit	Description
DN	Used in MPLS-based L3 VPNs. When a route learned from a customer network via OSPF is advertised across a BGP/MPLS VPN using Multiprotocol BGP and advertised back to a customer network via OSPF, a loop can happen where the OSPF route is redistributed back to the VPN service provider network via BGP. The DN-bit prevents this type of routing loop. When an OSPF router receives a Type 3, 5, or 7 LSA with the DN-bit set, it foes use that LSA for OSPF route calculations.
O	Originating router supports Type 9, 10, and 11 Opaque LSAs.
DC	Originating router supports OSPF over Demand Circuits.
L	Whether the OSPF packet contains a Link-Local Signaling (LLS) data block. This bit is set only in Hello and database description packets.
N/P	The N-bit is used only in Hello packets when the originating router supports Type-7 NSSA-External-LSAs. Neighboring routers with mismatched N-bit will not form a neighbor relationship. This restriction ensures that all OSPF routers within an area support NSSA capabilities. When the N-bit is set, the E-bit must be 0. The P-bit is used only in Type-7 NSSA-External-LSA headers. Due to this reason, the N- and P-bits share the same position in the options field. The P (Propagate) bit is set to inform an NSSA ABR to translate Type-7 LSAs into Type-5 LSAs.
MC	Originating router supports multicast extensions to OSPF (MOSPF)

Table 1-124: ospf LSA option bits output details (Continued)

Bit	Description
E	Originating router accepts AS External LSAs. The bit is set in all AS External LSAs and in all LSAs originated in the backbone and non-stub areas; and is be set to 0 in all Hellos and LSAs originated within a stub area. Additionally, this bit is used in Hello packets to indicate the capability of a router interface to send and receive Type-5 AS-External-LSAs. Neighboring routers with mismatched E-bit do not form a neighbor relationship. This restriction ensures that all OSPF routers within an area support the stub capabilities.
T	Originating router supports Multitopology OSPF (MT-OSPF.) Older OSPF specifications used this bit when the originating router support TOS-based routing. However, OSPF TOS-based routing was never deployed; therefore the T-bit was never used.

Type 1 Router LSAs (“router” Parameter)

Table 1-125 explains the fields for each database entry.

Table 1-125: router LSAs

Field	Description
Number of Links	Number of router links the LSA describes.
Link connected to	Description of the router link: another Router (point-to-point) a Transit Network Stub Network a Virtual Link
(Link ID)	Identifier of the router to which the link connects: Neighboring Router ID Designated Router address Network/subnet number Neighboring Router ID
(Link Data)	Extra information: Router Interface address Network Mask
Number of TOS metrics	Number of TOS (Type of Service) metrics for this link, not including the metric for TOS 0.
TOS 0 Metric	Cost of using this router link for TOS 0.

Type 2 Net Link States (“network” Parameter)

Table 1-126 explains the fields for each database entry.

Table 1-126: net LSAs

Field	Description
Network Mask	IP address mask for the network.
Attached Router	Identifiers of each router attached to the network.

© 2021 IP Infusion Inc. Proprietary

Type 3 Summary LSAs (“summary” Parameter) and Type 4 ASBR Summary LSAs (“asbr-summary” Parameter)

Table 1-127 explains the fields for each database entry.

Table 1-127: summary and ASBR summary link states

Field	Description
Network Mask	For Type 3 LSAs, the destination network's IP address mask. Not meaningful for Type 4 link state advertisements.
TOS: 0 Metric	Cost of using this router link for TOS 0.

Type 5 AS External LSAs (“external” Parameter)

Table 1-128 explains the fields for each database entry.

Table 1-128: external LSAs

Field	Description
Network Mask	IP address mask for the advertised destination
Metric Type	1: Type 1 external metric that is comparable directly (without translation) to the link state metric 2: Type 2 external metric that is considered larger than any link state path
TOS	Always zero.
Metric	The cost of this route.
Forward Address	Data traffic for the advertised destination is forwarded to this address.
External Route Tag	Custom field attached to each external route whose use is defined by the application.

Type 7 NSSA External Link States (“nssa-external” Parameter)

Table 1-129 explains the fields for each database entry.

Table 1-129: NSSA external LSAs

Field	Description
Network Mask	IP address mask for the advertised destination
Metric Type	1: Type 1 external metric that is comparable directly (without translation) to the link state metric 2: Type 2 external metric that is considered larger than any link state path
Metric	The cost of this route.
NSSA: Forward Address	Data traffic for the advertised destination is forwarded to this address.
External Route Tag	Custom field attached to each external route whose use is defined by the application.

show ip ospf igp-shortcut-lsp

Use this command to show the IGP shortcut LSP used by OSPF.

Command Syntax

```
show ip ospf igp-shortcut-lsp
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip ospf igp-shortcut-lsp
 Tunnel-endpoint     Tunnel-id     Tunnel-metric
 8.8.8.8             101           2              active
```

Table 1-130 explains the fields in the output.

Table 1-130: show ip ospf igp-shortcut-lsp output details

Field	Description
Tunnel-endpoint	Tunnel endpoint address of ospf.
Tunnel-id	Tunnel address (destination port) for the session.
Tunnel-metric	Number of tunnel-metric.
active/inactive	Whether the tunnel is active or inactive.

© 2021 IP Infusion Inc. Proprietary

show ip ospf igp-shortcut-route

Use this command to show the IGP shortcut route calculated by OSPF.

Command Syntax

```
show ip ospf (<0-65535>|) igp-shortcut-route
```

Parameters

<0-65535>	ID of the router process.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip ospf igp-shortcut-route
OSPF process 0:
8.8.8.8/32 [2] tunnel-id: 101, 8.8.8.8
15.15.15.15/32 [0] tunnel-id: 101, 8.8.8.8
20.20.15.0/24 [0] tunnel-id: 101, 8.8.8.8
```

Table 1-131 explains the fields in the output.

Table 1-131: show ip igp-shortcut-route output details

Field	Description
OSPF process	OSPF process identifier.
Destination	IP address of the destination port.
Metric	Number of tunnel metric.
Tunnel-ID	Tunnel address (destination port) for the session.
Tunnel-End-Point	Tunnel endpoint address of ospf.

© 2021 IP Infusion Inc. Proprietary

show ip ospf interface

Use this command to display interface information for OSPF.

Command Syntax

```
show ip ospf interface (IFNAME|)
```

Parameters

IFNAME	Interface name.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip ospf interface
eth1 is up, line protocol is up
 Internet Address 10.100.10.72/24, Area 0.0.0.0, MTU 1500
    Router ID 100.100.100.72, Network Type BROADCAST, Cost: 10, TE Metric 0
    Transmit Delay is 1 sec, State DR, Priority 1
    LDP-OSPF Sync configured
    Holddown timer : 50 seconds, Remaining time =  30seconds
    Designated Router (ID) 100.100.100.72, Interface Address 10.100.10.72
    Backup Designated Router (ID) 10.100.12.57, Interface Address 10.100.10.105
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:05
    Neighbor Count is 1, Adjacent neighbor count is 1
    Crypt Sequence Number is 0
    Hello received 19 sent 106, DD received 4 sent 3
    LS-Req received 1 sent 1, LS-Upd received 3 sent 3
    LS-Ack received 2 sent 3, Discarded 0
```

OSPF Interface Fields

Table 1-132 explains the fields for each interface entry.

Table 1-132: OSPF interface output details

Field	Description
Internet address	IP address and subnet mask of the interface.
Area	OSPF area to which the interface belongs.
MTU	Maximum Transmission Unit (MTU) of the interface.
Transmit Delay	Transmit delay of the interface.

© 2021 IP Infusion Inc. Proprietary

Table 1-132: OSPF interface output details

Field	Description
Priority	OSPF priority of the interface used for election of Designated Router (DR) and Backup Designated Router (BDR).
Hello	OSPF hello-interval.
Dead	OSPF dead-interval.
Wait	Hello wait-interval.
Retransmit	The period, in seconds, for which the router waits between retransmissions of OSPF packets that have not been acknowledged.
Hello due in	Time period for which router expects to receive hello packet.
Neighbor Count	OSPF neighbor count.
Adjacent neighbor	OSPF adjacent neighbor count.
Crypt Sequence Number	Used for authentication.
Hello received	Number of Hello packets and DD packets sent and received.
LS-Req	Number of LSA requests and LSA updates sent and received.
LS-Ack	Number of LSA acknowledgments sent and received number of LSA acknowledgment discards.

Example: DoNotAge

The following is sample output of this command when DoNotAge is enabled:

```
#show ip ospf interface eth1
eth1 is up, line protocol is up
 Internet Address 1.1.1.1/24, Area 0.0.0.0, MTU 1500
 Process ID 0, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 10
 Transmit Delay is 1 sec, State Waiting, Priority 1, TE Metric 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:02
 Neighbor Count is 0, Adjacent neighbor count is 0
 Crypt Sequence Number is 1106347721
 Hello received 0 sent 1, DD received 0 sent 0
 LS-Req received 0 sent 0, LS-Upd received 0 sent 0
 LS-Ack received 0 sent 0, Discarded 0
 Reduce LSA flooding
```

Example: Hello Suppression

The following is sample output of this command when Hello-Suppression is enabled:

```
#sh ip os interface
p7p1 is up, line protocol is up
  Internet Address 14.1.1.2/24, Area 0.0.0.0, MTU 1500
```

```
  Process ID 1, VRF (default), Router ID 2.2.2.2, Network Type POINTOMULTIPOINT, Cost:
1
  Reduce LSA flooding.
  Transmit Delay is 1 sec,  State Point-To-Point, TE Metric 1
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:03
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 1 neighbor(s)
  Hello received 5 sent 8, DD received 8 sent 6
  LS-Req received 2 sent 2, LS-Upd received 8 sent 9
  LS-Ack received 6 sent 6, Discarded 0
  No authentication
```


© 2021 IP Infusion Inc. Proprietary

show ip ospf multi-area-adjacencies

Use this command to display multi-area adjacency information for OSPF.

Command Syntax

```
show ip ospf (<0-65535>|) multi-area-adjacencies
```

Parameters

<0-65535>	The ID of the router process for which information should be displayed.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command:

```
#show ip ospf 1 multi-area-adjacencies

Multi-area-adjacency on interface eth1 to neighbor 20.20.20.10
Internet Address 20.20.20.11/24, Area 0.0.0.1, MTU 1500
Process ID 1, Router ID 10.10.10.10, Network Type POINTOPOINT, Cost: 10
Transmit Delay is 1 sec, State Point-To-Point
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:02
Neighbor Count is 0, Adjacent neighbor count is 0
Crypt Sequence Number is 1229928206
Hello received 0 sent 513, DD received 0 sent 0
LS-Req received 0 sent 0, LS-Upd received 0 sent 0
LS-Ack received 0 sent 0, Discarded 0
```

Table 1-133 explains the fields for each adjacency entry.

Table 1-133: show ip ospf multi-area-adjacencies output details

Field	Description
Multi-area-adjacency	Specifies the interface name and the router ID to which it is connected.
Internet Address	As Stated
Area	As Stated
MTU	Maximum Transmission Unit in bytes.
Process ID	The Process Identifier.
Router ID	As Stated
Network Type	In multi-area adjacencies, this is a point-to-point network with the neighbor.

Table 1-133: show ip ospf multi-area-adjacencies output details (Continued)

Field	Description
Cost	A reference bandwidth of 100 Mbps for cost calculation. The formula to calculate the cost is reference bandwidth divided by interface bandwidth.
Transmit Delay	A stated
State	As stated
Timer intervals configured	Hello timer = 10, Dead timer = 40, Wait timer = 40, Retransmit timer = 5
Hello due in	Countdown timer for a Hello message from the neighbor.
Neighbor Count	The number of neighbor.
Adjacent neighbor count	The number of neighbors participating in adjacencies.
Crypt Sequence Number	The 32-bit cryptographic sequence number appended on each OSPF protocol packet.
Hello received, sent	Hello packets sent and received.
DD received, sent	Database Description packets sent and received.
LS-Req received, sent	Link State Request packets sent and received.
LS-Upd received, sent	Link State Update packets sent and received.
LS-Ack received, sent, discarded	Link State Acknowledgement packets sent, received, or discarded.

© 2021 IP Infusion Inc. Proprietary

show ip ospf neighbor

Use this command to display information about OSPF neighbors.

Command Syntax

```
show ip ospf (<0-65535>|) neighbor
show ip ospf (<0-65535>|) neighbor all
show ip ospf (<0-65535>|) neighbor interface A.B.C.D
show ip ospf (<0-65535>|) neighbor A.B.C.D
show ip ospf (<0-65535>|) neighbor A.B.C.D detail
show ip ospf (<0-65535>|) neighbor detail
show ip ospf (<0-65535>|) neighbor detail all
```

Parameters

`<0-65535>`	The ID of the router process
`all`	Include downstatus neighbor
`A.B.C.D`	IPv4 address
`detail`	Details of neighbors

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface    Instance ID
1.1.1.1           1   Full/ -         inactive    14.1.1.1        p7p1                0
3.3.3.3           1   Full/ -         00:01:41    15.1.1.2        p8p1                0
3.3.3.3           1   Full/ -         inactive    15.1.1.2        VLINK0
```

OSPF Neighbor Fields

Table 1-134 explains the fields for each neighbor entry.

Table 1-134: OSPF neighbor output details

Field	Description
OSPF process	OSPF process identifier.
Neighbor ID	OSPF router identifier of the neighbor.

Table 1-134: OSPF neighbor output details

Field	Description
Pri	OSPF priority of the neighbor.
State	State of the OSPF neighbor: DependUpon: dummy state Down: no OSPF neighbors detected at this instant Attempt: in an NBMA environment, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval Init: hello packet received, but the receiving router's ID was not included in the hello packet 2-Way: bi-directional communication established between two routers ExStart: master and slave roles determined Exchange: database description packets (DBD) sent Loading: exchange of LSRs (link state request) and LSUs (link state update) packets Full: routers fully adjacent with each other.
Dead Time	If a new Hello is not received within this duration, the neighbor is declared dead.
Address	IP address of neighbor’s interface attached to the network.
Interface	The interface attached to the network on which the neighbor is located.
Instance ID	Instance identifier for the session.

Example: Detail Parameter

This is sample output from the command when the `detail` parameter is specified:

```
#show ip ospf neighbor detail
 Neighbor 10.10.10.50, interface address 10.10.10.50
 In the area 0.0.0.0 via interface eth0
 Neighbor priority is 1, State is Full, 5 state changes
 DR is 10.10.10.50, BDR is 10.10.10.10
 Options is 0x42 (*|O|-|-|-|-|E|-)
 Dead timer due in 00:00:38
 Neighbor is up for 00:53:07
 Database Summary List 0
 Link State Request List 0
 Link State Retransmission List 0
 Crypt Sequence Number is 0
 Thread Inactivity Timer on
 Thread Database Description Retransmission off
```

OSPF Neighbor Detail Fields

Table 1-135 explains the fields for each neighbor detail entry.

© 2021 IP Infusion Inc. Proprietary

Table 1-135: OSPF neighbor output detail

Field	Description
Neighbor	OSPF router identifier of the neighbor.
interface address	IP address of the neighbor interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	OSPF priority of the neighbor.
State	OSPF state as explained in Table 1-134.
state changes	Number of state changes since the neighbor was created.
Hello is suppressed	Hello suppression is enabled.
Poll interval	Poll timer value.
DR is	Router ID of the designated router for the interface.
BDR is	Router ID of the backup designated router for the interface.
Options	LSA options as explained in Table 1-124.
LLS Options	LSDB Resynchronization (LR) Restart Signal (RS-bit) Whether link-local signalling (LLS) and out-of-band (OOB) link-state database resynchronization are performed for nonstop forwarding (NSF).
OOB-Resync in progress (receiver)/last OOB-Resync	Last successful OOB resynchronization with the NSF-capable neighbor. The router waits before taking a neighbor adjacency down if the OOB resynchronization has not taken place since the time a restart signal (Hello packet with RS-bit set) was received from the neighbor.
Dead timer due in	Expected time before declaring the neighbor dead.
Poll due in	Poll timer thread.
Neighbor is up for	Time since the neighbor went into the two-way state.
Database Summary List	Number of LSAs in the neighbor’s database.
Link State Request List	Number of LSAs that need to be received from this neighbor to synchronize the neighbors' topological databases.
Link State Retransmission List	Number of advertisements flooded out an adjacency. To ensure flooding is reliable, advertisements are retransmitted until they are acknowledged.
Crypt Sequence Number is	MD5 cryptographic sequence number.
Thread Inactivity Timer	Off if hello suppression is enabled, on otherwise.
Thread Database Description Retransmission	Off if hello suppression is enabled, on otherwise.
Thread Link State Request Retransmission	Off if hello suppression is enabled, on otherwise.

Table 1-135: OSPF neighbor output detail (Continued)

Field	Description
Thread Link State Update Retransmission	Off if hello suppression is enabled, on otherwise.
Thread Poll Timer	Whether the poll timer thread is on.
Bidirectional Forwarding Detection is enabled	Status of BFD, enabled or disabled.

Example: Hello-Suppression Option

This is sample output from the command when the `detail` parameter is specified and Hello-Suppression is enabled:

```
#sh ip os neighbor detail
 Neighbor 1.1.1.1, interface address 14.1.1.1
    In the area 0.0.0.0 via interface p7p1
    Neighbor priority is 1, State is Full, 5 state changes
    Hello is suppressed
    DR is 0.0.0.0, BDR is 0.0.0.0
    Options is 0x62 (-|O|DC|-|-|-|E|-)
    Dead timer due in inactive
    Neighbor is up for 00:05:03
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Crypt Sequence Number is 0
    Thread Inactivity Timer off
    Thread Database Description Retransmission off
    Thread Link State Request Retransmission off
    Thread Link State Update Retransmission off
```


© 2021 IP Infusion Inc. Proprietary

show ip ospf route

Use this command to display the OSPF routing table.

Command Syntax

```
show ip ospf (<0-65535>|) route ( A.B.C.D |A.B.C.D/M |summary |)
show ip ospf (<0-65535>|) route ( A.B.C.D |A.B.C.D/M |summary | fast-reroute |)
```

Parameters

`<0-65535>`	Router process identifier.
`A.B.C.D`	Single route.
`A.B.C.D/M`	Single exact match route.
`summary`	Route counts.
`fast-reroute`	Fast-reroute routes.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip ospf route
OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
C 50.0.0.0/24 [10] is directly connected, eth1, Area 0.0.0.10
C 60.0.0.0/24 [10] is directly connected, eth3, Area 0.0.0.10
OSPF process 15:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
C 80.0.0.0/24 [1] is directly connected, eth4, Area 0.0.0.15
```

Header

Each entry in this table has a code preceding it indicating the source of the routing entry.

Table 1-136 explains the fields of route codes.

Table 1-136: route codes

Code	Meaning	Description
C	connected	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from routing protocols.
O	OSPF	Modifiers: IA - OSPF inter area N1 - OSPF NSSA external type 1 N2 - OSPF NSSA external type 2 E1 - OSPF external type 1 E2 - OSPF external type 2
D	discard	An ABR or ASBR performing summarization installs a discard route in its routing table for the summarized network range to prevent routing loops where portions of the summarized network range do not have a more specific route in the RIB. External and internal discard route entries are installed by default. During route summarization, routing loops can happen if data sent to a nonexisting network appears to be a part of the summary, and the router doing the summarization has a less specific route that points back to the sending router for the network.

Route Entry Fields

Table 1-137 shows the route entry fields.

Table 1-137: route entry output details

Field	Description
Codes	As explained in Table 1-136.
IP address	IP address of the remote network.
Metric	For OSPF the metric is cost, which indicates the best quality path to use to forward packets.
Next hop router IP address	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Outgoing interface name	Interface used to get to the next-hop address for this route.
Area	OSPF area identifier

Example: Process Identifier

The following is a sample output with the process identifier parameter.

```
#show ip ospf 10 route
OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
C 50.0.0.0/24 [10] is directly connected, eth1, Area 0.0.0.10
C 60.0.0.0/24 [10] is directly connected, eth3, Area 0.0.0.10
```


© 2021 IP Infusion Inc. Proprietary

show ip ospf valid

Use this command to display information about opaque LSAs.

Command Syntax

```
show ip ospf (<0-65535>|) opaque-link valid
```

Parameters

`<0-65535>`	The ID of the router process for which information will be displayed.
`opaque-link`	Displays information about the opaque link-local LSAs.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip ospf 1 opaque-link valid
```

show ip ospf virtual-links

Use this command to display virtual link information.

Command Syntax

```
show ip ospf (<0-65535>|) virtual-links (brief|)
```

Parameters

`<0-65535>`	The ID of the router process for which information will be displayed.
`brief`	Display summary of OSPF virtual-links.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is the display of the virtual link information for two routers, one with the virtual link up and one with virtual link down.

```
ospfd#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
 Transit area 0.0.0.1 via interface eth0
 Transmit Delay is 1 sec, State Point-To-Point,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:02
 Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
 Transit area 0.0.0.1 via interface *
 Transmit Delay is 1 sec, State Down,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in inactive
 Adjacency state Down
```

The following is the display of the virtual link information for two routers, one with the virtual link up and one with virtual link down when flood reduction is enabled

```
ospfd#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
 Transit area 0.0.0.1 via interface eth0
 Transmit Delay is 1 sec, State Point-To-Point,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:02
 Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
 Transit area 0.0.0.1 via interface *
 Transmit Delay is 1 sec, State Down,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in inactive
 Adjacency state Down
```


© 2021 IP Infusion Inc. Proprietary

```
    DoNotAge LSA Allowed
```

If Hello-Suppression is enabled

```
    M1#sh ip os virtual-links
    Virtual Link VLINK0 to router 3.3.3.3 is up
      Transit area 0.0.0.1 via interface p8p1
      Hello suppression enabled
      DoNotAge LSA allowed
      Local address 15.1.1.1/32
      Remote address 15.1.1.2/32
      Transmit Delay is 1 sec, State Point-To-Point,
      Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
        Hello due in inactive
      No authentication
        Adjacency state Full
    M1#
```

Table 1-138 explains the fields for each virtual-links entry.

Table 1-138: show ip ospf virtual-links output details

Field	Description
Virtual Link	Virtual link name, the router ID to which it is connected, and the state of the link.
Transit area	Transit area ID, the interface it uses, and its instance ID – an Instance ID should default to 0. It is only necessary to assign a value other than 0 on those links that will contain multiple separate communities of OSPF routers.
Local address	The local IP address and subnet mask.
Remote address	The remote IP address and subnet mask.
Transmit Delay	The delay, in seconds, between link-state transmits. This value must be the same for all nodes on the network. The range is 0 to 65535. The default is 1. The state is point-to-point.
Timer intervals configured	The configured values in seconds of the following timers: Hello, Dead, Wait, Retransmit.
Hello due in	A countdown timer that indicates when the next Hello packet should arrive.
Adjacency State	Whether the adjacency state is either up or down.

show ip protocols

Use this command to display OSPF process parameters and statistics.

Command Syntax

```
show ip protocols
show ip protocols ospf
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This is an example of the output from the `show ip protocols` command:

```
#show ip protocols
Routing Protocol is "ospf 200"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is
 Redistributed kernel filtered by filter1
  Incoming update filter list for all interfaces is
  Redistributing: kernel
  Routing for Networks:
 192.30.30.0/24
 192.40.40.0/24
  Routing Information Sources:
 GatewayDistanceLast Update
  Distance: (default is 110)
 AddressMaskDistance List
```

Table 1-139 explains the fields for each ip protocol entry.

Table 1-139: show ip protocols output details

Field	Description
Routing Protocol is "ospf 200"	Specifies the routing protocol used.
Invalid after 0 seconds	Specifies the value of the invalid parameter.
Hold down 0	Specifies the current value of the hold-down parameter.
Flushed after 0	Specifies the time in seconds after which the individual routing information will be thrown (flushed) out.
Outgoing update	Specifies whether the outgoing filtering list has been set.

© 2021 IP Infusion Inc. Proprietary

Table 1-139: show ip protocols output details

Field	Description
Incoming update	Specifies whether the incoming filtering list has been set.
Redistributing	Lists the protocol that is being redistributed.
Routing for Networks	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the IP Infusion software is using to build its routing table.

show ip route fast-reroute

Use this command to display routes with alternate next hops.

Command Syntax

```
show ip route fast-reroute
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip route fast-reroute
```


© 2021 IP Infusion Inc. Proprietary

shutdown

Use the this command to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away.

Use the no parameter of this command.

Command Syntax

```
shutdown
no shutdown
```

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#shutdown

#configure terminal
(config)#router ospf 100
(config-router)#no shutdown
```

snmp restart ospf

Use this command restart SNMP in OSPF

Command Syntax

```
snmp restart ospf
```

Parameter

None

Default

By default, SNMP resart is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart ospf
```


© 2021 IP Infusion Inc. Proprietary

summary-address

Use this command to summarize or suppress external routes with the specified address range.

Use the `no` option with this command to disable summary address.

An address range is a pairing of an address and a mask that is almost the same as IP network number. For example, if the specified address range is 192.168.0.0/255.255.240.0, it matches 192.168.1.0/24, 192.168.4.0/22, 192.168.8.128/25 and so on.

Redistributing routes from other protocols into OSPF requires the router to advertise each route individually in an external LSA. Use this command to advertise one summary route for all redistributed routes covered by a specified network address and mask. This minimizes the size of the OSPF link state database.

Command Syntax

```
summary-address (A.B.C.D/M | A.B.C.D A.B.C.D) (not-advertise|tag <0-4294967295>|)
no summary-address (A.B.C.D/M | A.B.C.D A.B.C.D) (not-advertise|tag)
```

Parameters

`A.B.C.D/M`	The range of addresses given as IPv4 starting address and a mask.
`A.B.C.D`	IP summary prefix e.g. i.i.i.i
`A.B.C.D`	IP summary prefix mask e.g. m.m.m.m
`not-advertise`	Suppress routes that match the range.
`tag`	Tag value to use as a “match” value for controlling redistribution via route maps.
`<0-4294967295>`	Set a tag value.

Default

By default, tag value is 0

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example uses the `summary-address` command to aggregate external LSAs that match the network 172.16.0.0/24 and assign a tag value of 3.

```
#configure terminal
(config)#router ospf 100
(config-router)#summary-address 172.16.0.0/16 tag 3
```

timers lsa arrival

This command sets the minimum interval to accept the same link-state advertisement (LSA) from OSPF neighbors.

Use the `no` form of this command to restore the default value.

Command Syntax

```
timers lsa arrival <0-600000>
no timers lsa arrival
```

Parameters

`<0-600000>`	The minimum delay in milliseconds between accepting the same LSA from neighbors.

Default

By default, Minimum LSA Arrival timer is 1 sec.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#timers lsa arrival 5000
```


© 2021 IP Infusion Inc. Proprietary

timers spf exp

Use this command to set the Shortest-Path First (SPF) best-path schedule minimum and maximum delay between receiving a change to SPF calculation in milliseconds.

Use no parameter of this command to unset the SPF best-path schedule.

Command Syntax

```
timers spf exp <0-2147483647> <0-2147483647>
no timers spf exp
```

Parameters

<0-2147483647>	The minimum delay in milliseconds between receiving a change to SPF calculation.
<0-2147483647>	The maximum delay in milliseconds between receiving a change to SPF calculation.

Default

Default minimum delay: 500 milliseconds

Default maximum delay: 50000 milliseconds (50 seconds)

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#timers spf exp 300 300
```

timers throttle lsa

This command sets the rate-limiting intervals for OSPF link-state advertisement (LSA) generation.

Use the `no` form of this command to restore the default values.

Command Syntax

```
timers throttle lsa all <0-600000> <1-600000> <1-600000>
no timers throttle lsa all
```

Parameters

`<0-600000>`	Start interval: The minimum delay in milliseconds for the generation of LSAs. The first instance of LSA is always generated immediately upon a local OSPF topology change. The generation of the next LSA is not before the start interval.
`<0-600000>`	Hold interval: The hold time in milliseconds. This value is used to calculate the subsequent rate limiting times for LSA generation.
`<0-600000>`	Maximum interval: The maximum wait time in milliseconds between generation of the same LSA.

Defaults

Default start interval: 0 milliseconds

Default hold interval: 5000 milliseconds

Default maximum interval: 5000 milliseconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#timers throttle lsa all 200 10000 45000
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 OSPFv3 Commands

This chapter provides an alphabetized reference for each of the OSPFv3 commands. It includes the following commands:

- abr-type
- area default-cost
- area nssa
- area range
- area stub
- area virtual-link
- auto-cost reference bandwidth
- bfd all-interfaces
- capability restart
- clear ipv6 ospf process
- debug ipv6 ospf
- debug ipv6 ospf bfd
- debug ipv6 ospf events
- debug ipv6 ospf ifsm
- debug ipv6 ospf lfa
- debug ipv6 ospf lsa
- debug ipv6 ospf nfsm
- debug ipv6 ospf nsm
- debug ipv6 ospf packet
- debug ipv6 ospf retransmission
- debug ipv6 ospf rib
- debug ipv6 ospf route
- default-information originate
- default-metric
- distance
- distribute-list
- enable db-summary-opt
- fast-reroute keep-all-paths
- fast-reroute tie-break
- ipv6 ospf bfd
- ipv6 ospf cost
- ipv6 ospf dead-interval
- ipv6 ospf display route single-line
- ipv6 ospf link-lsa-suppression
- ipv6 ospf mtu-ignore

© 2021 IP Infusion Inc. Proprietary

- ipv6 ospf neighbor
- ipv6 ospf network
- ipv6 ospf priority
- ipv6 ospf restart grace-period
- ipv6 ospf restart helper
- ipv6 ospf restart planned-only
- ipv6 ospf retransmit-interval
- ipv6 ospf transmit-delay
- ipv6 router ospf
- ipv6 te-metric
- log-adjacency-changes
- max-concurrent-dd
- passive-interface
- redistribute
- restart ipv6 ospf graceful
- router-id
- router ipv6 ospf
- show debugging ipv6 ospf
- show ipv6 ospf
- show ipv6 ospf database
- show ipv6 ospf interface
- show ipv6 ospf neighbor
- show ipv6 ospf route
- show ipv6 route fast-reroute
- show ipv6 ospfv3 topology
- show ipv6 ospf virtual-links
- show ipv6 vrf
- shutdown
- snmp restart ospf6
- summary-address
- timers spf exp

© 2021 IP Infusion Inc. Proprietary

abr-type

Use this command to set an OSPFv3 Area Border Router (ABR) type.

Use the `no` parameter with this command to revert the ABR type to the default setting (`cisco`).

Specifying the ABR type allows better functioning in a multi-vendor environment. The ABR types are:

- Cisco (RFC 3509): A router is considered an ABR if it has more than one area actively attached and one of them is the backbone area.
- IBM (RFC 3509): A router is considered an ABR if it has more than one area actively attached and the backbone area is configured. In this case the configured backbone need not be actively connected.
- Standard (RFC 2328): A router is considered an ABR if it has more than one area actively attached to it.

Command Syntax

```
abr-type (cisco|ibm|standard)
no abr-type
```

Parameters

`cisco`	Specify an alternative ABR using Cisco implementation. This is the default ABR type.
`ibm`	Specify an alternative ABR using IBM implementation.
`standard`	Specify a standard ABR.

Default

By default, ABR type is Cisco

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#abr-type standard
```

area default-cost

Use this command to specify the cost for default summary route sent into a stub or a NSSA area. If an area is configured as a stub, the OSPFv3 router originates one type-3 inter-area-prefix-LSA into the stub area. This command changes the metric for this LSA.

Use the `no` parameter with this command to remove the assigned default cost.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) default-cost (<0-16777215>)
no area (A.B.C.D|<0-4294967295>) default-cost
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`<0-16777215>`	The advertised cost for the default summary route used for a stub or NSSA area.

Default

By default, advertised cost for the default summary route is 1.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#area 1 default-cost 10
```


© 2021 IP Infusion Inc. Proprietary

area nssa

Use this command to set an area as a Not-So-Stubby-Area (NSSA). There are no external routes in an OSPF stub area, so you cannot redistribute from another protocol into a stub area. An NSSA allows external routes to be flooded within the area. These routes are then leaked into other areas. However, the external routes from other areas still do not enter the NSSA. You can configure an area to be a stub area or an NSSA, but not both.

This command simplifies administration when connecting a central site using OSPF to a remote site that is using a different routing protocol. You can extend OSPF to cover the remote connection by defining the area between the central router and the remote router as a NSSA.

Use the `no` form of this command to make an area a normal area.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) nssa
area (A.B.C.D|<0-4294967295>) nssa {translator-role (candidate|always)|stability-
  interval <0-2147483647>|no-redistribution|default-information-originate (metric
  <0-16777214>|metric-type <1-2>|)|no-summary}
no area (A.B.C.D|<0-4294967295>) nssa
no area (A.B.C.D|<0-4294967295>) nssa {translator-role|stability-interval|no-
  redistribution|default-information-originate|no-summary}
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`translator-role`	NSSA-ABR translator role:
`candidate`	Translate NSSA-LSA to Type-5 LSA if router is elected.
`always`	Always translate NSSA-LSA to Type-5 LSA.
`stability-interval`	Stability timer for a NSSA area. If an elected translator determines its services are no longer required, it continues to perform its duties for this time interval. This minimizes excess flushing of translated Type-7 LSAs and provides a more stable translator transition.
`<0-4294967295>`	Stability interval in seconds.
`no-redistribution`	Do not redistribute into the NSSA.
`default-information-originate`	Originate Type-7 default LSA into the NSSA.
`metric`	Specify metric for default routes.
`<0-16777214>`	Specify metric value.
`metric-type`	Specify metric type (see RFC 3101).

<1-2>	Specify metric type: 1: Type 1 external route 2: Type 2 external route
no-summary	Do not inject inter-area routes into the NSSA.
translate-candidate	Translate NSSA-LSA to Type-5 LSA if router is elected.
translate-always	Always translate NSSA-LSA to Type-5 LSA.

Default

By default, the nssa option value is candidate.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router ipv6 ospf
(config-router)#area 3 nssa translator-role candidate no-redistribution
default-information-originate metric 34 metric-type 2
```


© 2021 IP Infusion Inc. Proprietary

area range

Use this command to configure the OSPF address range. This command summarizes intra-area routes for an area. The single summary route is then advertised to other areas by the Area Border Routers (ABRs). Routing information is condensed at area boundaries and outside the area. If the network numbers in an area are assigned in a way such that they are contiguous, the ABRs can be configured to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

Use the `no` parameter with this command to remove the assigned area range.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) range X:X::X:X/M
area (A.B.C.D|<0-4294967295>) range X:X::X:X/M (not-advertise|)
no area (A.B.C.D|<0-4294967295>) range X:X::X:X/M (not-advertise|)
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`X:X::X:X/M`	The area IPv6 range prefix and length.
`not-advertise`	Does not advertise this range.

Default

By default, OSPF address range is advertised.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#area 1 range 2000::/3
```

area stub

Use this command to define an area as a stub area on all routers. There are two stub area router configuration commands: the `stub` and commands. In all routers attached to the stub area, configure the area by using the `stub` option of the area command. For an area border router (ABR) attached to the stub area, use the `area` command.

Use the `no` form of this command to make an area a normal area.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) stub
area (A.B.C.D|<0-4294967295>) stub no-summary
no area (A.B.C.D|<0-4294967295>) stub
no area (A.B.C.D|<0-4294967295>) stub no-summary
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`no-summary`	Stops an ABR from sending summary link advertisements into the stub area.

Default

No stub area is defined.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#area 1 stub no-summary
```


© 2021 IP Infusion Inc. Proprietary

area virtual-link

Use this command to configure a link between two backbone areas that are physically separated through other nonbackbone areas.

Use the `no` parameter with this command to remove the virtual link.

In OSPFv3, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection.You can configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these two routers joined by a virtual link as if they were connected by an unnumbered point-to-point network.

Configure the `hello-interval` to be the same for all routers attached to a common network. If the `hello-interval` is short, the router detects topological changes faster, but more routing traffic follows.

The `retransmit-interval` is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The `transmit-delay` is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet are increased by this amount. Set the transmit-delay to be greater than zero. Also, take into account the transmission and propagation delays for the interface.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D fall-over bfd
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D (dead-interval <1-65535>|hello-
  interval <1-65535>|retransmit-interval <1-1800>|transmit-delay <1-1800>)
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D instance-id (<0-31>|<64-95>)
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D fall-over bfd
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D (dead-interval|hello-
  interval|retransmit-interval|transmit-delay)
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D instance-id
```

Parameters

`A.B.C.D`	OSPF Area ID in IP64 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`A.B.C.D`	Specify router ID associated with a virtual link neighbor.
`dead-interval`	The interval in seconds during which no packets are received and after which the router acknowledges a neighboring router as off-line.
`<1-65535>`	The timer interval.
`hello-interval`	The interval in seconds the router waits before it sends a hello packet.
`<1-65535>`	The timer interval.
`retransmit-interval`	The interval in seconds the router waits before it retransmits a packet.
`<1-1800>`	The timer interval.
`transmit-delay`	The interval in seconds the router waits before it transmits a packet.

`<1-1800>`	The timer interval.
`instance-id`	The OSPFv3 instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.
`fall-over bfd`	Fall-over Bidirectional Forwarding Detection (BFD).

Default

Default hello interval:10 seconds.

Default dead interval:40 seconds.

Default retransmit interval: 5 seconds.

Default transmit delay: 1 second

Default instance-id: 0

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#area 1 virtual-link 10.10.11.50 hello 5 dead 10
(config-router)#area 1 virtual-link 10.10.11.50 instance-id 1
(config-router)#area 1 virtual-link 10.10.11.50 fall-over bfd
```


© 2021 IP Infusion Inc. Proprietary

auto-cost reference bandwidth

Use this command to control how OSPFv3 calculates default metrics for the interface.

By default, OSPFv3 calculates the OSPFv3 metric for an interface by dividing the reference bandwidth by the interface bandwidth. The auto-cost command is used to differentiate high bandwidth links. For multiple links with high bandwidth, specify a larger reference bandwidth value to differentiate cost on those links.

Use the `no` form of this command to assign cost based only on the interface bandwidth.

Command Syntax

```
auto-cost reference-bandwidth <1-4294967>
no auto-cost reference-bandwidth
```

Parameters

`<1-4294967>`	The reference bandwidth in Mbps per second.

Default

By default, reference bandwidth is 100Mbps

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example changes the reference bandwidth to 1Gbps to change the Fast Ethernet interface cost from 1 to 10.

```
#configure terminal
(config)#router ipv6 ospf 1
(config-router)#auto-cost reference-bandwidth 1000

(config)#router ipv6 ospf 1
(config-router)#no auto-cost reference-bandwidth
```

bfd all-interfaces

Use this command to enable Bidirectional Forwarding Detection (BFD) on all interfaces.

Use the `no` form of this command to disable BFD.

Command Syntax

```
bfd all-interfaces
no bfd all-interfaces
```

Parameters

None

Default

By default, BFD is disabled on all OSPF enabled interfaces.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example changes the reference bandwidth to 1Gbps to change the Fast Ethernet interface cost from 1 to 10.

```
#configure terminal
(config)#router ipv6 ospf 1
(config-router)#bfd all-interfaces
```


© 2021 IP Infusion Inc. Proprietary

capability restart

Use this command to enable OSPFv3 graceful restart capability. If a router is not restart-enabled, it cannot enter graceful restart mode and act as a helper.

Use the `no` parameter with this command to disable the feature.

Command Syntax

```
capability restart graceful
```

```
no capability restart
```

Parameter

None

Default

By default, capability restart graceful is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf 100
(config-router)#capability restart graceful

(config)#router ipv6 ospf 100
(config-router)#no capability restart
```

clear ipv6 ospf process

Use this command to clear and restart all OSPFv3 routing processes or a given OSPFv3 routing process.

Command Syntax

```
clear ipv6 ospf (WORD|) process
```

Parameters

WORD	OSPFv3 process tag.

Command Mode

Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ipv6 ospf Tag1 process
```


© 2021 IP Infusion Inc. Proprietary

debug ipv6 ospf

Use this command to specify all debugging options for OSPFv3.

Use the `no` form of this command to disable the options.

Command Syntax

```
debug ipv6 ospf (all|bfd|events|ifsm|lsa|nfsm|nsm|packet|retransmission|rib|route|)

no debug ipv6 ospf
  (all|bfd|events|ifsm|lsa|nfsm|nsm|packet|retransmission|rib|route|)
undebug ipv6 ospf (all|bfd|events|ifsm|lsa|nfsm|nsm|packet|rib|route)
no debug all ipv6 ospf
undebug all ipv6 ospf
no debug all
undebug all
```

Parameters

`all`	Enables all debugging information.
`bfd`	Debug OSPFv3 Bidirectional Forwarding Detection. (see debug ipv6 ospf bfd)
`events`	Debug OSPFv3 events (see debug ipv6 ospf events).
`ifsm`	Debug OSPFv3 Interface State Machines (see debug ipv6 ospf ifsm).
`lsa`	Debug OSPFv3 Link State Advertisements (see debug ipv6 ospf lsa).
`nfsm`	Debug OSPFv3 Neighbor State Machines (see debug ipv6 ospf nfsm).
`nsm`	Debug OSPFv3 NSM information (see debug ipv6 ospf nsm).
`packet`	Debug OSPFv3 packets (see debug ipv6 ospf packet).
`retransmission`	Debug OSPFv3 retransmission information. (see debug ipv6 ospf retransmission)
`rib`	Debug OSPFv3 Routing Information Base.(see debug ipv6 ospf rib)
`route`	Debug OSPFv3 route information (see debug ipv6 ospf route).

Command Mode

Privileged Exec and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf all
```

debug ipv6 ospf bfd

Use this command to specify the debugging options for OSPFv3 Bidirectional Forwarding Detection

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf bfd
no debug ipv6 ospf bfd
undebug ipv6 ospf bfd
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf bfd
```


© 2021 IP Infusion Inc. Proprietary

debug ipv6 ospf events

Use this command to display debug information related to OSPF internal events. Use this command without parameters to turn on all the options.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf events {(abr|asbr|os|router|vlink|nssa)|}
no debug ipv6 ospf events {(abr|asbr|os|router|vlink|nssa)|}
undebug ipv6 ospf events {(abr|asbr|os|router|vlink|nssa)|}
```

Parameters

`abr`	Debug ABR events
`asbr`	Debug ASBR events
`os`	Debug OS interaction events
`router`	Debug other router events
`vlink`	Debug virtual link events
`nssa`	Debug NSSA events

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#no debug ipv6 ospf events abr
#debug ipv6 ospf events asbr
```

debug ipv6 ospf ifsm

Use this command to specify debugging options for OSPFv3 Interface Finite State Machine (IFSM) troubleshooting.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf ifsm ({events|status|timers}|)
no debug ipv6 ospf ifsm ({events|status|timers}|)
undebug ipv6 ospf ifsm ({events|status|timers}|)
```

Parameters

`events`	Debug IFSM event information.
`status`	Debug IFSM status information.
`timers`	Debug IFSM timer information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf ifsm status
```


© 2021 IP Infusion Inc. Proprietary

debug ipv6 ospf lfa

Use this command to specify the debugging options for OSPFv3 Loop-free Alternate path

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf lfa
no debug ipv6 ospf lfa
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf lfa
```

debug ipv6 ospf lsa

Use this command to specify the debugging options for OSPFv3 Link State Advertisements (LSAs).

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf lsa {(generate|flooding|install|maxage|refresh)|}
no debug ipv6 ospf lsa {(generate|flooding|install|maxage|refresh)|}
undebug ipv6 ospf lsa {(generate|flooding|install|maxage|refresh)|}
```

Parameters

`generate`	Debug LSA generation.
`flooding`	Debug LSA flooding.
`install`	Debug LSA installation.
`maxage`	Debug the maximum age processing.
`refresh`	Debug LSA refresh.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf lsa
```


© 2021 IP Infusion Inc. Proprietary

debug ipv6 ospf nfsm

Use this command to specify debugging options for OSPFv3 Neighbor Finite State Machines (NFSMs).

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf nfsm {(events|status|timers)|}
no debug ipv6 ospf nfsm {(events|status|timers)|}
undebug ipv6 ospf nfsm {(events|status|timers)|}
```

Parameters

`events`	Debug NFSM event information.
`status`	Debug NFSM status information.
`timers`	Debug NFSM timer information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf nfsm events
#no debug ipv6 ospf nfsm timers
```

debug ipv6 ospf nsm

Use this command to specify the debugging options for OSPFv3 NSM information.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf nsm {(interface|redistribute)|}
no debug ipv6 ospf nsm {(interface|redistribute)|}
undebug ipv6 ospf nsm {(interface|redistribute)|}
```

Parameters

`redistribute`	Debug redistribute.
`interface`	Debug the NSM interface.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf nsm interface
```


© 2021 IP Infusion Inc. Proprietary

debug ipv6 ospf packet

Use this command to specify the packet debugging options for OSPFv3 information.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)


no debug ipv6 ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|
  detail}|)
undebug ipv6 ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)
```

Parameters

`hello`	Debug OSPFv3 hello.
`dd`	Debug OSPFv3 database description.
`ls-request`	Debug OSPFv3 link state request.
`ls-update`	Debug OSPFv3 link state update.
`ls-ack`	Debug OSPFv3 link state acknowledgment.
`send`	Debug packets sent
`recv`	Debug packets received.
`detail`	Debug detail information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf packet ls-request
```

debug ipv6 ospf retransmission

Use this command to specify the debugging options for OSPFv3 retransmission information.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf retransmission
no debug ipv6 ospf retransmission
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf retransmission
```


© 2021 IP Infusion Inc. Proprietary

debug ipv6 ospf rib

Use this command to specify the debugging options for OSPFv3 RIB information.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf rib {(interface|redistribute)|}

no debug ipv6 ospf rib {(interface|redistribute)|}
undebug ipv6 ospf rib {(interface|redistribute)|}
```

Parameters

`redistribute`	Debug redistribute.
`interface`	Debug the NSM interface.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ipv6 ospf rib interface
```

debug ipv6 ospf route

Use this command to specify which route calculation to debug. Use this command without parameters to turn on all the options.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf route {(ase|ia|install|spf)|}
no debug ipv6 ospf route {(ase|ia|install|spf)|}
undebug ipv6 ospf route {(ase|ia|install|spf)|}
```

Parameters

`ase`	Debug external route calculations.
`ia`	Debug inter-area route calculations.
`install`	Debug the route installation.
`spf`	Debug the SPF calculation.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#no debug ipv6 ospf route
#debug ipv6 ospf route ia
```


© 2021 IP Infusion Inc. Proprietary

default-information originate

Use this command to create a default external route into an OSPF routing domain.

The system acts like an Autonomous System Boundary Router (ASBR) when you use the `default-information originate` command to redistribute routes into an OSPF routing domain. An ASBR does not by default generate a default route into the OSPF routing domain.

When you give the `default-information originate` command, also specify a `route-map` to avoid a dependency on the default network in the routing table.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
default-information originate
default-information originate {metric <0-16777214>|metric-type (1|2)|route-map
  WORD|always}
no default-information originate
no default-information originate {metric|metric-type|route-map|always}
```

Parameters

`always`	Used to advertise the default route regardless of whether there is a default route.
`metric`	Sets the OSPF metric used in creating the default route.
`<0-16777214>`	Sets the OSPF metric used in creating the default route. The value used is specific to the protocol.
`metric-type`	The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).
`1`	Sets OSPF External Type 1 metric.
`2`	Sets OSPF External Type 2 metric (default).
`route-map`	Route map.
`WORD`	Specify the name of route map.

Default

Sets the OSPF metric used in creating the default route. The default metric value is 20. The value used is specific to the protocol. metric-type The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).

By default, 2 sets OSPF External Type 2 metric

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#default-information originate always metric 23 metric-type 2
route-map myinfo

(config)#router ipv6 ospf
(config-router)#no default-information originate metric metric-type route-map
```


© 2021 IP Infusion Inc. Proprietary

default-metric

Use this command to set a default metric for OSPF.

A default metric facilitates redistributing routes with incompatible metrics. If the metrics do not convert, the default metric provides an alternative. Use this command to use the same metric value for all redistributed routes. Use this command in conjunction with the redistribute command.

Use the `no` parameter with this command to return to the default state.

Command Syntax

```
default-metric <1-16777214>
no default-metric
```

Parameter

`<1-16777214>`	Default metric value.

Default

Default metric for redistributed routes will be 20.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#default-metric 100
```

distance

Use this command to define OSPFv3 route administrative distances based on route type. This command sets the distance for an entire group of routes rather than a specific route that passes an access list.

The administrative distance rates the trustworthiness of a routing information source. A higher distance value means a lower trust rating. For example, an administrative distance of 254 means that the routing information source cannot be trusted and should be ignored.

Use the `no` form of this command to restore the default value.

Command Syntax

```
distance <1-254>
distance ospfv3 {intra-area <1-254>|inter-area <1-254>|external <1-254>}
no distance (<1-254>|)
no distance ospfv3
```

Parameters

`<1-254>`	Used alone, this parameter specifies a default administrative distance used when no other specification exists for a routing information source.
`intra-area`	Routes within an area.
`<1-254>`	Distance for all routes within an area
`inter-area`	Routes from one area to another area.
`<1-254>`	Distance for all routes from one area to another area.
`external`	Routes from other routing domains learned by redistribution.
`<1-254>`	Distance for routes from other routing domains learned by redistribution.

Default

By default, distance value for each type of route is 110

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ipv6 ospf 100
(config-router)#distance ospfv3 inter-area 20 intra-area 10 external 40
```


© 2021 IP Infusion Inc. Proprietary

distribute-list

Use this command to filter networks in routing updates. This command redistributes other routing protocols into the OSPF routing table.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
distribute-list WORD out ((kernel|connected|static|rip|bgp|isis|ospf (WORD|<1-
  65535>|)))
distribute-list WORD in
no distribute-list WORD out ((kernel|connected|static|rip|bgp|isis|ospf (WORD|<1-
  65535>|)))
no distribute-list WORD in
```

Parameters

`WORD`	Specify the name of the access list.
`in`	Filter incoming routing updates.
`out`	Filter outgoing routing updates.
`kernel`	Specify kernel routes.
`connected`	Specify connected routes.
`static`	Specify static routes.
`rip`	Specify RIP routes.
`bgp`	Specify BGP routes.
`isis`	Specify IS-IS routes.
`ospf`	Specify OSPF routes.
`WORD`	Specify the OSPF process tag. If not specified, redistribute OSPF process with tag "null".
`<1-65535>`	Specify OSPF process ID <1-65535>. If not specified, redistribute OSPF instance with process ID 0.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the distribution of BGP routing updates based on the access list `list1` (network 172.10.0.0).

```
#configure terminal
(config)#access-list list1 permit 172.10.0.0/16
```

```
(config)#router ipv6 ospf 100
(config-router)#distribute-list list1 out bgp
(config-router)#redistribute bgp
```


© 2021 IP Infusion Inc. Proprietary

enable db-summary-opt

Use this command to enable the database summary list optimization for OSPFv3.

When this feature is enabled, the database exchange process is optimized by removing the LSA from the database summary list for the neighbor if the LSA instance in the summary list is the same as or less recent than the LSA in the database description packet received from the neighbor.

Use the `no` form of the command to disable database summary list optimization.

Command Syntax

```
enable db-summary-opt
```

```
no enable db-summary-opt
```

Parameters

None

Default

By default, db summary opt is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#enable db-summary-opt
(config-router)#no enable db-summary-opt
```

fast-reroute keep-all-paths

Use this command to enable fast rerouting on all OSPFv3 interfaces.

Use the `no` parameter with this command to disable fast rerouting.

Command Syntax

```
fast-reroute keep-all-paths
no fast-reroute keep-all-paths
```

Parameters

None

Defaults

By default, fast rerouting is disabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf 200
(config-router)#fast-reroute keep-all-paths
```


© 2021 IP Infusion Inc. Proprietary

fast-reroute tie-break

Use this command to set the tie-breaking policy for selecting a fast reroute repair path. You assign a priority to each type of repair path.

Use the `no` parameter with this command to set the tie-breaking policy for a specific type of repair path to its default priority. To set all types of repair paths to their default priorities, do not specify a repair path with the `no` form of this command.

Command Syntax

```
fast-reroute tie-break (primary-path|interface-disjoint|node-protecting|broadcast-
  interface-disjoint) index <1-4>
no fast-reroute tie-break (primary-path|interface-disjoint|node-
  protecting|broadcast-interface-disjoint) index <1-4>
no fast-reroute tie-break
```

Parameters

`primary-path`	When there are multiple loop-free alternate paths. The primary path is selected for an frr if it is node-protecting as well as link-protecting
`interface-disjoint`	Do not select point-to-point interfaces that have no alternate next hop for rerouting if the primary gateway fails, thus protecting the interface.
`node-protecting`	Bypass the `primary-path` gateway router which might not protect the router that is the next hop in the primary path.
`broadcast-interface-disjoint`	Do not use the interface if connected to a broadcast network. Repair paths protect links when a repair path and a protected primary path use *different* next-hop interfaces. However, on broadcast interfaces, if the repair path is computed via the same interface as the primary path, but their next-hop gateways are different, the router is protected but the link might not be.
`index`	Tie break priority. A lower value has higher preference.
`<1-4>`	Range of priority values.

Defaults

The default priority scheme is:

1. primary-path
2. interface-disjoint
3. node-protecting
4. broadcast-interface-disjoint

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf 200
(config-router)#fast-reroute tie-break interface-disjoint index 1
```


© 2021 IP Infusion Inc. Proprietary

ipv6 ospf bfd

Use this command to enable Bidirectional Forwarding Detection (BFD).

Use this command with either the no or disable parameter to disable BFD.

Command Syntax

```
ipv6 ospf bfd (disable|)
ipv6 ospf bfd (disable|)instance-id (<0-31>|<64-95>)
no ipv6 ospf bfd (disable|)
no ipv6 ospf bfd (disable|)instance-id (<0-31>|<64-95>)
```

Parameters

`disable`	Specify to disable BFD.
`instance-id`	Specify the instance. Default value for instance-id is 0.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast

Default

By default, IPv6 OSPF BFD is disabled. Default value for instance-id is 0.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 ospf bfd instance-id 2
```

Note: Interface level CLI: "ipv6 ospf bfd" will be displayed as "ipv6 ospf bfd instance-id 0" from 5.0 release.

ipv6 ospf cost

Use this command to specify the link-cost described in LSAs.

The cost (or metric) of an interface in OSPF indicates the overhead required to send packets across a certain interface. The value is taken to describe Link State information, and used for route calculation.

Use the `no` parameter with this command to reset the cost to default.

Command Syntax

```
ipv6 ospf cost <1-65535>
ipv6 ospf cost <1-65535> instance-id (<0-31>|<64-95>)
no ipv6 ospf cost
no ipv6 ospf cost instance-id (<0-31>|<64-95>)
```

Parameters

`cost`	Specify the link-state metric.
`<1-65535>`	Specify the link-state metric.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, ipv6 cost value is 10.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf cost 20 instance-id 1
```


© 2021 IP Infusion Inc. Proprietary

ipv6 ospf dead-interval

Use this command to set the amount of time that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down.

The dead interval is advertised in hello packets. OSPF compares the dead interval in a received packet to the dead interval configured for the receiving interface. If the intervals do not match, the hello packet is discarded.

Use the `no` parameter with this command to reset the interval to default.

Command Syntax

```
ipv6 ospf dead-interval <1-65535>
ipv6 ospf dead-interval <1-65535> instance-id (<0-31>|<64-95>)
no ipv6 ospf dead-interval
no ipv6 ospf dead-interval instance-id (<0-31>|<64-95>)
```

Parameters

`dead-interval`	Specify the interval.
`<1-65535>`	Specify the interval in seconds.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, dead interval is 40 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf dead-interval 20
```

ipv6 ospf display route single-line

Use this command to display the output of the show ipv6 ospf route command with each route entry in a single-line.

Use the `no` parameter with this command to display the output with each route entry in a multiple lines.

Command Syntax

```
ipv6 ospf display route single-line
no ipv6 ospf display route single-line
```

Parameters

None

Default

By default, show ipv6 ospf route displays routes in multiple lines

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 ospf display route single-line
```


© 2021 IP Infusion Inc. Proprietary

ipv6 ospf hello-interval

Use this command to specify the interval between `hello` packets.

The hello interval is advertised in the hello packets. An OSPF router compares the hello interval in a received packet to the interval configured for the receiving interface. If this interval does not match, the hello packet is discarded. A shorter hello interval ensures faster detection of topological changes, but results in more routing traffic.

Use the `no` parameter with this command to reset the interval to default.

Command Syntax

```
ipv6 ospf hello-interval <1-65535>
ipv6 ospf hello-interval <1-65535> instance-id (<0-31>|<64-95>)
no ipv6 ospf hello-interval
no ipv6 ospf hello-interval instance-id (<0-31>|<64-95>)
```

Parameters

`hello-interval`	Specify the interval.
`<1-65535>`	Specify the interval in seconds.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, hello interval is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf hello-interval 5 instance-id 1
```

ipv6 ospf link-lsa-suppression

Use this command to enable or disable link LSA (type 8) suppression. A type 8 LSA gives information about link-local addresses and a list of IPv6 addresses on the link.

If enabled and the interface type is *not* broadcast or NBMA, the router does not send type 8 link LSAs. This implies that other routers on the link determine the router's next-hop address using a mechanism other than the type 8 link LSA. This feature is implicitly disabled if the interface type is broadcast or NBMA.

Command Syntax

```
ipv6 ospf link-lsa-suppression (enable|disable)
ipv6 ospf link-lsa-suppression (enable|disable) instance-id (<0-31>|<64-95>)
```

Parameters

`enable`	Enable type 8 link LSA suppression
`disable`	Disable type 8 link LSA suppression (default).
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, type 8 link LSA suppression is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf link-lsa-suppression enable
```


© 2021 IP Infusion Inc. Proprietary

ipv6 ospf mtu-ignore

Use this command to configure OSPF so that it does not check the MTU size during DD (Database Description) exchange.

Use the `no` form of this command to make OSPF check the MTU size during DD exchange.

Command syntax

```
ipv6 ospf mtu-ignore
ipv6 ospf mtu-ignore instance-id (<0-31>|<64-95>)
no ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore instance-id (<0-31>|<64-95>)
```

Parameters

`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, during the DD exchange process, OSPF checks the MTU size described in DD packets received from its neighbor. If the MTU size does not match the interface MTU, the neighbor adjacency is not established. Using this command makes OSPF ignore this check and allows establishing of adjacency regardless of MTU size in the DD packet.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#interface eth1
(config-if)#ipv6 ospf mtu-ignore
```

ipv6 ospf neighbor

Use this command to connect OSPFv3 routers to non-broadcast multi-access (NBMA) networks.

One neighbor entry must be included for each known NBMA neighbor. The neighbor address must be a link-local address.

Note: For point-to-multipoint interfaces, the `cost` parameter is the only applicable option.

Use the `no` parameter with this command to remove a configuration.

Command Syntax

```
ipv6 ospf neighbor X:X::X:X (instance-id (<0-31>|<64-95>)|)
ipv6 ospf neighbor X:X::X:X {cost <1-65535>} (instance-id (<0-31>|<64-95>)|)
ipv6 ospf neighbor X:X::X:X {poll-interval <0-4294967295>|priority <0-255>}
  (instance-id (<0-31>|<64-95>)|)
no ipv6 ospf neighbor X:X::X:X ({cost|poll-interval|priority}|) (instance-id (<0-
  31>|<64-95>)|)
```

Parameters

`X:X::X:X`	Specify a neighbor IP address.
`instance-id`	Specify the instance.
`<0-255>`	Specify the instance ID.
`cost`	Cost of the interface. This parameter does not apply to NBMA networks.
`<1-65535>`	Cost of the interface.
`poll-interval`	Dead neighbor polling interval.
`<0-4294967295>`	Dead neighbor polling interval in seconds. It is recommended to set this value much higher than the hello interval.
`priority`	Specify a priority. This parameter does not apply to point-to-multipoint interfaces.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

Default cost is 10.

Default poll interval is 120 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
```


© 2021 IP Infusion Inc. Proprietary

```
(config)#interface eth0
(config-if)#ipv6 ospf neighbor 2000:500::1 cost 2 instance-id 3
```

ipv6 ospf network

Use this command to set an OSPFv3 network type.

Use the `no` option with this command to return to the default value.

Command Syntax

```
ipv6 ospf network (broadcast|non-broadcast|point-to-multipoint (non-
  broadcast|)|point-to-point) (instance-id (<0-31>|<64-95>)|)
no ipv6 ospf network (instance-id (<0-31>|<64-95>)|)
```

Parameters

`broadcast`	Sets the network type to broadcast.
`non-broadcast`	Sets the network type to NBMA.
`point-to-multipoint`	Sets the network type to point-to-multipoint.
`non-broadcast`	Sets the network type to NBMA.
`point-to-point`	Sets the network type to point-to-point.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, ipv6 ospf network is broadcast type

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to set the network to point-to-point type on the eth0 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf network point-to-point
```


© 2021 IP Infusion Inc. Proprietary

ipv6 ospf priority

Use this command to set the router priority for determining the designated router (DR) for the network.

A router with the higher router priority becomes the DR. If the priority is the same for two routers, the router with the higher router ID takes precedence.

Only routers with a nonzero priority value are eligible to become the designated or backup designated router. Configure router priority for broadcast or NBMA networks only and not for point-to-point networks.

Use the `no` parameter with this command to reset the value to default.

Command Syntax

```
ipv6 ospf priority <0-255>
ipv6 ospf priority <0-255> instance-id (<0-31>|<64-95>)
no ipv6 ospf priority instance-id (<0-31>|<64-95>)
```

Parameters

`priority`	Specify the router priority of the interface.
`<0-255>`	Specify the router priority of the interface. The default is 1.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, priority is 1

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf priority 127
```

ipv6 ospf restart grace-period

Use this command to enable the graceful restart feature and set the grace period for restarting the router.

If graceful restart is enabled, NSM is notified about the grace period. If the OSPF daemon unexpectedly shuts down, NSM sends this value to the OSPF daemon when it comes up again which uses this value to end the graceful state.

Use the `no` parameter with this command to revert to the default grace period.

Command Syntax

```
ipv6 ospf restart grace-period <2-1800>
no ipv6 ospf restart grace-period
```

Parameters

`grace-period`	Specify the grace period.
`<2-1800>`	Specify the grace period in seconds.

Default

By default, grace period is 120 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 ospf restart grace-period 250
```


© 2021 IP Infusion Inc. Proprietary

ipv6 ospf restart helper

Use this command to configure the helper behavior for graceful restart.

Use the `no` parameter with this command to revert to the default.

Command Syntax

```
ipv6 ospf restart helper {max-grace-period <2-1800>}
ipv6 ospf restart helper never (router-id A.B.C.D|)
no ipv6 ospf restart helper
no ipv6 ospf restart helper never
no ipv6 ospf restart helper {max-grace-period|never router-id (A.B.C.D|all)}
```

Parameters

`<2-1800>`	Help only if received grace-period is less than this value.
`A.B.C.D`	Router ID of neighbor to never to act as helper.
`never`	Prevent the neighbor from entering helper mode.
`max-grace-period`	Help only if received grace-period is less than this value.
`router-id`	Router of neighbor to never to act as helper.

Default

By default, router behave as helper. To disable it as helper, `ospf restart helper never` command should be configured. `ospf restart helper max-grace-period` – Max-grace-period to function as helper. If not configured, value will be the grace-period in restarting node.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 ospf restart helper never router-id 1.1.1.1

#configure terminal
(config)#no ipv6 ospf restart helper never
```

ipv6 ospf restart planned-only

Use this command to configure the OSPFv3 GR support for only planned restart.

Use the `no` parameter with this command to revert to the default.

Note: OSPFv3 supports only planned restart. Hence this command configuration and un-configuration does not have any functionality impact

Command Syntax

```
ipv6 ospf restart planned-only
```

```
no ipv6 ospf restart planned-only
```

Parameters

None

Default

By default, OSPFv3 supports planned restart only.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 ospf restart planned-only

#configure terminal
(config)#no ipv6 ospf restart planned-only
```


© 2021 IP Infusion Inc. Proprietary

ipv6 ospf retransmit-interval

Use this command to set the interval between retransmission of Link State Update packets. This interval is also used to retransmit DD packets and Link State Request packets.

After sending an LSA to a neighbor, the router keeps the LSA on the LS-retransmission list until it receives an acknowledgement. If the router does not receive an acknowledgment from the neighbor during the retransmit interval, it sends the LSA to the neighbor again.

Use the `no` parameter with this command to reset the interval to the default value.

Command Syntax

```
ipv6 ospf retransmit-interval <1-1800>
ipv6 ospf retransmit-interval <1-1800> instance-id (<0-31>|<64-95>)
no ipv6 ospf retransmit-interval
no ipv6 ospf retransmit-interval instance-id (<0-31>|<64-95>)
```

Parameters

`retransmit-interval`	
	Specify the interval.
`<1-1800>`	Specify the interval in seconds.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, ipv6 ospf retransmit interval is 5 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf retransmit-interval 3
```

ipv6 ospf transmit-delay

Use this command to set the estimated time it takes to transmit a Link State Update packet over the interface. The transmit-delay value is added to the LS age of LSAs and is advertised through this interface whenever the LSAs are transmitted.

Use the `no` parameter with this command to reset the delay to the default value.

Command Syntax

```
ipv6 ospf transmit-delay <1-1800>
ipv6 ospf transmit-delay <1-1800> instance-id (<0-31>|<64-95>)
no ipv6 ospf transmit-delay
no ipv6 ospf transmit-delay instance-id (<0-31>|<64-95>)
```

Parameters

`transmit-delay`	Specify the time to transmit a link-state update.
`<1-1800>`	Specify the time in seconds to transmit a link-state update.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, transmit delay is 1 second

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf transmit-delay 2
```


© 2021 IP Infusion Inc. Proprietary

ipv6 router ospf

Use this command to enable OSPFv3 routing on an interface.

Specify the process ID to configure multiple instances of OSPFv3. When running a single instance of OSPFv3, you do not need to specify a instance ID.

When OSPFv3 receives a packet, it checks if the instance ID in the packet matches the instance ID of the receiving interface.

Use the `no` parameter with this command to disable OSPFv3 routing on an interface.

Command Syntax

```
ipv6 router ospf area (A.B.C.D|<0-4294967295>)
ipv6 router ospf area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<64-95>)
ipv6 router ospf area (A.B.C.D|<0-4294967295>) tag WORD
ipv6 router ospf area (A.B.C.D|<0-4294967295>) tag WORD instance-id (<0-31>|<64-95>)
ipv6 router ospf tag WORD area (A.B.C.D|<0-4294967295>)
ipv6 router ospf tag WORD area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<64-95>)
no ipv6 router ospf area (A.B.C.D|<0-4294967295>)
no ipv6 router ospf area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<64-95>)
no ipv6 router ospf area (A.B.C.D|<0-4294967295>) tag WORD
no ipv6 router ospf area (A.B.C.D|<0-4294967295>) tag WORD instance-id (<0-31>|<64-95>)
no ipv6 router ospf tag WORD area (A.B.C.D|<0-4294967295>)
no ipv6 router ospf tag WORD area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<64-95>)
```

Parameters

`area`	OSPF Area ID in IPv4 address format.
`A.B.C.D`	OSPF area ID in IP address format.
`<0-4294967295>`	OSPF area ID as a decimal value.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.
`tag`	Tag value to use as a “match” value for controlling redistribution via route maps.
`WORD`	Set the tag value.

Default

By default, ipv6 router ospf is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 router ospf area 1 tag Tag1 instance-id 1
```


© 2021 IP Infusion Inc. Proprietary

ipv6 te-metric

Use this command to set the traffic engineering metric for an interface.

The traffic engineering metric is used in OSPF-TE Link State Advertisements. If the traffic engineering metric is not set, the ipv6 ospf cost value for an interface is used in OSPF-TE Link State Advertisements.

Use the `no` parameter with this command to unset the traffic engineering metric for this interface.

Command Syntax

```
ipv6 te-metric <1-65535>
ipv6 te-metric <1-65535> instance-id (<0-31>|<64-95>)
no ipv6 te-metric
no ipv6 te-metric instance-id (<0-31>|<64-95>)
```

Parameters

`te-metric`	Specify the TE metric.
`<1-65535>`	Specify the TE metric value.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, traffic engineering metric value is 0

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 te-metric 6
```

log-adjacency-changes

Use this command for the router to send a SYSLOG message when an OSPF neighbor goes up or down.

Use `no` parameter of this command to stop sending SYSLOG message.

Command Syntax

```
log-adjacency-changes (brief|detail|)
no log-adjacency-changes
```

Parameters

`detail`	Sends a SYSLOG message for each state change, not just when a neighbor goes up or down.

Default

None

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#log-adjacency-changes brief
(config-router)#log-adjacency-changes detail

#configure terminal
(config)#router ipv6 ospf
(config-router)#no log-adjacency-changes
```


© 2021 IP Infusion Inc. Proprietary

max-concurrent-dd

Use this command to limit the number of Database Descriptors (DD) that can be processed concurrently.

This command is useful when a router's performance is affected from simultaneously bringing up several OSPFv3 adjacencies. This command limits the maximum number of DD exchanges that can occur concurrently per OSPFv3 instance, thus allowing for all of the adjacencies to come up.

Use the `no` option with this command to remove the limit.

Command Syntax

```
max-concurrent-dd <1-65535>
no max-concurrent-dd
```

Parameters

`<1-65535>`	Specify the number of DD processes.

Default

By default, number of maximum concurrent DD processes is 5

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example set the `max-concurrent-dd` value to 4.

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#max-concurrent-dd 4
```

passive-interface

Use this command to suppress sending Hello packets on all interfaces, or on a specified interface.

This command configures OSPFv3 on simplex Ethernet interfaces. Since a simplex interface represents only one network segment between two devices, configure the transmitting interface as a passive interface. This ensures that OSPFv3 does not send hello packets for the transmitting interface. Both the devices can see each other via the hello packet generated for the receiving interface.

Use the `no` form with this command to resume sending `hello` packets on all interfaces, or on a specified interface.

Command Syntax

```
passive-interface (IFNAME |)
no passive-interface (IFNAME |)
```

Parameters

`IFNAME`	Specify an interface name

Default

By default, passive interface is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#passive-interface eth0
```


© 2021 IP Infusion Inc. Proprietary

redistribute

Use this command to import routes from other routing protocols, or from another OSPF instance, into OSPFv3 AS-external-LSAs.

OSPFv3 advertises routes learned from other routing protocols or from other OSPF instances, including static or connected routes. Each injected prefix is put into the AS-external-LSA with a specified metric and metric-type.

Use the `no` parameter with this command to stop redistribution.

Command Syntax

```
redistribute (kernel|connected|static|rip|bgp|isis|ospf (WORD|<1-65535>|)) {metric
  <0-16777214>|metric-type (1|2)|route-map WORD|tag <0-4294967295>}
no redistribute (kernel|connected|static|rip|bgp|isis|ospf (WORD|)) (metric|metric-
  type|route-map|tag|)
```

Parameters

`kernel`	Specify kernel routes.
`connected`	Specify connected routes.
`static`	Specify static routes.
`rip`	Specify RIP routes.
`bgp`	Specify BGP routes.
`isis`	Specify IS-IS routes.
`ospf`	Specify OSPF routes.
`WORD`	Specify an OSPFv3 Process Tag. If not specified, redistribute OSPF process with tag "null".
`<1-65535>`	Specify an OSPF process identifier. If not specified, redistribute OSPF instance with process ID 0.
`metric`	Specify the external metric.
`<0-16777214>`	Specify the external metric.
`metric-type`	Specify the external metric-type (see RFC 3101):
`1`	Set OSPF External Type 1 metric.
`2`	Set OSPF External Type 2 metric.
`route-map`	Specify a route map reference.
`WORD`	Specify name of the route-map.
`tag`	Tag value to use as a “match” value for controlling redistribution via route maps
`<0-4294967295>`	Specify the route tag.

Default

By default, redistribute is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows redistribution of BGP routes into the OSPFv3 routing table, with the metric as 10.

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#redistribute bgp metric 10 metric-type 1
```

The following example shows redistribution of static IPv4 routes into the OSPFv3 routing table.

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#redistribute static
```


© 2021 IP Infusion Inc. Proprietary

restart ipv6 ospf graceful

Use this command to restart OSPFv3 gracefully.

After this command is executed, the router immediately shuts down. NSM is notified that OSPF has shut down gracefully. NSM preserves routes installed by OSPF until the grace period expires.

Command Syntax

```
restart ipv6 ospf graceful (grace-period <1-1800>|)
```

Parameters

`grace-period`	Specify a grace period.
`<1-1800>`	Specify a grace period in seconds.

Default

By default, restart ipv6 ospf graceful is disabled. Default value of grace-period is 120 seconds.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#restart ipv6 ospf graceful grace-period 200
```

router-id

Use this command to specify a router ID for the OSPFv3 process.

Configure each router with a unique router-id. In an OSPFv3 router process that has active neighbors, a new router-id is used at the next reload or when you start the OSPFv3 manually.

Use the `no` form of this command to force OSPFv3 to stop the routing functionality.

Command Syntax

```
router-id A.B.C.D
no router-id
```

Parameters

`A.B.C.D`	Specify the router ID in IPv4 address format.

Default

By default, router id is loop-back IP address of IP address with highest IP

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows a fixed router ID `43.3.3.3`

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#router-id 43.3.3.3
```


© 2021 IP Infusion Inc. Proprietary

router ipv6 ospf

Use this command to initiate OSPFv3 routing process and enter Router mode to configure OSPFv3 routing process. For making the OSPFv3 routing process functional, you must specify OSPFv3 process tag in router mode and enable OSPFv3 on at least one interface. OSPFv3 is only enabled on interfaces where OSPFv3 process tag matches the tag specified using ipv6 router ospf area command in Interface mode.

Use the `no` parameter with this command to remove OSPFv3 process.

Command Syntax

```
router ipv6 ospf
router ipv6 ospf WORD
router ipv6 vrf ospf WORD
no router ipv6 ospf
no router ipv6 ospf WORD
no router ipv6 vrf ospf WORD
```

Parameters

`WORD`	Tag value to use as a “match” value for controlling redistribution via route maps.
`vrf`	Enable an IPv6 VRF routing process

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf Tag1
(config-router)#
```

show debugging ipv6 ospf

Use this command to display the OSPFv3 debugging options.

Command Syntax

```
show debugging ipv6 ospf
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging ipv6 ospf

OSPFv3 debugging status:
 OSPFv3 all packet debugging is on
 OSPFv3 all NFSM debugging is on
#
```


© 2021 IP Infusion Inc. Proprietary

show ipv6 ospf

Use this command to display global and area information about OSPFv3.

Command Syntax

```
show ipv6 ospf (WORD|)
```

Parameters

WORD	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 ospf
Routing Process "OSPFv3 0" with ID 1.2.3.4
SPF schedule delay 5 secs, Hold time between SPFs 10 secs Minimum LSA interval
5 secs,
Minimum LSA arrival 1 secs Number of external LSA 3. Checksum Sum 0x2CD6F
Number of areas
in this router is 1
Area BACKBONE(0)
Number of interfaces in this area is 1
SPF algorithm executed 3 times
Number of LSA 4. Checksum Sum 0x2A6AC
```

Table 2-140 explains the fields for each ospf entry.

Table 2-140: show ipv6 ospf output details

Field	Description
Area	Number of areas in device, area addresses, and so on.
Interface attached to this area	The device interfaces attached to the area.
SPF algorithm executed is N	The number of times (N) the OSPF Shortest Path First (SPF) algorithm is executed within the area.
Number of Area scoped LSAs is N	Number of LSAs (N) with a scope of the specified area.
SPF last updated	The interval in seconds that the SPF algorithm was last executed within the area.
Router	Number of router LSAs in the area.
Hold time	Minimum hold time between consecutive SPF calculations.
Checksum	LSA header checksum.

show ipv6 ospf database

Use this command to display information in the OSPFv3 Link State database.

Command Syntax

```
show ipv6 ospf database
show ipv6 ospf database (self-originate|max-age|adv-router A.B.C.D|)
show ipv6 ospf database (router|network|inter-prefix|inter-router|external|nssa-
  external|link|intra-prefix|te|grace)
show ipv6 ospf database (router|network|inter-prefix|inter-router|external|nssa-
  external|link|intra-prefix|te|grace) (self-originate|adv-router A.B.C.D|)
show ipv6 ospf database (router|network|inter-prefix|inter-router|external|nssa-
  external|link|intra-prefix|te|grace) A.B.C.D (self-originate|adv-router A.B.C.D|)
show ipv6 ospf WORD database
show ipv6 ospf WORD database (router|network|inter-prefix|inter-
  router|external|nssa-external|link|intra-prefix|te|grace)
show ipv6 ospf WORD database (router|network|inter-prefix|inter-
  router|external|nssa-external|link|intra-prefix|te|grace) adv-router A.B.C.D
```

Parameters

`self-originate`	Self-originated link states
`max-age`	LSAs in MaxAge list
`adv-router`	Advertising router for Type 8 Link LSAs (Link State Advertisements):
`A.B.C.D`	Router ID of the advertising router.
`router`	Router LSAs.
`network`	Network LSAs.
`inter-prefix`	Inter-Area-Prefix LSAs.
`inter-router`	Inter-Area-Router LSAs.
`external`	AS external LSAs.
`nssa-external`	NSSA LSAs.
`link`	Link LSAs.
`intra-prefix`	Intra-Area-Prefix LSAs (Type 9) with prefixes for stub and transit networks
`te`	Intra-area TE LSAs.
`grace`	Grace LSAs.
`A.B.C.D`	Link state ID as an IP address.
`WORD`	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

© 2021 IP Infusion Inc. Proprietary

Example: adv-router Parameter

This example shows using the `adv-router` parameter:

```
#show ipv6 ospf database link adv-router 10.70.0.58
            OSPFv3 Router with ID (10.70.0.58) (Process 100)
                Link-LSA (Interface eth1)
  LS age: 492
  LS Type: Link-LSA
  Link State ID: 0.0.0.3
  Advertising Router: 10.70.0.58
  LS Seq Number: 0x80000001
  Checksum: 0xC2D6
  Length: 68
  Priority: 1
  Options: 0x000013 (-|R|-|-|E|V6)
  Link-Local Address: fe80::204:75ff:feaa:fedb
  Number of Prefixes: 2
    Prefix: 5f00:1:2:10::/64
    Prefix Options: 0 (-|-|-|-)
```

Header

```
OSPFv3 Router with ID (10.70.0.58) (Process 100)
Link-LSA (Interface eth1)
```

The router ID and OSPFv3 process tag of the local router.

Interface name of the router associated with this Link-LSA.

OSPFv3 Database Fields

Table 2-141 explains the fields for each database entry.

Table 2-141: OSPFv3 database fields

Field	Description
LS age	The length of time in seconds since the LSA was originated.
LS Type	The type of LSA
Link State ID	Interface identifier of the originating router.
Advertising router	The Router ID of the router advertising this LSA. On a transit network, this is always the Designated Router ID.
LS Seq Number	Sequence number of an LSA.
Checksum	LSA header checksum (excluding the LS age field).
Length	The length in bytes of the LSA (including the 20-byte header).
Priority	The router priority of the interface attaching the originating router of the link.

Table 2-141: OSPFv3 database fields

Field	Description
Options	Bits in network LSAs that originate on the link: DC-bit: Whether the router supports OSPF over Demand Circuits. R-bit: Whether the router is active. If this bit is clear, routes which transit the advertising node cannot be computed. N-bit: How the router handles Type 7 LSAs. MC-bit: Whether IP multicast packets are forwarded. E-bit: Whether AS-External-LSAs are flooded. This bit is set in all AS External LSAs and in all LSAs. originated in the backbone and non-stub areas. V6-bit: Whether to include the router/link in routing calculations.
Link-Local Address	The originating router's link-local interface address.
Number of Prefixes	The number of IPv6 prefixes associated to the link: Prefix: The global IPv6 prefix associated to this link. Prefix Options: Each prefix is advertised along with an 8-bit capabilities field.They serve as input for routing calculations allowing, for example, some prefixes to be ignored or marked as not re-advertisable.
Referenced LS Type	Identifies the Router-LSA or Network-LSA with which the IPv6 prefixes are associated: Type 0x2001: prefixes associated with Router-LSA Type 0x2002: prefixes associated with Network-LSA
Referenced Link State ID	Referenced LS Type 0x2001: this field is 0 Referenced LS Type 0x2002: the interface ID of the link's Designated Router.
Referenced Advertising Router	Referenced LS Type 0x2001: ID of the originating router. Referenced LS Type 0x2002: ID of the Designated Router Prefix: Referenced LS Type 0x2001: global IPv6 prefix associated with the router Referenced LS Type 0x2002: global IPv6 prefix associated with the transit link Prefix Options: Bits in network LSAs that originate on the link: DC: How the router handles demand circuits R: Whether the router is active. If this bit is clear, routes which transit the advertising node cannot be computed. N: How the router handles Type 7 LSAs MC: Whether IP multicast packets are forwarded E: Whether AS-External-LSAs are flooded V6: Whether to include the router/link in routing calculations Metric: The cost of this prefix.

Example: intra-prefix and adv-router Parameters

This example shows using the `adv-router` and `intra-prefix` parameters.

Note: The same information for OSPFv2 can be viewed in type 1 router LSAs and type 2 network LSAs. However, in OSPFv3 all addressing information has been removed from router LSAs and network LSAs, leading to the introduction of the Intra-Area-Prefix LSA. In a transit network, the Intra-Area-Prefix-LSA serves the same purpose as a network LSA and on a point-to-point or point-to-multipoint network serves the same purpose as a router LSA.

```
#show ipv6 ospf database intra-prefix adv-router 10.70.0.58
           OSPFv3 Router with ID (10.70.0.58) (Process 100)
```


© 2021 IP Infusion Inc. Proprietary

```
               Intra-Area-Prefix-LSA (Area 0.0.0.0)
  LS age: 1435
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.70.0.58
  LS Seq Number: 0x80000001
  Checksum: 0x1B4E
  Length: 56
  Number of Prefixes: 2
  Referenced LS Type: 0x2002
  Referenced Link State ID: 0.0.0.3
  Referenced Advertising Router: 10.70.0.58
    Prefix: 5f00:1:2:10::/64
    Prefix Options: 0 (-|-|-|-)
    Metric: 0
    Prefix: 6f00:1:2:10::/64
    Prefix Options: 0 (-|-|-|-)
    Metric: 0
```

Header

```
OSPFv3 Router with ID (10.70.0.58) (Process 100)
Intra-Area-Prefix-LSA (Area 0.0.0.0)
```

- The router ID and OSPFv3 process tag for the router.
- Intra-Area-Prefix-LSA has area flooding scope. This LSA belongs to Area 0.0.0.0.

show ipv6 ospf interface

Use this command to display OSPFv3 interface information.

Command Syntax

```
show ipv6 ospf interface
show ipv6 ospf interface IFNAME
```

Parameters

`IFNAME`	The name of the interface.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Usage

This is a sample output from the `show ipv6 ospf interface` command displaying the OSPFv3 interface information:

```
#show ipv6 ospf interface
eth0 is up, line protocol is up
  Interface ID 3, Instance ID 0, Area 0.0.0.0
  IPv6 Link-Local Address fe80::248:54ff:fec0:f32d/10
 Router ID 1.2.3.4, Network Type BROADCAST, Cost: 10
 Transmit Delay is 1 sec, State Backup, Priority 1
 Designated Router (ID) 5.6.7.8
Interface Address fe80::203:47ff:fe4c:776e
 Backup Designated Router (ID) 1.2.3.4
Interface Address fe80::248:54ff:fec0:f32d
 Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
 Neighbor Count is 1, Adjacent neighbor count is 1
```

If Hello Suppression is enabled

```
RTR_B#show ipv6 ospf interface
eth1 is up, line protocol is up
  Interface ID 3
  IPv6 Prefixes
    fe80::5054:ff:fef3:f166/64 (Link-Local Address)
    2001::2/64
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 66
    Router ID 2.2.2.2, Network Type P2MP-NBMA, Cost: 1, TE Metric: 1
    Reduce LSA Flooding
    Transmit Delay is 1 sec, State Point-To-Point, Priority 1
    Timer interval configured, Hello 30, Dead 120, Wait 120, Retransmit 5
      Hello due in 00:00:32
    Neighbor Count is 1, Adjacent neighbor count is 1
    Suppress hello for 1 neighbor(s)
```


© 2021 IP Infusion Inc. Proprietary

```
        Hello received 2 sent 3, DD received 4 sent 6
        LS-Req received 1 sent 1, LS-Upd received 7 sent 4
        LS-Ack received 0 sent 3, Discarded 0
```

Table 2-142 explains the fields for each ospf interface entry.

Table 2-142: show ipv6 ospf interface output details

Field	Description
Interface Type and whether it is up or down.	Status of the interface type.
Line protocol	Status of the line protocol.
Interface ID	Interface for which information is displayed.
Instance ID	For running multiple instances of OSPFv3 on the router
Area	Area ID in A.B.C.D form
IPv6 Link-Local Address	link-local address is an IPv6 unicast address – cannot communicate to link-local addresses that are outside the directly connected network. In IPv6 (X:X::X:X/M) form.
Router ID	As stated – In A.B.C.D form.
Network Type	One of the following: • Ethernet is Broadcast • Serial p2p non-broadcast • NBMA – Non-Broadcast MultiAccess (NBMA) media
cost	The cost of sending packets over this interface – range is 1 to 65535.
Transmit Delay	The delay, in seconds, between link-state transmits. This value must be the same for all nodes on the network. The range is 1 to 65535. The default is 1.
Priority	OSPFv3 router priority for the interface. The range is 0 to 255. A router with priority 0 can never become the designated router, the default is 1.
Designated Router (ID)	The ID number of the Designated Router (DR).
Interface Address	The IPV6 address of this device.
Backup Designated Router	The ID number or the Backup Designated Router (BDR).
Interface Address	The IPv6 address of the Backup Designated Router.
Timer interval configured	The timer values of the following instances: Hello, Dead, Wait, Retransmit.
Hello due in	The countdown for receiving the next Hello packet.
Neighbor Count is	Number of neighbor count.
Adjacent neighbor count is	Number of adjacent neighbor count.

show ipv6 ospf neighbor

Use this command to display information about an OSPFv3 neighbor.

Command Syntax

```
show ipv6 ospf neighbor
show ipv6 ospf WORD neighbor
show ipv6 ospf neighbor INTERFACE
show ipv6 ospf WORD neighbor INTERFACE
show ipv6 ospf neighbor INTERFACE detail
show ipv6 ospf WORD neighbor INTERFACE detail
show ipv6 ospf neighbor detail
show ipv6 ospf WORD neighbor detail
show ipv6 ospf neighbor A.B.C.D
show ipv6 ospf WORD neighbor A.B.C.D
```

Parameters

WORD	Tag value to use as a “match” value for controlling redistribution via route maps.
INTERFACE	Display the name of the Interface
A.B.C.D	Neighbor IP address.
detail	Details of neighbors

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the show ipv6 ospf neighbor command displaying information about the OSPFv3 neighbor.

```
#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID Pri State Dead Time Interface Instance ID
5.6.7.8 1 Full/DR 00:00:38 eth0 0
```

If Hello Suppression is enabled

```
RTR_B#
RTR_B#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/ -         inactive    eth1       0
4.4.4.4           1   Full/DR         00:00:40    eth2       0
4.4.4.4           1   Full/ -         inactive    VLINK1     0
```


© 2021 IP Infusion Inc. Proprietary

```
RTR_B#

RTR_B#
RTR_B#show ipv6 ospf neighbor detail
 Neighbor 1.1.1.1, interface address fe80::5054:ff:feb3:d3bc
    In the area 0.0.0.0 via interface eth1
    Neighbor priority is 1, State is Full, 7 state changes
    Hello is suppressed
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x000133 (AF|*|*|DC|R|-|-|E|V6)
    Dead timer due in inactive
    Database Summary List 0
    Link State Request List 0
```

Table 2-143 explains the fields for each ospf neighbor entry.

Table 2-143: show ipv6 ospf neighbor output details

Field	Description
Neighbor	Router ID of the neighbor router.
interface address	IPv6 address of the neighbor's interface.
In the area	The neighbor router's area ID.
via interface	Neighbor router's interface name.
Neighbor Priority is	OSPFv3 router priority for the interface. The range is 0 to 255. A router with priority 0 can never become the designated router, the default is 1.
State	The Link State Address (LSA) of the neighbor, and there has been 7 state changes, and sending Hello packets is suppressed.
DR	Designated Router (DR) ID
BDR	Backup Designated Router (BDR) ID
Options is	The hexadecimal representation of the seven bits in the Options Field of Hello packets (see RFC 5340): • AF-bit – Address Family bit. • V6-bit – If this bit is clear, the router/link should be excluded from IPv6 routing calculations. • E-bit – This bit describes the way AS-external-LSAs are flooded. • N-bit – This bit indicates whether or not the router is attached to an NSSA. • R-bit – This bit (the `Router' bit) indicates whether the originator is an active router. If the router bit is clear, then routes that transit the advertising node cannot be computed. Clearing the router bit is appropriate for a multi-homed host that wants to participate in routing, but does not want to forward non-locally addressed packets. • DC-bit – This bit describes the router's handling of demand circuits, as specified in [DEMAND]. • *-bit – These bits are reserved for migration of OSPFv2 protocol extensions.

Table 2-143: show ipv6 ospf neighbor output details (Continued)

Field	Description
Dead timer due in	The countdown timer for marking neighbor connections dead. In this example, the Deat Timer has been deactivated.
Database Summary List	Describes routes to IPv6 address prefixes that belong to other areas.
Link State Request List	Sent or received when Link-State Request packets finds that parts of the Link State Database are out of date.
Timer interval configured	The set values for the following packet types: Hello, Dead, Wait, Retransmit.
Neighbor Count	The number of known neighbors.
Adjacent neighbor count	The number of directly adjacent neighbors.

© 2021 IP Infusion Inc. Proprietary

show ipv6 ospf route

Use this command to display the IPv6 routing table for OSPFv3.

The routes can be displayed in two ways:

- Each routing entry in a single-line
- Each routing entry in multiple lines

By default, the routing table is displayed in the multi-line format. For a single line display, give the ipv6 ospf display route single-line command.

Command Syntax

```
show ipv6 ospf route
show ipv6 ospf WORD route
```

Parameters

WORD	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is sample output in single-line format:

```
#show ipv6 ospf route
Destination Metric Next-hop
3ffe:1:1::/48 10 directly connected, eth0
3ffe:2:1::/48 10 directly connected, eth0
3ffe:2:2::/48 10 directly connected, eth0
3ffe:3:1::/48 10 directly connected, eth0
3ffe:3:2::/48 10 directly connected, eth0
3ffe:3:3::/48 10 directly connected, eth0
E2 3ffe:100:1::1/128 10/20 via fe80::203:47ff:fe4c:776e, eth0
E2 3ffe:100:2::1/128 10/20 via fe80::203:47ff:fe4c:776e, eth0
E2 3ffe:100:3::1/128 10/20 via fe80::203:47ff:fe4c:776e, eth0
IA 3ffe:101:1::/48 20 via fe80::203:47ff:fe4c:776e, eth0
IA 3ffe:101:2::/48 20 via fe80::203:47ff:fe4c:776e, eth0
IA 3ffe:101:3::/48 20 via fe80::203:47ff:fe4c:776e, eth0
```

The following is sample output in multi-line format:

```
#show ipv6 ospf route
Destination Metric
Next-hop Interface
3ffe:1:1::/48 10
-- eth0
3ffe:2:1::/48 10
-- eth0
3ffe:2:2::/48 10
```

```
-- eth0
3ffe:3:1::/48 10
-- eth0
3ffe:3:2::/48 10
-- eth0
3ffe:3:3::/48 10
-- eth0
E2 3ffe:100:1::1/128 10/20
fe80::203:47ff:fe4c:776e eth0
```

Table 2-144 explains the fields for each ospf route entry.

Table 2-144: show ipv6 ospf route output details

Field	Description
IP address	IP address of the remote network.
Metric	For OSPF the metric is cost, which indicates the best quality path to use to forward packets.
Next hop router IP address	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Outgoing interface name	Interface used to get to the next-hop address for this route.

© 2021 IP Infusion Inc. Proprietary

show ipv6 route fast-reroute

Use this command to display loop-free alternate routes with alternate next hops.

Command Syntax

```
show ipv6 route fast-reroute
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Usage

```
#show ipv6 route fast-reroute
```

show ipv6 ospfv3 topology

Use this command to display information about OSPFv3 topology for each area.

Command Syntax

```
show ipv6 ospfv3 topology
show ipv6 ospfv3 WORD topology
show ipv6 ospfv3 topology area (A.B.C.D|<0-4294967295>)
show ipv6 ospfv3 WORD topology area (A.B.C.D|<0-4294967295>)
```

Parameters

`WORD`	Tag value to use as a “match” value for controlling redistribution via route maps.
`area`	OSPFv3 area ID
`A.B.C.D`	OSPFv3 Area ID in IPv4 address format.
`<0-4294967295>`	OSPFv3 Area ID as a decimal value.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 ospfv3 topology
OSPFv3 paths to Area (0.0.0.0) routers
Router ID Bits Metric Next-Hop Interface
1.2.3.4 --
5.6.7.8 E 10 5.6.7.8 eth0
```

Example

```
#show ipv6 ospfv3 topology

OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
1.2.3.4                                               --
5.6.7.8          E     10         5.6.7.8              eth0
```

Table 2-145 explains the fields for each ospfv3 topology entry.

Table 2-145: show ipv6 ospfv3 topology output details

Field	Description
OSPFv3 path to Area	Area ID in IPv4 format.
Router ID	ID in IPv4 format,

© 2021 IP Infusion Inc. Proprietary

Table 2-145: show ipv6 ospfv3 topology output details

Field	Description
Bits	Bits appended to packets: • V-bit Indicates whether the advertising router is an endpoint of a virtual link. • E-bit Indicates whether the advertising router is an Autonomous System Border Router (ASBR). • B-bit Indicates whether the advertising router is an Area Border Router (ABR). • W-bit When set, the router is a wild-card multicast receiver.
Metric	The value of ospfv3 metric.
Next-Hop	The next-hop identifier.
Interface	The interface name through which the virtual link extends.

show ipv6 ospf virtual-links

Use this command to display information about OSPFv3 virtual-links.

Command Syntax

```
show ipv6 ospf virtual-links
show ipv6 ospf WORD virtual-links
```

Parameters

WORD	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 5.6.7.8 is up
Transit area 0.0.0.1 via interface eth0, instance ID 0
Local address 3ffe:1234:1::1/128
Remote address 3ffe:5678:3::1/128
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Adjacency state Up
```

If Hello Suppression is enabled

```
RTR_B#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 4.4.4.4 is up
  Transit area 0.0.0.1 via interface eth2, instance ID 0
  Hello suppression Enabled
  DoNotAge LSA allowed
  Local address 2002::1/128
  Remote address 2002::2/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in inactive
    Adajcency state Full
RTR_B#
RTR_B#
```

Table 2-146 explains the fields for each ospf virtual-links entry.

© 2021 IP Infusion Inc. Proprietary

Table 2-146: show ipv6 ospf virtual-links output details

Field	Description
Virtual Link	Virtual link name, the router ID to which it is connected, and the state of the link.
Transit area	Transit area ID, the interface it uses, and its instance ID – an Instance ID should default to 0. It is only necessary to assign a value other than 0 on those links that will contain multiple separate communities of OSPF routers.
Local address	The local IPV6 address and subnet mask.
Remote address	The remote IPv6 address and subnet mask.
Transmit Delay	The delay, in seconds, between link-state transmits. This value must be the same for all nodes on the network. The range is 1 to 65535. The default is 1. The state is point-to-point.
Timer intervals configured	The configured values in seconds of the following timers: Hello, Dead, Wait, Retransmit.
Hello due in	A countdown timer that indicates when the next Hello packet should arrive.
Adjacency State	Whether the adjacency state is either up or down.

show ipv6 vrf

Use this command to list information about VRFs.

Command Syntax

```
show ipv6 vrf (WORD|)
```

Parameter

`WORD`	VPN Routing/Forwarding instance name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is a sample output of the `show ipv6 vrf` command displaying VRF information:

```
#show ipv6 vrf
Name              Interfaces

qa                eth0
you               eth1
myVRF             eth2
```

Table 2-147 explains the fields.

Table 2-147: show ipv6 vrf output details

Field	Description
Name	Name of the interface.
Interfaces	Type of an interface.

© 2021 IP Infusion Inc. Proprietary

shutdown

Use this command to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away.

Use the `no` parameter of this command, not to temporarily shut a protocol.

Command Syntax

```
shutdown
no shutdown
```

Parameter

None

Default

None

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#shutdown

#configure terminal
(config)#router ipv6 ospf
(config-router)#no shutdown
```

snmp restart ospf6

Use this command restart SNMP in OSPFv3

Command Syntax

```
snmp restart ospf6
```

Parameter

None

Default

By default, SNMP restart is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart ospf6
```


© 2021 IP Infusion Inc. Proprietary

summary-address

Use this command to summarize or suppress external routes with the specified address range.

An address range is a pairing of a starting address and a mask that is almost the same as IP network number. For example:

- If the specified IPV6 address range is 2020:100:100:2000::/53, it matches 2020:100:100:2222::/64, 2020:100:100:2666::/64 and so on.
- If the specified IPV4 address range is 192.168.0.0/255.255.240.0, it matches 192.168.1.0/24, 192.168.4.0/22, 192.168.8.128/25 and so on.

Redistributing routes from other protocols into OSPF requires the router to advertise each route individually in an external LSA. Use this command to advertise one summary route for all redistributed routes covered by a specified network address and mask. This minimizes the size of the OSPF link state database.

Use the `no` form this command to remove summary addresses.

Command Syntax

```
summary-address X:X::X:X/M (not-advertise|(all-tag (<0-4294967295> ))| )
  (translate-tag (<0-4294967295>) | )
summary-address A.B.C.D/M (not-advertise|tag <0-4294967295>|)
no summary-address A.B.C.D/M
no summary-address X:X::X:X/M (not-advertise|all-tag|translate-tag)
no summary-address A.B.C.D/M (not-advertise|tag)
```

Parameters

`X:X::X:X/M`	The range of addresses given as IPv6 starting address and a mask.
`A.B.C.D/M`	The range of addresses given as IPv4 starting address and a mask.
`not-advertise`	Suppress routes that match the range.
`tag`	Tag value to use as a “match” value for controlling redistribution via route maps.
`<0-4294967295>`	Set a tag value. The default is 0.
`all-tag`	Set tag for all summarized type-5, translated type5 and type-7 LSA.
`translate-tag`	Set tag only for summarized translated type-5 LSA.

Default

By default, summary-address value is 0

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example uses the `summary-address` command to aggregate external LSAs that match the network 172.16.0.0/24 and assign a tag value of 3.

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#summary-address 2020:100:100:2000::/53 all-tag 3
```


© 2021 IP Infusion Inc. Proprietary

timers spf exp

Use this command to set the Shortest-Path First (SPF) best-path schedule minimum and maximum delay between receiving a change to SPF calculation in milliseconds.

Use `no` parameter of this command to unset the SPF best-path schedule.

Command Syntax

```
timers spf exp <0-2147483647> <0-2147483647>
no timers spf exp
```

Parameters

`<0-2147483647>`

The minimum delay in milliseconds between receiving a change to SPF calculation.

`<0-2147483647>`

The maximum delay in milliseconds between receiving a change to SPF calculation.

Default

Default minimum delay: 500 milliseconds

Default maximum delay: 50000 milliseconds (50 seconds)

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#timers spf exp 300 300
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 OSPF VPN Commands

This chapter provides an alphabetized reference of the OSPF VPN commands. It includes the following commands:

- capability vrf-lite
- router ospf vrf
- domain-id

capability vrf-lite

Use this command to enable the `vrf-lite` capability for an OSPF instance.

Use the `no` parameter with this command to disable the same for an OSPF instance.

Command Syntax

```
capability vrf-lite
no capability vrf-lite
```

Parameters

None

Default

By default, VRF lite capability for an OSPF instance is disabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ospf 100
(config-router)#capability vrf-lite
(config)#router ospf 100
(config-router)#no capability vrf-lite
```


© 2021 IP Infusion Inc. Proprietary

router ospf vrf

Use this command to specify a VRF instance in OSPF. To use this command, you must first create a VRF Name in the NSM using the `ip vrf` command. Associate the same name with the OSPF instance using this command.

Command Syntax

```
router ospf <1-65535> WORD
```

Parameters

`<1-65535>`	Routing process ID; should be unique for each routing process.
`WORD`	Name of the VRF to associate with this OSPF instance.

Default

By default, router ospf vrf is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100 myVRF
(config-router)#
```

domain-id

Use this command to specify the domain ID for a OSPF bound to VRF.

The routes sent from OSPF to the VPN cloud are sent along with the domain ID. In this way, the domain ID acts as an identification for the route received from each OSPF domain.

Use the `no` form of this command to remove a domain ID.

Command Syntax

```
domain-id ((A.B.C.D (secondary|)) | (type (type-as|type-as4|type-back-comp) value HEX_DATA (secondary|)))
no domain-id ((A.B.C.D (secondary|)) | (type (type-as|type-as4|type-back-comp) value HEX_DATA (secondary|)))
```

Parameters

`A.B.C.D`	Domain ID in IP address format.
`secondary`	Domain ID is secondary. If not specified the domain ID is primary.
`type`	Domain type:
`type-as`	AS format. Hexadecimal value is 0x0005.
`type-as4`	AS4 format. Hexadecimal value is 0x0205.
`type-back-comp`	Used for backward compatibility. Hexadecimal value is 0x8000.
`value`	Domain ID.
`HEX_DATA`	Domain ID in hexadecimal.
`secondary`	Domain ID is secondary. If not specified the domain ID is primary

Default

No domain ID is defined.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows configuring a primary domain ID in IP address format.

```
#configure terminal
(config)#router ospf 100 vrf
(config-router)#domain-id 12.12.12.12
```

The following example shows configuring a secondary domain ID in IP address format.

```
#configure terminal
(config)#router ospf 100 vrf
```


© 2021 IP Infusion Inc. Proprietary

```
(config-router)#domain-id 13.13.13.13 secondary
```

The following example shows configuring a primary domain ID in AS type format.

```
#configure terminal
(config)#router ospf 100 vrf
(config-router)#domain-id type type-as value 123456abcdef
```

© 2021 IP Infusion Inc. Proprietary

Border Gateway Protocol Command Reference

Contents

This document contains these chapters and appendices:

- Chapter 1, *BGP Commands*
- Chapter 2, *BGP Labeled Unicast Commands*
- Chapter 3, *BGP Virtual Private Network Commands*
- Chapter 4, *BGP Show Commands*
- Appendix 5, *Regular Expressions*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 BGP Commands

This chapter describes the BGP configuration commands.

- address-family
- aggregate-address
- auto-summary
- bgp aggregate-nexthop-check
- bgp always-compare-med
- bgp as-local-count
- bgp bestpath as-path ignore
- bgp bestpath as-path multipath-relax
- bgp bestpath compare-confed-aspath
- bgp bestpath compare-routerid
- bgp bestpath dont-compare-originator-id
- bgp bestpath med
- bgp bestpath tie-break-on-age
- bgp client-to-client reflection
- bgp cluster-id
- bgp confederation identifier
- bgp confederation peers
- bgp config-type
- bgp dampening
- bgp default local-preference
- bgp deterministic-med
- bgp enforce-first-as
- bgp extended-asn-cap
- bgp fast-external-failover
- bgp graceful-restart
- bgp g-shut
- bgp g-shut-capable
- bgp g-shut-local-preference
- bgp log-neighbor-changes
- bgp nexthop-trigger delay
- bgp nexthop-trigger enable
- bgp rfc1771-path-select
- bgp rfc1771-strict
- bgp router-id
- bgp scan-time

© 2021 IP Infusion Inc. Proprietary

- bgp table-map
- bgp update-delay
- clear bgp (A.B.C.D|X:X::X:X)
- clear bgp *
- clear bgp <1-4294967295>
- clear bgp dampening
- clear bgp external
- clear bgp flap-statistics
- clear bgp peer-group
- clear bgp statistics
- clear ip bgp A.B.C.D
- clear ip bgp A.B.C.D vrf
- clear ip bgp table-map
- debug bgp
- distance bgp
- exit-address-family
- ip as-path access-list
- ip community-list <1-99>
- ip community-list <100-500>
- ip community-list expanded
- ip community-list standard
- ip community-list WORD
- ip extcommunity-list <1-99>
- ip extcommunity-list <100-500>
- ip extcommunity-list expanded
- ip extcommunity-list standard
- l2vpn-unnumbered-mode
- match ip peer
- max-paths
- neighbor activate
- neighbor advertisement-interval
- neighbor allowas-in
- neighbor as-origination-interval
- neighbor attribute-unchanged
- neighbor authentication-key
- neighbor capability dynamic
- neighbor capability graceful-restart
- neighbor capability orf prefix-list
- neighbor capability route-refresh

© 2021 IP Infusion Inc. Proprietary

- neighbor collide-established
- neighbor default-originate
- neighbor description
- neighbor disallow-infinite-holdtime
- neighbor distribute-list
- neighbor dont-capability-negotiate
- neighbor ebgp-multihop
- neighbor enforce-multihop
- neighbor fall-over bfd
- neighbor filter-list
- neighbor g-shut
- neighbor g-shut-timer
- neighbor limit
- neighbor local-as
- neighbor maximum-prefix
- neighbor next-hop-self
- neighbor optional-as
- neighbor override-capability
- neighbor passive
- neighbor peer-group
- neighbor WORD peer-group range
- neighbor port
- neighbor prefix-list
- neighbor remote-as
- neighbor remove-private-AS
- neighbor restart-time
- neighbor route-map
- neighbor route-reflector-client
- neighbor route-server-client
- neighbor send-community
- neighbor shutdown
- neighbor soft-reconfiguration inbound
- neighbor strict-capability-match
- neighbor timers
- neighbor unsuppress-map
- neighbor update-source
- neighbor version
- neighbor weight
- neighbor WORD peer-group

- network
- network synchronization
- redistribute
- restart bgp gracefull
- router bgp
- snmp restart bgp
- synchronization
- timers bgp
- v4-unnumbered-mode
- undebug bgp
- bgp unnumbered-mode

© 2021 IP Infusion Inc. Proprietary

address-family

Use the address family command to enter the IPv4 or VPNv4 address family mode allowing configuration of address-family specific parameters. To leave the address family mode and return to the Configure mode use the `exit-address-family` command.

This command configures the routing exchange between Provider Edge (PE) and Customer Edge (CE) devices. The BGP sessions between PE routers can carry different types of routes (VPN-IPv4 and IPv4 routes). Address families are used to control the type of BGP session. Configure a BGP address family for each VRF configured on the PE router and a separate address family to carry VPN-IPv4 routes between PE routers. All non VPN BGP neighbors are defined using router mode. All VPN BGP neighbors are defined under its associated address family mode. The BGP process with no address-family specified is the default address-family, where any sessions are configured that either are not associated with a VRF or are used to carry IPv4 routes.

Use the `no` parameter with this command to disable the address-family configurations.

Command Syntax

```
address-family ipv4
address-family ipv4 (unicast|multicast)
address-family ipv4 vrf NAME
address-family l2vpn evpn
address-family rtfilter unicast
address-family vpn4
address-family vpn4 unicast
no address-family ipv4 vrf NAME
no address-family ipv4 (unicast|multicast)
no address-family l2vpn evpn
no address-family rtfilter unicast
no address-family vpnv4
no address-family vpnv4 unicast
```

Parameters

`ipv4`	IPv4 address family
`unicast`	Unicast address prefixes
`multicast`	Multicast address prefixes
`vrf`	Virtual Private Network (VPN) routing/forwarding instance
`NAME`	VPN routing/forwarding instance name
`unicast`	Unicast address prefixes
`l2vpn evpn`	Layer 2 VPN routing sessions with EVPN endpoint information distributed to BGP peers
`rtfilter`	Route target filter: on an iBGP peer or Route Reflector (RR), only send IPv4 and IPv6 prefixes to PE routers when a PE has a VRF that imports those specific prefixes.
`unicast`	Unicast address prefixes
`vpnv4`	VPN version 4 address family
`unicast`	Unicast address prefixes

Applicability

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 7657
(config-router)#neighbor 3ffe:506::1 remote-as 7657
(config-router)#neighbor 3ffe:506::1 interface eth1

#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 3ffe:506::1 activate
(config-router-af)#exit-address-family
```


© 2021 IP Infusion Inc. Proprietary

aggregate-address

Use this command to configure BGP aggregate entries.

Aggregates are used to minimize the size of routing tables. Aggregation combines the characteristics of several different routes and advertises a single route.The `aggregate-address` command creates an aggregate entry in the BGP routing table if any more-specific BGP routes are available in the specified range. Using the `summary-only` parameter advertises the prefix only, suppressing the more-specific routes to all neighbors. In the following example Router1 will propagate network 172.0.0.0 and suppresses the more specific route 172.10.0.0.

The `as-set` parameter creates an aggregate entry advertising the path for this route, consisting of all elements contained in all paths being summarized. Use this parameter to reduce the size of path information by listing the AS number only once, even if it was included in multiple paths that were aggregated. The `as-set` parameter is useful when aggregation of information results in an incomplete path information.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
aggregate-address A.B.C.D/M
aggregate-address A.B.C.D/M as-set
aggregate-address A.B.C.D/M as-set summary-only
aggregate-address A.B.C.D/M summary only
aggregate-address A.B.C.D/M summary-only as-set
no aggregate-address A.B.C.D/M
```

Parameters

`A.B.C.D/M`	Aggregate prefix
`as-set`	Generate AS set path information
`summary-only`	Filter more specific routes from updates

Default

By default, aggregate address A.B.C.D/M is disabled

Command Mode

Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#aggregate-address 10.0.0.0/8 as-set summary-only

(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#no aggregate-address 10.0.0.0/8
```

auto-summary

Use this command to enable sending summarized routes by a BGP speaker to its peers in the router configuration mode or in the address-family configuration mode. Auto-summary is used by a BGP router to advertise summarized routes to its peers. Auto-summary can be enabled if certain routes have already been advertised: in this case, configuring auto-summary advertises the summarized routes first, then corresponding non-summarized routes are withdrawn. If certain routes have already been advertised, and auto-summary is disabled, non-summarized routes are first advertised, then the corresponding summarized routes are withdrawn from all the connected peers.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
auto-summary
```

```
no auto-summary
```

Parameters

None

Default

By default, auto-summary is disabled

Command Mode

Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 11
(config-router)#address-family ipv4 unicast
(config-router-af)#auto-summary
```


© 2021 IP Infusion Inc. Proprietary

bgp aggregate-nexthop-check

Use this command to set the BGP option to perform aggregation only when next-hop matches the specified IP address.

Use the `no` parameter with this command to disable this functionality.

Command Syntax

```
bgp aggregate-nexthop-check
no bgp aggregate-nexthop-check
```

Parameters

None

Default

By default, bgp aggregate nexthop check is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp aggregate-nexthop-check
```

bgp always-compare-med

Use this command to compare the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal. MED comparison is done only among paths from the same autonomous system (AS). Use `bgp always-compare-med` command to allow comparison of MEDs from different ASs. The MED parameter is used to select the best path. A path with lower MED is preferred. If the bgp table shows the following and the always-compare-med is enabled:

```
Route1: as-path 400, med 300
Route2: as-path 200, med 200
Route3: as-path 400, med 250
```

Route1 is compared to Route2. Route2 is best of the two (lower MED). Next, Route2 is compared to Route3 and Route2 is chosen best path again (lower MED). If always-compare-med was disabled, MED is not taken into account when Route1 and Route2 are compared, because of different ASs and MED is compared for only Route1 and Route3. In this case, Route3 would be the best path. The selected route is also affected by the `bgp deterministic-med` command. Please see `bgp deterministic-med` command for details. If this command is used to compare MEDs for all paths, it should be configured on every BGP router in the AS.

Use the `no` parameter with this command to disallow the comparison.

Command Syntax

```
bgp always-compare-med
```

```
no bgp always-compare-med
```

Parameters

None

Default

By default, bgp always compare med is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp always-compare-med
```


© 2021 IP Infusion Inc. Proprietary

bgp as-local-count

Use this command to set the number of times the local-AS (Autonomous System) is to be prepended.

Use the `no` parameter with this command to stop prepending the local AS count.

Command Syntax

```
bgp as-local-count <2-64>
no bgp as-local-count <2-64>
```

Parameter

`<2-64>`	The number of times the local-AS is to be prepended

Default

By default, bgp as local count is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp as-local-count 55

(config)#router bgp 100
(config-router)#no bgp as-local-count 55
```

bgp bestpath as-path ignore

Use this command to prevent the router from considering the autonomous system (AS) path length as a factor in the algorithm for choosing a best path route.

Use the `no` parameter with this command to allow the router to consider the AS path length in choosing a best path route.

Command Syntax

```
bgp bestpath as-path ignore
```

```
no bgp bestpath as-path ignore
```

Parameters

None

Default

By default, bgp bestpath as-path ignore is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath as-path ignore

(config)#router bgp 100
(config-router)#no bgp bestpath as-path ignore
```


© 2021 IP Infusion Inc. Proprietary

bgp bestpath as-path multipath-relax

Use this command to relax the “same AS-Path” requirement so any candidate eBGP AS-Path with the same AS-path length might be used for eBGP load-balancing.

Note: This feature does not load-balance between eBGP and iBGP paths.

Normally eBGP load-balancing requires the candidate routes to be equal-cost paths with identical BGP attributes having the same weight, Local-Pref, AS-Path (both the AS numbers and the AS path length), origin, MED, and different next-hop.

Use the `no` parameter with this command to return to normal operation.

Command Syntax

```
bgp bestpath as-path multipath-relax
```

```
no bgp bestpath as-path multipath-relax
```

Parameters

None

Default

By default, as-path multipath-relax is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath as-path multipath-relax

(config)#router bgp 100
(config-router)#no bgp bestpath as-path multipath-relax
```

bgp bestpath compare-confed-aspath

Use this command to allow comparing of the confederation AS path length. This command specifies that the AS confederation path length must be used when available in the BGP best path decision process. It is effective only when bgp bestpath as-path ignore command has not been used.

Use the `no` parameter with this command to ignore consideration of AS confederation path length in BGP best path selection.

Command Syntax

```
bgp bestpath compare-confed-aspath
```

```
no bgp bestpath compare-confed-aspath
```

Parameters

None

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath compare-confed-aspath

(config)#router bgp 100
(config-router)#no bgp bestpath compare-confed-aspath
```


© 2021 IP Infusion Inc. Proprietary

bgp bestpath compare-routerid

Use this command to compare router IDs for identical eBGP paths. When comparing similar routes from peers, the BGP router does not consider the router ID of the routes. By default, it selects the first received route. Use this command to include router ID in the selection process; similar routes are compared and the route with the lowest router ID is selected. The router IS is the highest IP address on the router, with preference given to loopback addresses. Router ID can be manually set by using the bgp router-id command.

Use the `no` parameter with this command to disable this functionality.

Command Syntax

```
bgp bestpath compare-routerid
```

```
no bgp bestpath compare-routerid
```

Parameters

None

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath compare-routerid

(config)#router bgp 100
(config-router)#no bgp bestpath compare-routerid
```

bgp bestpath dont-compare-originator-id

Use this command to change the default bestpath selection by not comparing an originator-ID for an identical EBGP path.

Use the `no` parameter with this command to disable this functionality.

Command Syntax

```
bgp bestpath dont-compare-originator-id
```

```
no bgp bestpath dont-compare-originator-id
```

Parameters

None

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath dont-compare-originator-id

(config)#router bgp 100
(config-router)#no bgp bestpath dont-compare-originator-id
```


© 2021 IP Infusion Inc. Proprietary

bgp bestpath med

Use this command to specify two MED (Multi Exit Discriminator) attributes, `confed` and `missing-as-worst`.

The `confed` attribute enables MED comparison along paths learned from confederation peers. The MEDs are compared only if there is no external Autonomous System (an AS not within the confederation) in the path. If there is an external autonomous system in the path, the MED comparison is not made. For example in the following paths, the MED is not compared with Route3 as it is not in the confederation. MED is compared for Route1 and Route2 only.

```
Path1 = 32000 32004, med=4
Path2 = 32001 32004, med=2
Path3 = 32003 1, med=1
```

The `missing-as-worst` attribute to consider a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path. If `missing-as-worst` is disabled, the missing MED is assigned the value of 0, making the path with the missing MED attribute the best path.

Use the `no` parameter with this command to prevent BGP from considering the MED attribute in comparing paths.

Command Syntax

```
bgp bestpath med confed missing-as-worst
bgp bestpath med (confed|missing-as-worst|remove-recv-med|remove-send-med)
bgp bestpath med missing-as-worst confed
no bgp bestpath med confed missing-as-worst
no bgp bestpath med (confed|missing-as-worst|remove-recv-med|remove-send-med)
no bgp bestpath med missing-as-worst confed
```

Parameters

`confed`	Compare MED along confederation paths
`missing-as-worst`	Treat missing MED as the least preferred one
`remove-recv-med`	Remove received MED attribute
`remove-send-med`	Remove sent MED attribute

Command Mode

Router mode

Default

By default, MED value is zero.

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
```

```
(config)#router bgp 100
(config-router)#bgp bestpath med missing-as-worst

(config)#router bgp 100
(config-router)#bgp bestpath med remove-recv-med
(config-router)#no bgp bestpath med remove-recv-med

(config)#router bgp 100
(config-router)#bgp bestpath med remove-send-med
(config-router)#no bgp bestpath med remove-send-med
```


© 2021 IP Infusion Inc. Proprietary

bgp bestpath tie-break-on-age

Use this command to always select a preferred older route even when the `bgp bestpath compare-routerid` command is configured.

Use the `no` parameter with this command to disable this functionality.

Command Syntax

```
bgp bestpath tie-break-on-age
```

```
no bgp bestpath tie-break-on-age
```

Parameters

None

Default

By default, tie-break-on-age is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath tie-break-on-age

(config)#router bgp 100
(config-router)#no bgp bestpath tie-break-on-age
```

bgp client-to-client reflection

Use this command to configure routers as route reflectors. Route reflectors are used when all Interior Border Gateway Protocol (iBGP) speakers are not fully meshed. If the clients are fully meshed the route reflector is not required, use `no bgp client-to-client reflection` command to disable the client-to-client route reflection.

Use the `no` parameter with this command to turn off client-to-client reflection.

Command Syntax

```
bgp client-to-client reflection
```

```
no bgp client-to-client reflection
```

Parameters

None

Default

When a router is configured as a route reflector, client-to-client reflection is enabled by default.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp client-to-client reflection

(config)#router bgp 100
(config-router)#no bgp client-to-client reflection
```


© 2021 IP Infusion Inc. Proprietary

bgp cluster-id

Use this command to configure the cluster ID if the BGP cluster has more than one route reflector. A cluster includes route reflectors and its clients. Usually, each cluster is identified by the router ID of its single route reflector but to increase redundancy sometimes a cluster may have more than one route reflector. All router reflectors in such a cluster are then identified by a cluster ID. The `bgp cluster-id` command is used to configure the 4 byte cluster ID for clusters with more than one route reflectors.

Use the `no` parameter with this command (without any arguments) to remove a previously configured route reflector cluster ID.

Command Syntax

```
bgp cluster-id <1-4294967295>
bgp cluster-id A.B.C.D
no bgp cluster-id
```

Parameters

`<1-4294967295>`	Route reflector ID as a 32-bit quantity
`A.B.C.D`	Route reflector ID in an IPv4 address format

Default

By default, cluster id is set bgp cluster id

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following configuration creates a cluster-id 5 including two route-reflector-clients.

```
#configure terminal
(config)#router bgp 100
(config-router)#neighbor 2.2.2.2 remote-as 200
(config-router)#neighbor 3.3.3.3 remote-as 200
(config-router)#neighbor 5.5.5.5 remote-as 200
(config-router)#neighbor 6.6.6.6 remote-as 200
(config-router)#bgp cluster-id 5
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 3.3.3.3 route-reflector-client
(config-router-af)#neighbor 5.5.5.5 route-reflector-client
```

© 2021 IP Infusion Inc. Proprietary

bgp confederation identifier

Use this command to specify a BGP confederation identifier.

Use the `no` parameter with this command to remove a BGP confederation identifier.

Command Syntax

```
bgp confederation identifier <1-65535>
no bgp confederation identifier
```

Parameter

`<1-65535>`	Routing domain confederation AS number

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp confederation identifier 1
```


© 2021 IP Infusion Inc. Proprietary

bgp confederation peers

Use this command to configure the Autonomous Systems (AS) that belong to a confederation. A confederation allows an AS to be divided into several ASs. The AS is given a confederation identifier. External BGP (eBGP) routers view only the whole confederation as one AS. Each AS is fully meshed within itself and is visible internally to the confederation.

Use the `no` parameter with this command to remove an autonomous system from the confederation.

Command Syntax

```
bgp confederation peers <1-65535>
no bgp confederation peers <1-65535>
```

Parameter

`<1-65535>`	AS numbers of eBGP peers that are in the same confederation

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following configuration example, the neighbor 172.210.30.2 and 172.210.20.1 have iBGP connection within AS 100, neighbor 173.213.30.1 is a BGP connection with a confederation peer 200 and neighbor 6.6.6.6 has an eBGP connection to external AS 300.

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp confederation identifier 300
(config-router)#bgp confederation peers 200
(config-router)#neighbor 172.210.30.2 remote-as 100
(config-router)#neighbor 172.210.20.1 remote-as 100
(config-router)#neighbor 173.213.30.1 remote-as 200
(config-router)#neighbor 6.6.6.6 remote-as 300
```

In this configuration, the neighbor 5.5.5.4 has an eBGP connection to confederation 300.

```
#configure terminal
(config)#router bgp 500
(config-router)#neighbor 5.5.5.4 remote-as 300
```

© 2021 IP Infusion Inc. Proprietary

bgp config-type

Use this command to set the BGP configuration to the `standard` type. After setting the configuration to the `standard` type, use the neighbor send-community command to send out BGP community attributes. The `zebos` configuration type is the default and requires no specific configuration for sending out BGP standard community and extended community attributes.

For the `standard` type, the `no synchronization` command is always shown in the configuration, whereas for the `zebos` type, this command is the default.

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
bgp config-type (standard|zebos)
no bgp config-type
```

Parameters

`standard`	Standard style configuration
`zebos`	OcNOS style configuration

Default

The default configuration type is: bgp config-type zebos

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp config-type standard
```


© 2021 IP Infusion Inc. Proprietary

bgp dampening

Use this command to enable BGP route dampening and set various parameters. Route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the `suppress` limit the advertisement of the route is suppressed. This penalty is decayed according to the configured `half time` value. Once the penalty is lower than the `reuse` limit, the route advertisement is un-suppressed. The dampening information is purged from the router once the penalty becomes less than half of the `reuse` limit.

Use the `no` parameter with this command to unset BGP dampening parameters.

Command Syntax

```
bgp dampening
bgp dampening <1-45>
bgp dampening <1-45> <1-20000> <1-20000> <1-255>
bgp dampening <1-45> <1-20000> <1-20000> <1-255> <1-45>
bgp dampening route-map WORD
no bgp dampening
```

Parameters

`<1-45>`	Reachability half-life time for the penalty in minutes. The time for the penalty to decrease to one-half of its current value.
`<1-20000>`	Value to start reusing a route. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed.
`<1-20000>`	Value to start suppressing a route. When the penalty for a route exceeds the suppress value, the route is suppressed
`<1-255>`	Maximum duration to suppress a stable route in minutes.
`<1-45>`	Un-reachability half-life time for the penalty in minutes.
`route-map`	Route map to specify criteria for dampening.
`WORD`	Route-map name.

Defaults

The default reachability half-life is 15 minutes.

The default reuse limit is 750.

The default suppress limit is 2000.

The default max-suppress value is 4 times the half-life time, or 60 minutes.

Command Mode

Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 11
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp dampening 20 800 2500 80 25
```


© 2021 IP Infusion Inc. Proprietary

bgp default local-preference

Use this command to change the default local preference value.Local preference indicates the preferred path when there are multiple paths to the same destination. The path having a higher preference is preferred. The preference is sent to all routers and access servers in the local autonomous system.

Use the `no` parameter with this command to revert to the default value for local preference.

Command Syntax

```
bgp default local-preference <0-4294967295>
no bgp default local-preference
no bgp default local-preference <0-4294967295>
```

Parameter

`<0-4294967295>` Local preference value

Default

By default, local preference value is 100

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp default local-preference 2345555
```

bgp deterministic-med

Use this command to compare the Multi Exit Discriminator (MED) variable when choosing among routes advertised by different peers in the same autonomous system. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal.

For a correct comparison result, enable this command on all routers in a local AS. After enabling this command, all paths for the same prefix are grouped together and arranged according to their MED value. Based on this comparison, the best path is then chosen. This command compares MED variable when choosing routes advertised by different peers in the same AS, to compare MED, when choosing routes from neighbors in different ASs use the bgp always-compare-med command.

When the bgp deterministic-med command is enabled, routes from the same AS are grouped together, and the best routes of each group are compared. If the BGP table showed:

```
Route1: as-path 200, med 300, internal
Route2: as-path 400, med 200, internal
Route3: as-path 400, med 250, external
```

BGP would have a group of Route1 and a second group of Route2 and Route3 (the same ASs). The best of each group is compared. Route1 is the best of its group because it is the only route from AS 200. Route1 is compared to the Route2, the best of group AS 400 (the lower MED). Since the two routes are not from the same AS, the MED is not considered in the comparison. The external BGP route is preferred over the internal BGP route, making Route3 the best route; the preferred route would be different if `always-compare-med` command is enabled (See `always-compare-med` command).

Use the `no` parameter with this command to disallow this setting.

Command Syntax

```
bgp deterministic-med
```

```
no bgp deterministic-med
```

Parameters

None

Default

By default, bgp deterministic med is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp deterministic-med

(config)#router bgp 100
(config-router)#no bgp deterministic-med
```


© 2021 IP Infusion Inc. Proprietary

bgp enforce-first-as

Use this command to enforce the first AS for eBGP routes. This command specifies that any updates received from an external neighbor that do not have the neighbor's configured Autonomous System (AS) at the beginning of the AS_PATH in the received update must be denied. Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.

Using the `no` parameter with this command to disable this feature.

Command Syntax

```
bgp enforce-first-as

no bgp enforce-first-as
```

Parameters

None

Default

By default, enforce-first-as is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp enforce-first-as

(config)#router bgp 100
(config-router)#no bgp enforce-first-as
```

bgp extended-asn-cap

Use this command to configure a BGP router to send 4-octet ASN capabilities. If attempting to change the AS capability from 2 to 4 or 4 to 2, a prompt occurs to remove the VRF configuration (if it exists), and reconfiguration is required, because the route distinguisher (RD) configuration would have been created with the current (2 octet or 4 octet) capability, and must be reconfigured before attempting to change the capability.

While loading from a saved configuration with AS4 capability and BGP VRF configuration, the capability will not be changed because of the above described reason.

Use the `no` parameter with this command to prevent a BGP router from sending 4-octet ASN capabilities.

Command Syntax

```
bgp extended-asn-cap
```

```
no bgp extended-asn-cap
```

Parameters

None

Default

By default, the bgp extended ASN capability and Four-octet capabilities are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp extended-asn-cap
```


© 2021 IP Infusion Inc. Proprietary

bgp fast-external-failover

Use this command to reset a BGP session immediately, if the interface used for BGP connection goes down.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
bgp fast-external-failover
no bgp fast-external-failover
```

Parameters

None

Default

By default, fast-external failover is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp fast-external-failover
```

bgp graceful-restart

Use this command to enable BGP graceful-restart capabilities. The restart-time parameter is used for setting the maximum time that a graceful-restart neighbor waits to come back up after a restart. This value is applied to all neighbors unless you explicitly override it by configuring the corresponding value on the neighbor. The stalepath-time parameter is used to set the maximum time to preserve stale paths from a gracefully restarted neighbor. All stalepaths, unless reinstated by the neighbor after a re-establishment, will be deleted at the expiration of this timer.

Use the `no` parameter with this command to restore the router to its default state.

Command Syntax

```
bgp graceful-restart
bgp graceful-restart graceful-reset
bgp graceful-restart restart-time <1-3600>
bgp graceful-restart stalepath-time <1-3600>
no bgp graceful-restart
no bgp graceful-restart graceful-reset
no bgp graceful-restart restart-time
no bgp graceful-restart stalepath-time
```

Parameters

`graceful-reset`	The BGP daemon is not restarted, so that any changes in network configurations that cause BGP reset do not affect packet forwarding.
`restart-time`	Maximum time needed for neighbors to restart. Default is 90 seconds.
`<1-3600>`	Delay value in seconds.
`stalepath-time`	Maximum time to retain stale paths from restarting neighbors. Default is 360 seconds.
`<1-3600>`	Delay value in seconds.

Default

By default, the maximum time for neighbors to restart is 90 seconds.

By default, the maximum time to retain stale paths from restarting neighbors is 360 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#bgp graceful-restart

#configure terminal
(config)#router bgp 10
```


© 2021 IP Infusion Inc. Proprietary

```
(config-router)#no bgp graceful-restart
```

bgp g-shut

Use this command to gracefully shut down all BGP IPv4 sessions under this router. The BGP graceful shutdown feature reduces packet loss during maintenance activity.

Use the `no` parameter with this command to bring up all the sessions under this router after completion of maintenance activity using the `bgp g-shut` command.

Command Syntax

```
bgp g-shut
```

```
no bgp g-shut
```

Parameters

None

Default

By default, bgp g-shut is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp g-shut

#configure terminal
(config)#router bgp 100
(config-router)#no bgp g-shut
```


© 2021 IP Infusion Inc. Proprietary

bgp g-shut-capable

Use this command to enable the graceful shutdown capability at the router level and make available the graceful-shutdown related commands at the router and BGP neighbor levels.

Use the `no` parameter with this command to disable the graceful shutdown capability on a router.

Note: The graceful shutdown capability cannot be disabled on a router that is in a graceful shutdown state until it comes out this state--after the graceful shutdown has been initiated and the impacted BGP sessions are up again.

Command Syntax

```
bgp g-shut-capable
```

```
no bgp g-shut-capable
```

Parameters

None

Default

By default, the graceful shutdown capability is disabled at the router level

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp g-shut-capable

#configure terminal
(config)#router bgp 100
(config-router)#no bgp g-shut-capable
```

bgp g-shut-local-preference

Use this command to sets the local preference of the router to use during graceful shutdown. The local preference value indicates the preferred path when there are multiple paths to the same destination in a single routing database. The path with a higher preference value is the preferred one. The preferred path is sent to all routers and access servers in the local autonomous system.

Use the `no` parameter with this command to revert to the default setting.

Command Syntax

```
bgp g-shut-local-preference <0-4294967295>
no bgp g-shut-local-preference
```

Parameters

`<0-4294967295>` Local preference value

Default

By default, the local preference value is set to 0

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp g-shut-local-preference 22
```


© 2021 IP Infusion Inc. Proprietary

bgp log-neighbor-changes

Use this command to enable logging of status change messages without turning on debug bgp commands. OcNOS has many logging services for neighbor status, including `debug bgp fsm` and `debug bgp events`. However, these commands cause system performance degradation. If you need to log neighbor status changes only, IP Infusion Inc. recommends turning off all debug commands and using the `bgp log-neighbor-changes` command instead. A sample output of the log is:

```
%Protocol-Severity-Events: Message-text
```

A sample output of the log for an `interface down` event is:

```
%BGP-5-ADJCHANGE: neighbor 10.10.0.24 Down Interface flap
```

This command logs the following events:

- BGP Notification Received
- Erroneous BGP Update Received
- User reset request
- Peer time-out
- Peer Closing down the session
- Interface flap
- Router ID changed
- Neighbor deleted
- Member added to peer group
- Administrative shutdown
- Remote AS changed
- RR client configuration modification
- Soft reconfiguration modification

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
bgp log-neighbor-changes
no bgp log-neighbor-changes
```

Parameters

None

Default

By default, bgp log neighbor changes is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#router bgp 100
(config-router)#bgp log-neighbor-changes
```


© 2021 IP Infusion Inc. Proprietary

bgp nexthop-trigger delay

Use this command to set the delay time for nexthop address tracking. This command configures the delay interval between routing table walks for nexthop delay tracking, after which BGP does a routing table scan on receiving a nexthop change trigger from NSM. The time period determines how long BGP waits before it walks the full BGP table to determine which prefixes are affected by the nexthop changes, after it receives the trigger from NSM about one or more nexthop changes.

Use the `no` parameter with this command to reset the timer value to the default value.

Command Syntax

```
bgp nexthop-trigger delay <1-100>
no bgp nexthop-trigger delay
```

Parameter

`<1-100>`	Nexthop trigger delay interval in seconds

Default

By default, nexthop-trigger delay time is 5 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp nexthop-trigger delay 6

#configure terminal
(config)#no bgp nexthop-trigger delay
```

bgp nexthop-trigger enable

Use this command to enable nexthop address tracking. Nexthop address tracking is an event-driven notification system that monitors the status of routes installed in the Routing Information Base (RIB) and reports nexthop changes that affect internal BGP (iBGP) or external BGP (eBGP) prefixes directly to the BGP process. This improves the overall BGP convergence time, by allowing BGP to respond rapidly to nexthop changes for routes installed in the RIB.

If nexthop tracking is enabled after certain routes are learned, the registration of all nexthops for selected BGP routes is done after the nexthop tracking feature is enabled. If nexthop tracking is disabled, and if there are still some selected BGP routes, BGP de-registers the nexthops of all selected BGP routes from NSM.

Use the `no` parameter with this command to disable this feature. If the `no` command is given when nexthop tracking is in the process of execution, an error appears and nexthop tracking is not disabled. However, if the nexthop tracking timer is running at the time of negation, the nexthop tracking timer is stopped, and nexthop tracking is disabled.

Command Syntax

```
bgp nexthop-trigger enable
```

```
no bgp nexthop-trigger enable
```

Parameters

None

Default

By default, nexthop address tracking is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp nexthop-trigger enable
```


© 2021 IP Infusion Inc. Proprietary

bgp rfc1771-path-select

Use this command to set RFC 1771 compatible path selection.

Use the `no` parameter with this command to revert this setting.

Command Syntax

```
bgp rfc1771-path-select
no bgp rfc1771-path-select
```

Parameters

None

Default

Standard compatible path selection mechanism.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp rfc1771-path-select
```

bgp rfc1771-strict

Use this command to set the origin path attribute to “IGP” when the origin is a protocol such as RIP, OSPF, or ISIS as specified in RFC 1771. Otherwise, the origin is always set to “incomplete” which is the industry standard.

Use the `no` parameter with this command to revert this setting.

Command Syntax

```
bgp rfc1771-strict
```

```
no bgp rfc1771-strict
```

Parameters

None

Default

By default, bgp rfc1771 strict is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bgp rfc1771-strict
```


© 2021 IP Infusion Inc. Proprietary

bgp router-id

Use this command to manually configure a fixed router ID as a BGP router identifier. When this command is used to configure a fixed router ID, the current router identifier is overridden and the peers are reset.

Use the `no` parameter with this command to remove a manually configured fixed router ID.

Command Syntax

```
bgp router-id A.B.C.D
no bgp router-id
no bgp router-id A.B.C.D
```

Parameter

`A.B.C.D`	Router ID in an IPv4 address format

Default

Once the BGP router-id is elected, it may be re-elected in the following cases:

a. When an explicit BGP router-id is configured/un-configured

b. When the router's (global) router-id is set/unset (holds true when (a) is not applicable),

c. When the BGP process is cleared (holds true when both (a) & (b) are not applicable and the IP address(es) on the active interfaces are updated, which may result in a change in the router's router-id).

If no loopback interface is configured, the highest IP address is the BGP router-id.

When a loopback interface is configured, the BGP router-id is set to the IP address of the loopback interface.

Note: IP Infusion Inc. recommends that you always configure a router identifier to avoid unpredictable behavior if the address of a loopback interface changes.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp router-id 10.1.2.7

(config)#router bgp 100
(config-router)#no bgp router-id 10.1.2.7
```

bgp scan-time

Use this command to configure scanning intervals of BGP routers. This interval is the period after which router checks the validity of the routes in its database. To disable BGP scanning, set the scan-time interval to 0 seconds.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
bgp scan-time <0-60>
no bgp scan-time
no bgp scan-time <0-60>
```

Parameter

`<0-60>`	Scanning interval in seconds

Default

By default, scan-time interval is 60 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp scan-time 10
```


© 2021 IP Infusion Inc. Proprietary

bgp table-map

Use this command to enable or disable suppression/modification of incoming BGP updates to IP RIB/FIB table installation.

In a dedicated route reflector, all the routes it receives may not be required to be stored or only few selected routes need to be stored, because it may not lie in the data path.

Table maps are particularly useful to attain this restriction. Table-map command can be used in two ways:

- When a simple table-map command is given, the route map referenced in the table-map command shall be used to set certain properties (such as the traffic index) of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.
- When the option ‘filter’ is given in the table map command, the route map referenced is used to control whether a BGP route is to be downloaded to the IP RIB (hence the filter). A BGP route is not downloaded to the RIB if it is denied by the route map.

Use this command in Address Family mode to set the table map rule per an IPv4 or IPv6 family.

Use the `no` parameter with this command to remove the table-map rule.

Command Syntax

```
table-map WORD (|filter)
```

Parameter

`WORD`	Specify the route-map name to apply.
`filter`	Filer the routes. If present, the incoming routes are pruned as per the rule specified in route-map-name. If not, it is used to alter the incoming packet information.

Default

All BGP routes will be downloaded to IP RIB

Command Mode

Address Family IPv4 mode, and Address Family IPv6 mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to set the table-map command without filter for BGP for all address families.

```
#configure terminal
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#table-map abc
```

The following example shows how to set the table-map command with filter for BGP for all address families.

```
#configure terminal
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#table-map abc filter
```

The following example shows how to set the table-map command without filter for BGP for an IPv6 address family.

```
(config)#router bgp 100
(config-router)#address-family ipv6
(config-router-af)#table-map abc
```

The following example shows how to set the table-map command with filter for BGP for an IPv6 address family.

```
(config)#router bgp 100
(config-router)#address-family ipv6
(config-router-af)#table-map abc filter
```


© 2021 IP Infusion Inc. Proprietary

bgp update-delay

Use this command to set the update delay for a graceful-restart capable router. The update-delay value is the maximum time a graceful-restart capable router, which is restarting, will defer route-selection and advertisements to all its graceful-restart capable neighbors. This maximum time starts from the instance the first neighbor attains established state after restart. The restarting router prematurely terminates this timer when end-of-RIB markers are received from all its graceful-restart capable neighbors.

Use the `no` form of this command to set to the update delay to its default value.

Command Syntax

```
bgp update-delay <1-3600>
no bgp update-delay
no bgp update-delay <1-3600>
```

Parameters

`<1-3600>`	Delay interval in seconds

Default

By default, update-delay value is 120 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#bgp update-delay 345
```

clear bgp (A.B.C.D|X:X::X:X)

Use this command to reset a BGP neighbor address.

Command Syntax

```
clear bgp (A.B.C.D|X:X::X:X|WORD)
clear bgp (A.B.C.D|X:X::X:X) in
clear bgp (A.B.C.D|X:X::X:X) in prefix-filter
clear bgp (A.B.C.D|X:X::X:X) out
```

Parameters

`A.B.C.D`	IPv4 neighbor address.
`X:X::X:X`	IPv6 neighbor address.
`WORD`	Interface name
`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear bgp 3.3.3.3
```


© 2021 IP Infusion Inc. Proprietary

clear bgp *

Use this command to reset the BGP connection for all peers.

Command Syntax

```
clear bgp *
clear bgp * in
clear bgp * in prefix-filter
clear bgp * out
clear bgp * soft
clear bgp * soft in
clear bgp * soft out
clear ip bgp *
clear ip bgp * in
clear ip bgp * in prefix-filter
clear ip bgp * out
clear ip bgp * soft
clear ip bgp * soft in
clear ip bgp * soft out
clear ip bgp * ipv4 (unicast|multicast) in
clear ip bgp * ipv4 (unicast|multicast) in prefix-filter
clear ip bgp * ipv4 (unicast|multicast) out
clear ip bgp * ipv4 (unicast|multicast) soft
clear ip bgp * ipv4 (unicast|multicast) soft in
clear ip bgp * ipv4 (unicast|multicast) soft out
```

Parameters

`in`	Incoming advertised routes should be cleared.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
`in`	Clear incoming advertised routes.
`prefix-filter`	

	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear bgp *
#clear ip bgp * ipv4 unicast in prefix-filter
```


© 2021 IP Infusion Inc. Proprietary

clear bgp <1-4294967295>

Use this command to reset a BGP connection for all peers in a specified Autonomous System.

Command Syntax

```
clear bgp <1-4294967295>
clear bgp <1-4294967295> in
clear bgp <1-4294967295> in prefix-filter
clear bgp <1-4294967295> out
clear bgp <1-4294967295> soft
clear bgp <1-4294967295> soft in
clear bgp <1-4294967295> soft out
clear ip bgp <1-4294967295>
clear ip bgp <1-4294967295> in
clear ip bgp <1-4294967295> in prefix-filter
clear ip bgp <1-4294967295> out
clear ip bgp <1-4294967295> soft
clear ip bgp <1-4294967295> soft in
clear ip bgp <1-4294967295> soft out
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) in
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) in prefix-filter
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) out
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) soft
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) soft in
clear ip bgp <1-4294967295> ipv4 (unicast|multicast) soft out
```

Parameters

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
	Clear incoming advertised routes.
`in`	Clear incoming advertised routes.

`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear bgp 4294967277
#clear ip bgp 4294967277
```


© 2021 IP Infusion Inc. Proprietary

clear bgp dampening

Use this command to reset BGP route flap dampening information.

Command Syntax

```
clear bgp ipv4 (unicast|multicast) dampening
clear bgp ipv4 (unicast|multicast) dampening A.B.C.D/M
clear ip bgp dampening
clear ip bgp dampening A.B.C.D/M
clear ip bgp ipv4 (unicast|multicast) dampening
clear ip bgp ipv4 (unicast|multicast) dampening A.B.C.D/M
```

Parameters

`ipv4`	IPv4 address family.
`multicast`	Multicast prefixes
`unicast`	Unicast prefixes
`A.B.C.D/M`	IP prefix (network/length), for example, 35.0.0.0/8

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp dampening 10.10.0.121/24
#clear ip bgp ipv4 unicast dampening
```

© 2021 IP Infusion Inc. Proprietary

clear bgp external

Use this command to reset the BGP connection for all external peers.

Command Syntax

```
clear bgp external
clear bgp external in
clear bgp external in prefix-filter
clear bgp external out
clear bgp external soft
clear bgp external soft in
clear bgp external soft out
clear ip bgp external
clear ip bgp external in
clear ip bgp external in prefix-filter
clear ip bgp external out
clear ip bgp external soft
clear ip bgp external soft in
clear ip bgp external soft out
clear ip bgp external ipv4 (unicast|multicast) in
clear ip bgp external ipv4 (unicast|multicast) in prefix-filter
clear ip bgp external ipv4 (unicast|multicast) out
clear ip bgp external ipv4 (unicast|multicast) soft
clear ip bgp external ipv4 (unicast|multicast) soft in
clear ip bgp external ipv4 (unicast|multicast) soft out
```

Parameters

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
`in`	Clear incoming advertised routes.
`prefix-filter`	

© 2021 IP Infusion Inc. Proprietary

	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip bgp external
```

clear bgp flap-statistics

Use this command to reset BGP flap statistics.

Command Syntax

```
clear bgp ipv4 (unicast|multicast) flap-statistics
clear bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M vrf (all | default |
  VRFNAME )
clear bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M
clear ip bgp flap-statistics
clear ip bgp flap-statistics A.B.C.D/M
clear ip bgp ipv4 (unicast|multicast) flap-statistics
clear ip bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M vrf (all | default
  | VRFNAME )
clear ip bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M
```

Parameters

`ipv4`	IPv4 address family.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
`A.B.C.D/M`	IP prefix (network/length), for example, 35.0.0.0/8
`VRFNAME`	VPN routing or forwarding instance name
`all`	All VRF's
`default`	Default VRF

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp flap-statistics
#clear ip bgp ipv4 unicast flap-statistics
```


© 2021 IP Infusion Inc. Proprietary

clear bgp peer-group

Use this command to reset the BGP connection for all members of a peer group.

Command Syntax

```
clear bgp peer-group WORD
clear bgp peer-group WORD in
clear bgp peer-group WORD in prefix-filter
clear bgp peer-group WORD out
clear bgp peer-group WORD soft
clear bgp peer-group WORD soft in
clear bgp peer-group WORD soft out
clear ip bgp peer-group WORD
clear ip bgp peer-group WORD in
clear ip bgp peer-group WORD in prefix-filter
clear ip bgp peer-group WORD out
clear ip bgp peer-group WORD soft
clear ip bgp peer-group WORD soft in
clear ip bgp peer-group WORD soft out
clear ip bgp peer-group WORD ipv4 (unicast|multicast) in
clear ip bgp peer-group WORD ipv4 (unicast|multicast) in prefix-filter
clear ip bgp peer-group WORD ipv4 (unicast|multicast) out
clear ip bgp peer-group WORD ipv4 (unicast|multicast) soft
clear ip bgp peer-group WORD ipv4 (unicast|multicast) soft in
clear ip bgp peer-group WORD ipv4 (unicast|multicast) soft out
```

Parameters

`WORD`	BGP peer-group name.
`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
	Clear incoming advertised routes.

`in`	Clear incoming advertised routes.
`prefix-filter`	
	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp peer-group P1
```


© 2021 IP Infusion Inc. Proprietary

clear bgp statistics

Use this command to reset all BGP statistics.

Command Syntax

```
clear bgp statistics
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear bgp statistics
```

clear ip bgp A.B.C.D

Use this command to reset an IPv4 BGP neighbor address.

Command Syntax

```
clear ip bgp (A.B.C.D|WORD) in
clear ip bgp A.B.C.D in prefix-filter
clear ip bgp (A.B.C.D|WORD) out
clear ip bgp (A.B.C.D|WORD) soft
clear ip bgp (A.B.C.D|WORD) soft in
clear ip bgp (A.B.C.D|WORD) soft out
clear ip bgp A.B.C.D ipv4 (unicast|multicast) in
clear ip bgp A.B.C.D ipv4 (unicast|multicast) in prefix-filter
clear ip bgp A.B.C.D ipv4 (unicast|multicast) out
clear ip bgp A.B.C.D ipv4 (unicast|multicast) soft
clear ip bgp A.B.C.D ipv4 (unicast|multicast) soft in
clear ip bgp A.B.C.D ipv4 (unicast|multicast) soft out
```

Parameters

`A.B.C.D`	IPv4 address
`WORD`	Interface name
`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

© 2021 IP Infusion Inc. Proprietary

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp 35.0.0.1 in
```

clear ip bgp A.B.C.D vrf

Use this command to reset the VPN Routing/Forwarding (VRF) instance for a peer address.

Command Syntax

```
clear ip bgp A.B.C.D vrf WORD
clear ip bgp A.B.C.D vrf WORD in
clear ip bgp A.B.C.D vrf WORD out
clear ip bgp A.B.C.D vrf WORD soft
clear ip bgp A.B.C.D vrf WORD soft in
clear ip bgp A.B.C.D vrf WORD soft out
```

Parameters

`A.B.C.D`	IPv4 address
`WORD`	VPN routing/forwarding instance name
`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp 35.0.0.1 vrf
```


© 2021 IP Infusion Inc. Proprietary

clear ip bgp table-map

Use this command to apply the modified table map or route map rules to the BGP routes in the existing IP routing table.

Command Syntax

```
clear ip bgp table-map (vrf (VRFNAME|all|default))
clear ip bgp ipv4 (unicast | multicast) table-map(vrf (VRFNAME|all|default))
```

Parameters

`vrf`	Select a VPN Routing/Forwarding Instance.
`VRFNAME`	Specify a VPN Routing/Forwarding instance name.
`all`	Select all VRFs.
`default`	Select default VRFs.
`unicast`	Unicast prefixes.
`multicast`	Multicast prefixes.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp table-map vrf all
```

debug bgp

Use this command to enable all BGP troubleshooting functions. Use this command without any parameters to turn on normal bgp debug information.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug bgp (all|)
debug bgp bfd
debug bgp dampening
debug bgp events
debug bgp filters
debug bgp fsm
debug bgp keepalives
debug bgp mpls
debug bgp nht
debug bgp nsm
debug bgp updates
debug bgp updates (in|out)
debug bgp vpls
no debug bgp (all|)
no debug bgp bfd
no debug bgp dampening
no debug bgp events
no debug bgp filters
no debug bgp fsm
no debug bgp keepalives
no debug bgp mpls
no debug bgp nht
no debug bgp nsm
no debug bgp updates
no debug bgp vpls
undebug bgp (all|)
undebug bgp bfd
undebug bgp dampening
undebug bgp events
undebug bgp filters
undebug bgp fsm
undebug bgp keepalives
```


© 2021 IP Infusion Inc. Proprietary

```
undebug bgp mpls
undebug bgp nht
undebug bgp nsm
undebug bgp updates
undebug bgp vpls
```

Parameters

`all`	Used only with the `no` form; turns off all debugging for BGP
`bfd`	Enable debugging for BGP Bidirectional Forwarding Detection
`dampening`	Enable debugging for BGP dampening
`events`	Enable debugging for BGP events
`filters`	Enable debugging for BGP filters
`fsm`	Enable debugging for BGP Finite State Machine (FSM)
`keepalives`	Enable debugging for BGP keepalives
`mpls`	Enable debugging for BGP Multiprotocol Label Switching (MPLS)
`nht`	Enable debugging for BGP NHT
`nsm`	Enable debugging for NSM messages
`updates`	Enable debugging for BGP updates
`in`	Debug inbound updates
`out`	Debug outbound updates
`vpls`	Enable debugging for BGP Virtual Private LAN Service (VPLS)

Command Mode

Privileged Exec mode and Configure Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug bgp
#debug bgp events
```

distance bgp

Use this command to define an administrative distance. A distance is a rating of trustworthiness of a router. The higher the distance the lower the trust rating. Administrative distances can be set for external, internal and local routes. External paths are routes learned from a neighbor outside of the AS. Internal routes are routes learned from another router within the same AS. Local routes are for a router that is redistributed from another process.

If the administrative distance is changed, it could create inconsistency in the routing table and obstruct routing. Use this command in Address Family mode to set the administrative distance per an IPv4 family.

Use the `no` parameter with this command to remove an administrative distance.

Command Syntax

```
distance bgp <1-255> <1-255> <1-255>
no distance bgp
no distance bgp <1-255> <1-255> <1-255>
```

Parameters

`<1-255>`	Distance for BGP external routes
`<1-255>`	Distance for BGP internal routes
`<1-255>`	Distance for BGP local routes

Command Mode

Address Family IPv4 mode, Address Family IPv6 mode

Defaults

Default distance for external routes is 20.

Default distance for internal routes is 200.

Default distance for local routes is 200.

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to set the administrative distance for BGP for all address families.

```
#configure terminal
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#distance bgp 34 23 15
```


© 2021 IP Infusion Inc. Proprietary

exit-address-family

Use this command to exit Address-Family-vrf, Address-Family-vpnv4 mode.

For information on how to enter the address family mode (IPv4, VPNv4), see address-family.

Command Syntax

```
exit-address-family
```

Parameters

None

Default

No default value is specified

Command Mode

Address Family-vrf and Address Family-vpnv4 mode.

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following examples shows the change in the prompt after using this command.

```
#configure terminal
(config)#router bgp 100
(config-router)#address-family ipv4 multicast
(config-router-af)#exit-address-family
(config-router)#
```

ip as-path access-list

Use this command to define a BGP Autonomous System (AS) path access list. A named community list is a filter based on regular expressions. If the regular expression matches the specified string representing the AS path of the route, then the permit or deny condition applies. Use this command to define the BGP access list globally; use the neighbor router configuration command to apply a specific access list.

Use the no parameter with this command to disable use of the access list.

Command Syntax

```
ip as-path access-list WORD (deny|permit) LINE
no ip as-path access-list WORD
no ip as-path access-list WORD (deny|permit) LINE
```

Parameters

`WORD`	Access list name
`deny`	Reject packets
`permit`	Forward packets
`LINE`	An ordered list as a regular expression

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip as-path access-list mylist deny ^65535$
```


© 2021 IP Infusion Inc. Proprietary

ip community-list <1-99>

Use this command to specify a standard community list (1 to 99) that specifies BGP community attributes.

Use the `no` parameter with this command to delete the community list entry.

Command Syntax

```
ip community-list <1-99> (deny|permit)
ip community-list <1-99> (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]
no ip community-list <1-99> (deny|permit)
no ip community-list <1-99> (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]
```

Parameters

`deny`	Reject the community
`permit`	Accept the community
`AA:NN`	Community number
`internet`	Advertise routes to the internet community
`local-AS`	Do not advertise routes to external BGP peers
`no-advertise`	Do not advertise routes to other BGP peers
`no-export`	Do not advertise routes outside of Autonomous System boundary

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip community-list 55 permit 7675:80 7675:90

(config)#no ip community-list 55 permit 7675:80 7675:90
```

ip community-list <100-500>

Use this command to specify an expanded community list (100 to 500) that specifies BGP community attributes.

Use the `no` parameter with this command to delete the community list entry.

Command Syntax

```
ip community-list <100-500> (deny|permit)
ip community-list <100-500> (deny|permit) LINE
no ip community-list <100-500>
no ip community-list <100-500> (deny|permit) LINE
```

Parameters

`deny`	Reject community
`permit`	Accept community
`LINE`	An ordered list as a regular expression

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip community-list 225 permit 6789906
(config)#ip community-list expanded CLIST permit .*
```


© 2021 IP Infusion Inc. Proprietary

ip community-list expanded

Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32-bits long.

There are two kinds of community-lists: expanded and standard. The standard community-list defines the community attributes in a specified format and not with regular expressions. The expanded community-list defines the community attributes with regular expressions.Use the `no` parameter with this command to delete the community list entry.

Command Syntax

```
ip community-list expanded WORD (deny|permit) LINE
no ip community-list expanded WORD
no ip community-list expanded WORD (deny|permit) LINE
```

Parameters

`WORD`	Community list name
`deny`	Reject community
`permit`	Accept community
`LINE`	An ordered list as a regular expression

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip community-list 125 permit 6789906
(config)#ip community-list expanded CLIST permit .*
```

ip community-list standard

Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32-bits long. There are two kinds of community-lists: expanded and standard. The standard community-list defines the community attributes in a specified format without regular expressions. The expanded community-list defines the community attributes with regular expressions.

Use this command to add a standard community-list entry. The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value that does not match the standard community value is automatically treated as expanded.

Use the `no` parameter with this command to delete the standard community-list entry.

Command Syntax

```
ip community-list standard WORD (deny|permit)
ip community-list standard WORD (deny|permit) [AA:NN|internet|local-AS|no-
  advertise|no-export]
no ip community-list standard WORD (deny|permit) [AA:NN|internet|local-AS|no-
  advertise|no-export]
```

Parameters

`WORD`	Community list name
`deny`	Reject the community
`permit`	Accept the community
`AA:NN`	Community number
`internet`	Advertise routes to the internet community
`local-AS`	Do not advertise routes to external BGP peers
`no-advertise`	Do not advertise routes to other BGP peers
`no-export`	Do not advertise routes outside of Autonomous System boundary

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip community-list standard CLIST permit 7675:80 7675:90 no-export
(config)#ip community-list 34 permit 5675:50 no-advertise
```


© 2021 IP Infusion Inc. Proprietary

ip community-list WORD

Use the community-list commands to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. There are two kinds of community-lists: the expanded and standard. The `standard community-list` defines the community attributes in a specified format and not with regular expressions. The `expanded community-list` defines the community attributes with regular expressions.

Use the `no` parameter with this command to delete the community list entry.

Command Syntax

```
ip community-list WORD (deny|permit)
ip community-list WORD (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]
no ip community-list WORD
no ip community-list WORD (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]
```

Parameters

`WORD`	Community list name
`deny`	Reject the community
`permit`	Accept the community
`AA:NN`	Community number
`internet`	Advertise routes to the internet community
`local-AS`	Do not advertise routes to external BGP peers
`no-advertise`	Do not advertise routes to other BGP peers
`no-export`	Do not advertise routes outside of Autonomous System boundary

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip community-list mylist permit 7675:80 7675:90

(config)#no ip community-list mylist permit 7675:80 7675:90
```

ip extcommunity-list <1-99>

Use this command to create an entry for a standard extended community list.

Use the `no` parameter with this command to delete the community-list entry.

Command Syntax

```
ip extcommunity-list <1-99> (deny|permit) LINE (rt|soo)
no ip extcommunity-list <1-99> (deny|permit) LINE (rt|soo)
```

Parameters

`deny`	Reject community
`permit`	Accept community
`LINE`	One of the following:
`rt`	Route target extended community in aa:nn or IPaddr:nn format
`soo`	Site-of-origin extended community in aa:nn or IPaddr:nn format

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip extcommunity-list 3 permit rt 10.10.23.123:67

(config)#ip extcommunity-list 25 deny soo 1465:22
```


© 2021 IP Infusion Inc. Proprietary

ip extcommunity-list <100-500>

Use this command to create an extended community list.

Use the `no` parameter with this command to delete the community-list entry.

Command Syntax

```
ip extcommunity-list <100-500> (deny|permit) LINE
no ip extcommunity-list <100-500> (deny|permit) LINE
```

Parameters

`<100-500>`	Extended community list number (expanded)
`deny`	Reject the community
`permit`	Accept the community
`LINE`	Any regular expression:

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip extcommunity-list 125 permit 4567:335

(config)#ip extcommunity-list 231 deny *.
```

ip extcommunity-list expanded

Use this command to create an expanded community list.

Use the `no` parameter with this command to delete the expanded community-list entry.

Command Syntax

```
ip extcommunity-list expanded WORD
ip extcommunity-list expanded WORD (deny|permit) LINE
no ip extcommunity-list expanded WORD
no ip extcommunity-list expanded WORD (deny|permit) LINE
```

Parameters

`WORD`	Expanded community list name
`deny`	Reject the community
`permit`	Accept the community
`LINE`	One of the following:
`rt`	Route target extended community in aa:nn or IPaddr:nn format
`soo`	Site-of-origin extended community in aa:nn or IPaddr:nn format

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip extcommunity-list 125 permit 4567335
(config)#ip extcommunity-list expanded CLIST permit .*
```


© 2021 IP Infusion Inc. Proprietary

ip extcommunity-list standard

Use this command to create and delete a standard extended-community list. The extended community attribute is 8 bytes in 2 formats. The sub-type can be route target (`rt`) or site of origin (`soo`). Thus, the sub-type of each community must be specified when creating the extended community list. Regarding the formats, an extended community is based on a 6-byte value. These 6-bytes are represented in 4-btye:2-byte format, and may be entered in one of the following forms:

- Format 1, aa.nn: The 16-bit value of the AS (aa) number is represented in the higher-order 4-bytes. If the extended ASN capability is enabled, the AS number is represented using higher-order 4-bytes. The nn assigned value is represented in the low-order 2-bytes in both cases.
- Format 2, IPaddr:nn: In this format, the higher-order 4-bytes are used to represent the IP address, and the low-order 2-bytes are used to represent the assigned value.

Use the `no` parameter with this command to delete the extended-community-list entry.

Command Syntax

```
ip extcommunity-list standard WORD (deny|permit) (rt|soo) (aa:nn)
no ip extcommunity-list standard WORD (deny|permit) (rt|soo) (aa:nn)
```

Parameters

`WORD`	Extended community list name
`deny`	Reject the community
`permit`	Accept the community
`rt`	Route target extended community in aa:nn or IPaddr:nn format
`soo`	Site-of-origin extended community in aa:nn or IPaddr:nn format

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip extcommunity-list standard 36 permit rt 5675:50
(config)#ip extcommunity-list standard CLIST permit soo 10.10.32.15:70
```

l2vpn-unnumbered-mode

Use this command to configure the unnumbered peer with all the neighbor configs applicable in L2VPN EVPN address family.

Use the `exit` parameter with this command to leave L2VPN unnumbered mode.

Command Syntax

```
bgp l2vpn-unnumbered-mode
exit-l2vpn-unnumbered-mode
```

Parameters

None

Applicability

No default value is specified

Command Mode

Address-family IPv4 Unicast Mode

Applicability

This command was introduced in OcNOS-OTN version 4.2.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#address-family l2vpn evpn
(config-router-af)#bgp l2vpn-unnumbered-mode
(config-router-l2vpn-unnum)#
```


© 2021 IP Infusion Inc. Proprietary

match ip peer

Use this command to apply policies based on the route source of which the BGP TCP/IP session formed using an IPv4 address in the update message.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
match ip peer (<1-199>|<1300-2699>|WORD)
no match ip peer (<1-199>|<1300-2699>|WORD)
```

Parameters

`<1-199>`	IP access-list number
`<1300-2699>`	IP access-list number (expanded range)
`WORD`	Access-list name

Default

By default, import bgp route is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#route-map in-A permit 10
(route-map)#match ip peer 1
```

max-paths

Use this command to set the number of equal-cost multi-path (ECMP) routes for eBGP or iBGP. You can install multiple BGP paths to the same destination to balance the load on the forwarding path.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
max-paths (ebgp|ibgp|) <2-64>
no max-paths ebgp (<2-64>|)
no max-paths ibgp (<2-64>|)
```

Parameters

`ebgp`	eBGP ECMP session
`ibgp`	iBGP ECMP session
`<2-64>`	Number of routes

Default

Available for the IPv4 and IPv6 unicast addresses.

Command Mode

Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures 7 routes for ECMP for iBGP.

```
#configure terminal
(config)#router bgp 11
(config-router)#address-family ipv4 unicast
(config-router-af)#max-paths ibgp 7
```


© 2021 IP Infusion Inc. Proprietary

neighbor activate

Use this command to enable the exchange of specific address family routes with a neighboring router. After a TCP connection is opened with a neighboring router, use this command to enable or disable the exchange of address family information. To enable the exchange of multicast and VPNv4 address prefix types, activate neighbors using this command in address family mode.

Use the `no` parameter with this command to disable exchange of information with a neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) activate
no neighbor (A.B.C.D|X:X::X:X|WORD) activate
```

For L2VPN-unnumbered mode:

```
neighbor WORD activate
no neighbor WORD activate
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default activate is disabled. For all address-families, use this command to enable a neighbor to exchange routing information of a specific address-family with a neighbor.

Command Mode

Address Family mode and l2vpn-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#address-family vpnv4 unicast
(config-router-af)#neighbor 10.10.20.1 activate

(config)#router bgp 100
(config-router)#address-family l2vpn evpn
(config-router-af)#bgp l2vpn-unnumbered-mode
(config-router-l2vpn-unnum)#neighbor eth1 activate
```

neighbor advertisement-interval

Use this command to set a minimum interval between the sending of BGP routing updates. To reduce the flapping of routes, set a minimum advertisement interval so that the BGP routing updates are sent only per interval seconds. BGP dampening can also be used to control the effects of flapping routes.

Use the `no` parameter with this command to set the interval time to default.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) advertisement-interval <0-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) advertisement-interval
no neighbor (A.B.C.D|X:X::X:X|WORD) advertisement-interval <0-65535>
```

For BGP ununbered mode:

```
neighbor WORD advertisement-interval <0-65535>
no neighbor WORD advertisement-interval
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<0-65535>`	Advertisement interval value in seconds

Default

By default, neighbor value for ebgp peer is 30 seconds and IBGP peer is 5 seconds

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.3 advertisement-interval 45
```

For unnumbered peer this configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 advertisement-interval 20
```


© 2021 IP Infusion Inc. Proprietary

neighbor allowas-in

Use this command to advertise prefixes (routes) even when the source of the prefixes is from the same Autonomous System (AS) number.

Use this command in a scenario where two routers at different locations use the same Autonomous System number and are connected via an ISP. Once prefixes arrive from one branch at the ISP, they are tagged with the customer's AS number. By default, when the ISP passes the prefixes to the other router, the prefixes are dropped if the other router uses the same AS number. Use this command to advertise the prefixes at the other side. Control the number of times an AS number is advertised by specifying a number.

In a hub and spoke configuration in a VPN, a PE (Provider Edge) router advertises all prefixes containing duplicate AS numbers. Use this command to configure two VRFs on each PE router to receive and advertise prefixes. One of the VRFs receives prefixes with AS numbers from all PE routers and then advertises them to neighboring PE routers. The other VRF receives prefixes with AS numbers from the CE (Customer Edge) router and advertises them to all PE routers in the hub and spoke configuration.

Use the `no` parameter with this command to reset to default.

For unnumbered peer IPv4 unicast mode commands are configured under v4-unnumbered-mode.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) allowas-in
neighbor (A.B.C.D|X:X::X:X|WORD) allowas-in <1-10>
no neighbor (A.B.C.D|X:X::X:X|WORD) allowas-in
```

For v4-unnumbered mode:

```
neighbor WORD allowas-in
neighbor WORD allowas-in <1-10>
no neighbor WORD allowas-in
```

Parameters

`A.B.C.D`	IPv4 neighbor address.
`X:X::X:X`	IPv6 neighbor address.
`WORD`	Name of peer group.

Note: For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.

`<1-10>`	Number of times to allow the advertisement of an AS number

Default

By default, when the ISP passes the prefixes to the other router, the prefixes are dropped if the other router uses the same AS number, default number of local AS is 3

Command Mode

v4-unnumbered mode and Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.0.1 allowas-in 3

#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 allowas-in 3

#con terminal
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 allowas-in 6
```

For unnumbered peer configs in L2vpn evpn mode are configured under l2vpn-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family l2vpn evpn
(config-router-af)#neighbor eth1 allowas-in 7
```

 © 2021 IP Infusion Inc. Proprietary

neighbor as-origination-interval

Use this command to set the minimum interval between sending of AS-origination routing updates.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) as-origination-interval <1-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) as-origination-interval
no neighbor (A.B.C.D|X:X::X:X|WORD) as-origination-interval <1-65535>
```

For BGP unnumbered mode:

```
neighbor WORD as-origination-interval interval <0-65535>
no neighbor WORD as-origination-interval
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-65535>`	AS origination interval in seconds

Default

By default, neighbor as origination interval is 15 seconds

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.75 as-origination-interval 555
```

For unnumbered peer this configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 as-origination-interval 50
```

neighbor attribute-unchanged

Use this command to advertise unchanged BGP attributes to the specified neighbor.

Use the `no` parameter with this command to disable this function.

For unnumbered peer IPv4 unicast mode commands are configured under v4-unnumbered-mode.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) attribute-unchanged ({ as-path|next-hop|med }|)
no neighbor (A.B.C.D|X:X::X:X|WORD) attribute-unchanged (({ as-path|next-hop|
  med }|)
```

For v4-unnumbered mode:

```
neighbor WORD attribute-unchanged ({ as-path|next-hop|med }|)
no neighbor WORD attribute-unchanged (({ as-path|next-hop|med }|)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`as-path`	AS path attribute
`next-hop`	Nexthop attribute
`med`	Multi-exit discriminator attribute

Default

By default, the neighbor attribute-unchanged is disabled

Command Mode

Address Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.0.75 attribute-unchanged as-path med

(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#OcNOS(config-router-v4-unnum)#neighbor eth1
attribute-unchanged as-path
```


© 2021 IP Infusion Inc. Proprietary

neighbor authentication-key

Use this command to enable message digest5 (MD5) authentication on a TCP connection between two BGP peers. Configuring MD5 authentication between two BGP peers, means that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be established.

Use the `no` parameter with this command to delete the MD5 authentication.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) authentication-key (0 | 1 |) <WORD>
<WORD> plain text password
neighbor (A.B.C.D|X:X::X:X|WORD) authentication-key <WORD>
<WORD> encrypted password
no neighbor (A.B.C.D|X:X::X:X|WORD) authentication-key <WORD>
<WORD> encrypted password
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of the BGP peer group
`0`	Unencrypted password
`WORD`	Unencrypted password (maximum length 80 characters)
`1`	Encrypted password (default)
`WORD`	Encrypted password (maximum length 162 characters)

Default

Not applicable

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 11
(config-router)#neighbor 10.10.0.73 authentication-key 0 myPass
(config-router)#no neighbor 10.10.0.73 authentication-key 0xba76ef302e2f20af
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 authentication-key 0 key1
```

neighbor capability dynamic

Use this command to enable the dynamic capability for a specific peer. This command allows a BGP speaker to advertise or withdraw an address family capability to a peer in a non-disruptive manner.

Use the `no` parameter with this command to disable the dynamic capability.

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) capability dynamic
no neighbor (A.B.C.D|X:X::X:X|WORD) capability dynamic
```

For v4-unnumbered mode:

```
neighbor WORD capability dynamic
no neighbor WORD capability dynamic
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor capability dynamic is disabled

Command Mode

Router mode and Address Family v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.1 capability dynamic

(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 activate
(config-router-v4-unnum)#neighbor eth1 capability dynamic
```


© 2021 IP Infusion Inc. Proprietary

neighbor capability graceful-restart

Use this command to advertise the graceful restart capability to its neighbor. This configuration indicates that the BGP speaker has the ability to preserve its forwarding state for the address family when BGP restarts.

You must first specify a neighbor's `remote-as` identification number assigned by the neighbor router.

Note: The graceful restart capability is advertised only when the graceful restart capability has been enabled using the bgp graceful-restart command.

Use the `no` parameter with this command to not advertise the graceful restart capability to its neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) capability graceful-restart
no neighbor (A.B.C.D|X:X::X:X|WORD) capability graceful-restart
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, the graceful-restart is disabled

Command Mode

Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.10.50 capability graceful-restart
```

neighbor capability orf prefix-list

Use this command to enable Outbound Router Filtering (ORF) and advertise the ORF capability to its neighbors. The ORFs send and receive capabilities to lessen the number of updates exchanged between neighbors. By filtering updates, this option minimizes generating and processing of updates.

The two routers exchange updates to maintain the ORF for each router:

- The local router advertises the ORF capability in `send` mode.
- The remote router receives the ORF capability in `receive` mode, applying the filter as outbound policy.

Only an individual router or a peer group can be configured to be in `receive` or `send` mode. A peer-group member cannot be configured to be in `receive` or `send` mode.

Use the `no` parameter with this command to disable this function.

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) capability orf prefix-list (both|receive|send)
no neighbor (A.B.C.D|X:X::X:X|WORD) capability orf prefix-list (both|receive|send)
```

For v4-unnumbered mode:

```
neighbor WORD capability orf prefix-list (both|receive|send)
no neighbor WORD capability orf prefix-list (both|receive|send)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`both`	The local router can send ORF entries to its peer, as well as receive ORF entries from its peer.
`receive`	The local router is willing to receive ORF entries from its peer
`send`	The local router is willing to send ORF entries to its peer

Default

By default, the orf prefix-list is disabled

Command Mode

Router Address Family (IPv4 unicast, IPv4 multicast, IPv6, v4-unnumbered) mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
```


© 2021 IP Infusion Inc. Proprietary

```
(config-router-af)#neighbor 10.10.0.5 capability orf prefix-list both
(config-router-af)#neighbor effe:2897::0003:3ed5 capability orf prefix-list
receive

(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 capability orf prefix-list both
```

neighbor capability route-refresh

Use this command to advertise to peer about route refresh capability. If route refresh capability is supported, then router can dynamically request that the peer re-advertises its Adj-RIB-Out.

Use the `no` parameter with this command to disable this function

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) capability route-refresh
no neighbor (A.B.C.D|X:X::X:X|WORD) capability route-refresh
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor capability route refresh is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.1 capability route-refresh
```


© 2021 IP Infusion Inc. Proprietary

neighbor collide-established

Use this command to include a neighbor already in an established state for conflict resolution when a TCP connection collision is detected. This command is not required for most network deployments, so users should only use this command when required.

Note: The associated functionality of including an “established” neighbor into TCP connection collision conflict resolution is automatically enabled when a neighbor is configured for BGP graceful-restart.

Use the `no` option with this command to turn this feature off.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) collide-established
no neighbor (A.B.C.D|X:X::X:X|WORD) collide-established
```

For BGP unnumbered mode:

```
neighbor WORD collide-established
no neighbor WORD collide-established
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor collide is disabled

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 3.3.3.3 collide-established
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 collide-established
```

neighbor default-originate

Use this command to allow a BGP local router to send the default route 0.0.0.0 to a neighbor to use as a default route. This command can be used with standard or extended access lists.

Use the `no` parameter with this command to send no route as a default.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) default-originate
neighbor (A.B.C.D|X:X::X:X|WORD) default-originate route-map WORD
no neighbor (A.B.C.D|X:X::X:X|WORD) default-originate
no neighbor (A.B.C.D|X:X::X:X|WORD) default-originate route-map WORD
```

For v4-unnumbered mode:

```
neighbor WORD default-originate
neighbor WORD default-originate route-map WORD
no neighbor WORD default-originate
no neighbor WORD default-originate route-map WORD
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Route map name

Default

By default, neighbor default originate is disabled

Command Mode

Route Address Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.10.1 default-originate route-map myroute
```

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

```
#con terminal
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 default-originate
```


© 2021 IP Infusion Inc. Proprietary

neighbor description

Use this command to associate a description with a neighbor. This command helps to identify a neighbor quickly. This command is useful for an ISP that has multiple neighbor relationships.

Use the `no` parameter with this command to remove the description.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) description LINE
no neighbor (A.B.C.D|X:X::X:X|WORD) description
no neighbor (A.B.C.D|X:X::X:X|WORD) description LINE
```

For BGP unnumbered mode:

```
neighbor WORD description LINE
no neighbor WORD description
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`LINE`	Neighbor description (up to 80 characters)

Default

By default, the neighbor description is disabled

Command Mode

Router mode and Address Family and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 1.2.3.4 description Backup router for sales

(config)#router bgp 100
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 description Bank of America
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 description unnbered-peer1
```

neighbor disallow-infinite-holdtime

Use this command to disallow configuration of infinite hold-time. This command enables the local BGP speaker to reject a hold-time of “0” seconds from a peer (during exchange of open messages) or a user (during configuration).

The `no` form of this command allows the BGP speaker to accept a hold-time of “0” from a peer or during configuration.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) disallow-infinite-holdtime
no neighbor (A.B.C.D|X:X::X:X|WORD) disallow-infinite-holdtime
```

For BGP unnumbered mode:

```
neighbor WORD disallow-infinite-holdtime
no neighbor WORD disallow-infinite-holdtime
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor disallow infinite holdtime is disabled

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config-router)#neighbor 10.11.4.26 disallow-infinite-holdtime
(config-router)#neighbor 3ffe::45 disallow-infinite-holdtime
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 disallow-infinite-holdtime
```


© 2021 IP Infusion Inc. Proprietary

neighbor distribute-list

Use this command to filter route updates from a particular BGP neighbor. Use only one distribute list per BGP neighbor.

Use the `no` parameter with this command to remove an entry.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) distribute-list (<1-199>|<1300-2699>|WORD)
  (in|out)
no neighbor (A.B.C.D|X:X::X:X|WORD) distribute-list (<1-199>|<1300-2699>|WORD)
  (in|out)
```

For v4-unnumbered mode:

```
neighbor WORD distribute-list (<1-199>|<1300-2699>|WORD) (in|out)
no neighbor WORD distribute-list (<1-199>|<1300-2699>|WORD) (in|out)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-199>`	IP access-list number
`<1300-2699>`	IP access-list number (expanded-range)
`WORD`	Access-list name
`in`	Filter incoming advertised routes
`out`	Filter outgoing advertised routes

Default

By default, neighbor distribute list is disabled

Command Mode

Address Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 1.2.3.4 distribute-list mylist out
```

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 distribute-list list1 in
```

© 2021 IP Infusion Inc. Proprietary

neighbor dont-capability-negotiate

Use this command to disable capability negotiation. This command is used to allow compatibility with older BGP versions that have no capability parameters used in open messages between peers.

Use the `no` parameter with this command to enable capability negotiation.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) dont-capability-negotiate
no neighbor (A.B.C.D|X:X::X:X|WORD) dont-capability-negotiate
```

For BGP unnumbered mode:

```
neighbor WORD dont-capability-negotiate
no neighbor WORD dont-capability-negotiate
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, capability negotiation is disabled

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.34 dont-capability-negotiate
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 dont-capability-negotiate
```


© 2021 IP Infusion Inc. Proprietary

neighbor ebgp-multihop

Use this command to accept and try BGP connections to external peers on indirectly connected networks. Multihop is not established if the only route to the multihop peer is a default route. This avoids loop formation.

Use the `no` parameter with this command to return to the default.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop
neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop <1-255>
no neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop
no neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop <1-255>
```

For BGP unnumbered mode:

```
neighbor WORD ebgp-multihop
neighbor WORD ebgp-multihop <1-255>
no neighbor WORD ebgp-multihop
no neighbor WORD ebgp-multihop <1-255>
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-255>`	Maximum hop count

Default

By default, maximum hop count is 255

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.34 remote-as 20
(config-router)#neighbor 10.10.10.34 ebgp-multihop 5
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 ebgp-multihop
```

neighbor enforce-multihop

Use this command to enforce BGP neighbors to perform multihop.

Use the `no` parameter with this command to turn off this feature.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) enforce-multihop
no neighbor (A.B.C.D|X:X::X:X|WORD) enforce-multihop
```

For BGP unnumbered mode:

```
neighbor WORD enforce-multihop
no neighbor WORD enforce-multihop
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, the maximum hop count is 255

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.34 remote-as 20
(config-router)#neighbor 10.10.0.34 enforce-multihop
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 enforce-multihop
```


© 2021 IP Infusion Inc. Proprietary

neighbor fall-over bfd

Use this command to enable the BFD for BGP peers.

Use the `no` form of the command to disable the BFD option for BGP peers.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) fall-over bfd (multihop|)
no neighbor (A.B.C.D|X:X::X:X|WORD) fall-over bfd (multihop|)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format.
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`multihop`	Enable multihop

Default

Bidirectional Forwarding Detection for BGP peers is disabled by default.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#router bgp 100
(config-router)#neighbor 10.2.3.4 fall-over bfd
(config-router)#
(config-router)#neighbor 10.2.3.4 fall-over bfd multihop
```

neighbor filter-list

Use this command to set up a BGP filter. This command specifies an access list filter on updates based on the BGP autonomous system paths. Each filter is an access list based on regular expressions.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) filter-list WORD (in|out)
no neighbor (A.B.C.D|X:X::X:X|WORD) filter-list WORD (in|out)
```

For v4-unnumbered mode:

```
neighbor WORD filter-list WORD (in|out)
no neighbor WORD filter-list WORD (in|out)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Name of an autonomous system path access list
`in`	Filter incoming advertised routes
`out`	Filter outgoing advertised route

Default

By default, filter list is disabled

Command Mode

Address Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.34 remote-as 20
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.0.34 filter-list out in
```

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 filter-list list2 in
```


© 2021 IP Infusion Inc. Proprietary

neighbor g-shut

Use this command to start a graceful shutdown for the BGP session of the specified BGP neighbor. The BGP session for this neighbor is shut down after the graceful shutdown timer expires.

If there is no alternate path available for traffic to flow prior the actual shutdown of the BGP session, this path is made available for 60 seconds or for configured time after which the path is no longer available and traffic is dropped.

Use the `no` parameter with this command to bring up the session again for the specified BGP neighbor whose BGP session had been shut down using the `neighbor g-shut` command.

Note: The graceful shutdown capability is not supported on iBGP sessions.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) g-shut
no neighbor (A.B.C.D|X:X::X:X|WORD) g-shut
```

Parameters

`A.B.C.D`	Neighbor IPv4 address
`X:X::X:X|`	Neighbor IPv6 address
`WORD`	Neighbor tag

Default

By default, neighbor g-shut is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#neighbor 1.1.1.2 g-shut

#configure terminal
(config)#router bgp 100
(config-router)#no neighbor 1.1.1.2 g-shut
```

neighbor g-shut-timer

Use this command to configure the value of the graceful shutdown timer. After the timer expires, the BGP session initiated for graceful shutdown is shut down.

Use the `no` parameter with this command to revert to the default setting.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) g-shut-timer <10-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) g-shut-timer <10-65535>
```

Parameters

`A.B.C.D`	Neighbor IPv4 address
`X:X::X:X`	Neighbor IPv6 address
`WORD`	Neighbor tag
`<10-65535>`	Graceful shutdown timer in seconds

Default

By default, the timer value is set to 60 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#neighbor 1.1.1.2 g-shut-timer 120
```


© 2021 IP Infusion Inc. Proprietary

neighbor limit

Use this command to specify the maximum number of peers that can be configured in the BGP dynamic peer-group.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
neighbor WORD limit <1-200>
no neighbor WORD (limit <1-200>|)
```

Parameters

`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command.
`<1-200>`	The maximum number of peers that can be configured in a BGP dynamic peer-group.

Default

By default, neighbor word limit is disabled

Command Mode

Router mode and Address Family VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 11
(config-router)#neighbor group1 limit 120
```

neighbor local-as

Use this command to specify an AS (autonomous system) number to use with BGP neighbor.

Use the `no` parameter with this command to disable this command.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) local-as <1-4294967295>
no neighbor (A.B.C.D|X:X::X:X|WORD) local-as <1-4294967295>
```

For BGP unnumbered mode:

```
neighbor WORD local-as <1-4294967295>
no neighbor WORD local-as <1-4294967295>
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-4294967295>`	Neighbor's AS number when extended capabilities are configured

Note: The AS number 23456 is a reserved 2-byte AS number. An old BGP speaker (2-byte implementation) should be configured with 23456 as its remote AS number while peering with a non-mappable new BGP speaker (4-byte implementation).

Default

By default, local as is disabled

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 11
(config-router)#neighbor 10.10.0.34 local-as 12345
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 local-as 300
```


© 2021 IP Infusion Inc. Proprietary

neighbor maximum-prefix

Use this command to set the number of prefixes that can be received from a neighbor.

Use the `no` parameter with this command to disable this function.

Note: For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> <1-100|>
neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> stop-update
neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> warning-only
neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> <1-100> warning-only
no neighbor (A.B.C.D|X:X::X:X) maximum-prefix <1-4294967295>
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-4294967295>`	Maximum number of prefixes accepted from this peer
`stop-update`	Stop installing routes when the maximum number of prefixes is exceeded.
`<1-100>`	Threshold value percent <1-100>
`warning-only`	Only give a warning message when the limit is exceeded. When this parameter is not specified and extra prefixes are received, the router ends the peering. A terminated peer remains down until the `clear ip bgp A.B.C.D` command is given.

Default

By default, neighbor maximum prefix is disabled

Command Mode

Address Family mode ad v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.0.72 maximum-prefix 1244 warning-only

(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 maximum-prefix 3
```

neighbor next-hop-self

Use this command to make the router the next hop for a BGP-speaking neighbor or peer group. This command allows a BGP router to change the nexthop information that is sent to the iBGP peer. The nexthop information is set to the IP address of the interface used to communicate with the neighbor.

Use the `no` parameter with this command to disable this feature.

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) next-hop-self
no neighbor (A.B.C.D|X:X::X:X|WORD) next-hop-self
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, next hop self is disabled

Command Mode

Address Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 remote-as 100
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.0.72 next-hop-self

(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 next-hop-self
```


© 2021 IP Infusion Inc. Proprietary

neighbor optional-as

Use this command to specify an AS (autonomous system) number to use with BGP dynamic peer-group.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
neighbor WORD optional-as <1-4294967295>
no neighbor WORD optional-as <1-4294967295>
```

Parameters

`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-4294967295>`	The range from which the optional AS number must be configured.

Default

By default, neighbor optional as is disabled

Command Mode

Router mode and Address Family VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor group1 optional-as 400
```

neighbor override-capability

Use this command to ignore received capabilities and use locally configured values.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) override-capability
no neighbor (A.B.C.D|X:X::X:X|WORD) override-capability
```

For BGP unnumbered mode:

```
neighbor WORD override-capability
no neighbor WORD override-capability
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, override-capability is disabled

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 override-capability
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 override-capability
```


© 2021 IP Infusion Inc. Proprietary

neighbor passive

Use this command to make a BGP neighbor passive.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) passive
no neighbor (A.B.C.D|X:X::X:X|WORD) passive
```

For BGP unnumbered mode:

```
neighbor WORD passive
no neighbor WORD passive
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor passive is disabled

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 passive
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 passive
```

neighbor peer-group

Use this command to add a neighbor to an existing peer group. Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as distribute and filter lists. The peer group is then configured easily with any of the neighbor commands. Any changes made to the peer group affect all members.

See Usage below for when a peer group and a neighbor have conflicting attribute configurations.

To create a peer group, use the neighbor WORD peer-group command, and then use this command to add neighbors to the group.

Use the no parameter with this command to remove a neighbor from a named peer group.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X) peer-group WORD
no neighbor (A.B.C.D|X:X::X:X) peer-group WORD
```

For BGP unnumbered mode:

```
neighbor WORD peer-group WORD
no neighbor WORD peer-group WORD
```

Parameters

A.B.C.D	Address of the BGP neighbor in IPv4 format
X:X::X:X	Address of the BGP neighbor in IPv6 format
WORD	Peer group name

Default

No default value is specified

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor group1 peer-group
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

Note: For unnumbered peer we use peergroup key word to bind the unnumbered peer in group.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 peergroup ipi
```


© 2021 IP Infusion Inc. Proprietary

Usage

When a *peer group* and a *peer* (neighbor) have conflicting attribute configurations the following rules apply:

- Outbound attribute configurations of a peer group *replace* peer member configurations of the same attributes when a peer becomes member of that peer group. Outbound attribute modifications to group members are not allowed.
- A peer group member's inbound attribute configurations take precedence over the peer group configuration.

These commands control outbound attribute updates:

- neighbor activate
- neighbor advertisement-interval
- neighbor as-origination-interval
- neighbor attribute-unchanged
- neighbor capability orf prefix-list
- neighbor distribute-list with an access-list number and the `out` parameter
- neighbor dont-capability-negotiate
- neighbor filter-list with the `out` parameter
- neighbor next-hop-self
- neighbor prefix-list with an access-list name and the `out` parameter
- neighbor remove-private-AS
- neighbor route-map with the `out` parameter
- neighbor route-reflector-client
- neighbor route-server-client
- neighbor send-community
- neighbor unsuppress-map

These commands control inbound attribute updates:

- neighbor allowas-in
- neighbor collide-established
- neighbor description
- neighbor distribute-list with an access-list number and the `in` parameter
- neighbor ebgp-multihop
- neighbor enforce-multihop
- neighbor filter-list with the `in` parameter
- neighbor g-shut
- neighbor g-shut-timer
- neighbor local-as
- neighbor maximum-prefix
- neighbor override-capability
- neighbor passive
- neighbor authentication-key
- neighbor port

- neighbor prefix-list with an access-list name and the `in` parameter
- neighbor remote-as
- neighbor restart-time
- neighbor route-map with the `in` parameter
- neighbor shutdown
- neighbor soft-reconfiguration inbound
- neighbor strict-capability-match
- neighbor update-source
- neighbor weight

© 2021 IP Infusion Inc. Proprietary

neighbor WORD peer-group range

Use this command to create a dynamic peer group.

Use the no parameter with this command to remove a peer group.

Command Syntax

```
neighbor WORD peer-group range (A.B.C.D/M|X:X::X:X/M)
no neighbor WORD peer-group range (A.B.C.D/M|X:X::X:X/M)
```

Parameters

A.B.C.D/M	IP Prefix
X:X::X:X/M	IPv6 Prefix
WORD	Peer group name

Default

No default value is specified

Command Mode

Router mode and Address Family VRF mode.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor group1 peer-group range 10.10.10.0/24
```

neighbor port

Use this command to set the BGP port number of a neighbor.

Use the `no` parameter with this command to remove a port number from a BGP neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) port <0-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) port
no neighbor (A.B.C.D|X:X::X:X|WORD) port <0-65535>
```

For BGP unnumbered mode:

```
neighbor WORD port <0-65535>
no neighbor WORD port
no neighbor WORD port <0-65535>
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<0-65535>`	Port number

Default

By default, neighbor port is disabled

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 port 643
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 port 500
```


© 2021 IP Infusion Inc. Proprietary

neighbor prefix-list

Use this command to specify a prefix list for filtering BGP advertisements.

Filtering by prefix list matches the prefixes of routes with those listed in the prefix list. If there is a match, the route is used. An empty prefix list permits all prefixes. If a given prefix does not match any entries of a prefix list, the route is denied access. When multiple entries of a prefix list match a prefix, the entry with the smallest sequence number is considered to be a real match.

The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router does not need to go through the rest of the prefix list. For efficiency the most common matches or denies are listed at the top. The neighbor distribute-list command is an alternative to this command and only one of them can be used to filter the same neighbor in any direction.

Use the `no` parameter with this command to remove an entry.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) prefix-list WORD (in|out)
no neighbor (A.B.C.D|X:X::X:X|WORD) prefix-list WORD (in|out)
```

For v4-unnumbered mode:

```
neighbor WORD prefix-list WORD (in|out)
no neighbor WORD prefix-list WORD (in|out)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Name of an access list
`in`	Apply access list to incoming advertisements
`out`	Apply access list to outgoing advertisements

Default

By default, neighbor prefix list is disabled

Command Mode

Address Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip prefix-list list1 deny 30.0.0.0/24
(config)#router bgp 12
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.10.10 prefix-list list1 in
```

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 prefix-list list2 out
```


© 2021 IP Infusion Inc. Proprietary

neighbor remote-as

Use this command to establish a BGP peering relationship with a customer edge router.

The specified neighbor only exchanges unicast address prefixes, unless the neighbor is also activated using the neighbor activate command, which allows the exchange of other routing information.

Use the `no` parameter with this command to delete this peering.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) remote-as (<1-4294967295>|internal|external)
no neighbor (A.B.C.D|X:X::X:X|WORD) remote-as (<1-4294967295>|internal|external)
```

For BGP unnumbered mode:

```
neighbor WORD remote-as (internal|external)
no neighbor WORD remote-as (internal|external)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group. For an unnumbered interface (RFC 5549), specify an interface name configured with neighbor discovery or an IPv4 address with /31 or /30.
`<1-4294967295>`	Neighbor's autonomous system number (ASN) when extended capabilities are configured. If the specified ASN matches the ASN number specified in the router BGP global configuration, the neighbor is identified as internal. If the ASN does no match, the neighbor is identified as external to the local AS.
`internal`	iBGP peer.
`external`	eBGP peer.

Default

By default, neighbor remote is disabled

Command Mode

Router mode and Address Family-vrf mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#router bgp 11
(config-router)#neighbor 10.10.0.73 remote-as 345
(config-router)#neighbor 11.11.0.74 remote-as 23456
```

Note: The last command in the example above should be used when the local speaker is OBGP and the neighbor is NBGP with a 4-octet ASN.

```
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.0.1 remote-as 65000

(config)#router bgp 100
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 remote-as 65000

(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 remote-as internal
(config-router-unnum)#show running bgp

router bgp 100
    !
    bgp unnumbered-mode
    neighbor eth1 remote-as internal
    neighbor eth2 remote-as external
    exit-unnumbered-mode
    !
```

 © 2021 IP Infusion Inc. Proprietary

neighbor remove-private-AS

Use this command to remove the private autonomous system number (ASN) from outbound updates. Private ASNs are not advertised to the Internet. This command is used with external BGP peers only. The router removes the ASNs only if the update includes private ASNs. If the update includes both private and public ASNs, the system treats it as an error.

Use the `no` parameter with this command to revert to default.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) remove-private-AS
no neighbor (A.B.C.D|X:X::X:X|WORD) remove-private-AS
```

For v4-unnumbered mode:

```
neighbor WORD remove-private-AS
no neighbor WORD remove-private-AS
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor remove private AS is disabled

Command Mode

Address Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.0.63 remove-private-AS
```

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 remove-private-AS
```

© 2021 IP Infusion Inc. Proprietary

neighbor restart-time

Use this command to set a different restart-time than the global restart-time configured using the bgp graceful-restart command.

Use the `no` parameter with this command to restore the router to its default state.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) restart-time <1-3600>
no neighbor (A.B.C.D|X:X::X:X|WORD) restart-time <1-3600>
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-3600>`	The maximum time that a graceful-restart neighbor waits to come back up after a restart. Make sure that this value does not exceed the stalepath-time specified in router mode.

Default

By default, restart time is 90 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 3.3.3.3 restart-time 45
```


© 2021 IP Infusion Inc. Proprietary

neighbor route-map

Use this command to apply a route map to incoming or outgoing routes. This command filters updates and modifies attributes. A route map is applied to inbound or outbound updates. Only the routes that pass the route map are sent or accepted in updates.

Use the `no` parameter with this command to a route map.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) route-map WORD (in|out)
no neighbor (A.B.C.D|X:X::X:X|WORD) route-map WORD (in|out)
```

For v4-unnumbered mode:

```
neighbor WORD route-map WORD (in|out)
no neighbor WORD route-map WORD (in|out)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Name of the route map
`in`	Apply access list to incoming advertisements
`out`	Apply access list to outgoing advertisements

Default

No default value is specified

Command Mode

Address Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the configuration of the route map named `rmap2` and then the use of this map name in the `neighbor route-map` command.

```
#configure terminal
(config)#route-map rmap2 permit 6
(config-route-map)#match origin incomplete
(config-route-map)#set metric 100
(config-route-map)#exit
(config)#router bgp 12
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.10.10 route-map rmap2 in
```

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 route-map rmap1 in
```


© 2021 IP Infusion Inc. Proprietary

neighbor route-reflector-client

Use this command to make the router a BGP route reflector and set a specified neighbor as its client.

Using route reflectors reduces the number of iBGP peers within an AS. An AS can have more than one route reflector. A route reflector treats other route reflectors as other iBGP speakers.

Use the `no` parameter with this command to indicate that the neighbor is not a client.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) route-reflector-client
no neighbor (A.B.C.D|X:X::X:X|WORD) route-reflector-client
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

No default value is specified

Command Mode

Address Family mode and L2VPN mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following configuration, Router1 is the route reflector for clients 3.3.3.3 and 2.2.2.2; it also has a non-client peer 6.6.6.6.

```
#configure terminal
(config)#router bgp 200
(config-router)#neighbor 3.3.3.3 remote-as 200
(config-router)#neighbor 2.2.2.2 remote-as 200
(config-router)#neighbor 6.6.6.6 remote-as 200
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 3.3.3.3 route-reflector-client
(config-router-af)#neighbor 2.2.2.2 route-reflector-client
```

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 route-reflector-client
```

For unnumbered peer, configs in L2vpn EVPN mode are configured under l2vpn-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family l2vpn evpn
(config-router-af)#neighbor eth1 route-reflector-client
```

neighbor route-server-client

Use this command to make a neighbor a route server client.

Use the `no` parameter with this command to remove the configuration of a neighbor as route server client.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) route-server-client
no neighbor (A.B.C.D|X:X::X:X|WORD) route-server-client
```

For v4-unnumbered mode:

```
neighbor WORD route-server-client
no neighbor WORD route-server-client
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

No default value is specified

Command Mode

Address Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.0.72 route-server-client

#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
(config-router-af)#no neighbor 10.10.0.72 route-server-client
```

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 route-server-client
```


© 2021 IP Infusion Inc. Proprietary

neighbor send-community

Use this command to send that a community attribute to a BGP neighbor.

The community attribute groups destinations in a certain community and applies routing decisions according to those communities. On receiving community attributes, the router reannounces them to the neighbor.

By default, both `standard` and `extended` community attributes are sent to a neighbor. To explicitly send only the `standard` or `extended` community attribute, run the bgp config-type command with the `standard` parameter before running this command.

Use the `no` parameter with this command to not announce community attributes to the neighbor. Use the `extended` and `no` parameters to remove extended communities. Specifying no other parameter with `no` removes standard communities only.

See also neighbor send-community in Chapter 3, *BGP Virtual Private Network Commands*.

Command Syntax

```
no neighbor (A.B.C.D|X:X::X:X|WORD) send-community
no neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard)
neighbor (A.B.C.D|X:X::X:X|WORD) send-community
neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`both`	Send Standard and Extended Community attributes
`extended`	Send Extended Community attributes
`standard`	Send Standard Community attributes

Default

By default, both communities (standard and extended) are sent to every BGP neighbor.

Command Mode

Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.10.1 remote-as 200
(config-router-af)#no neighbor 10.10.0.1 send-community extended
```

neighbor shutdown

Use this command to terminate active sessions for a specified neighbor and clear all related routing information.

If a peer group is specified, a large number of peering sessions might be terminated. The `show ip bgp summary` command displays a summary of BGP neighbors and their connections.

Use the `no` parameter with this command to re-enable a neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) shutdown
no neighbor (A.B.C.D|X:X::X:X|WORD) shutdown
```

Foe BGP unnumbered mode:

```
neighbor WORD shutdown
no neighbor WORD shutdown
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor shutdown is enabled

Command Mode

Router mode and Address Family-vrf mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 shutdown

(config)#router bgp 100
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 shutdown
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 shutdown
```


© 2021 IP Infusion Inc. Proprietary

neighbor soft-reconfiguration inbound

Use this command to store updates for inbound soft reconfiguration.

Soft-reconfiguration can be used instead of BGP route refresh capability. Using this command enables local storage of all the received routes and their attributes. This requires additional memory. When a soft reset (inbound) is done on this neighbor, the locally stored routes are re-processed according to the inbound policy. The BGP neighbor connection is not affected.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) soft-reconfiguration inbound
no neighbor (A.B.C.D|X:X::X:X|WORD) soft-reconfiguration inbound
```

For v4-unnumbered mode:

```
neighbor WORD soft-reconfiguration inbound
no neighbor WORD soft-reconfiguration inbound
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, the neighbor soft reconfiguration inbound is disabled

Command Mode

Address Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.10.10 soft-reconfiguration inbound
```

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 soft-reconfiguration inbound
```

neighbor strict-capability-match

Use this command to close the BGP connection if a capability value does not match the remote peer.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) strict-capability-match
no neighbor (A.B.C.D|X:X::X:X|WORD) strict-capability-match
```

For BGP unnumbered mode:

```
neighbor WORD strict-capability-match
no neighbor WORD strict-capability-match
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, strict capability match is disabled

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 strict-capability-match
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 strict-capability-match
```


© 2021 IP Infusion Inc. Proprietary

neighbor timers

Use this command to set the timers for a specific BGP neighbor.

Use the `no` parameter with this command to clear the timers for a BGP neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) timers <0-65535> <0-65535>
neighbor (A.B.C.D|X:X::X:X|WORD) timers connect <1-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) timers
no neighbor (A.B.C.D|X:X::X:X|WORD) timers connect
```

For BGP unnumbered mode:

```
neighbor WORD timers <0-65535> <0-65535>
neighbor WORD timers connect <1-65535>
no neighbor WORD timers
no neighbor WORD timers connect
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<0-65535>`	Keepalive interval. Keepalive messages are sent by a router to inform another router that the BGP connection between the two is still active. The keepalive interval is the period of time between each keepalive message sent by the router.
`<0-65535>`	Holdtime interval which is the time the router waits to receive a keepalive message. If the router does not receive a message in this period, the router declares the neighbor dead. The holdtime value should be at least 3 times the keepalive time.
`connect`	BGP connect timer
`<1-65535>`	Connect timer

Defaults

By default, keepalive timer value is 30 seconds

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 timers 60 230
```

```
(config-router)#neighbor 10.10.10.10 timers connect 10

(config-router)#no neighbor 10.10.10.10 timers
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 timers 40 120
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 timers connect 50
```


© 2021 IP Infusion Inc. Proprietary

neighbor unsuppress-map

Use this command to selectively leak more-specific routes to a particular neighbor.

When the aggregate-address command is used with the `summary-only` option, the more-specific routes of the aggregate are suppressed to all neighbors. Use the `neighbor unsuppress-map` command to selectively leak more-specific routes to a particular neighbor.

Use the `no` parameter with this command to restore the setting to the default level.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) unsuppress-map WORD
no neighbor (A.B.C.D|X:X::X:X|WORD) unsuppress-map WORD
```

For v4-unnumbered mode:

```
neighbor WORD unsuppress-map WORD
no neighbor WORD unsuppress-map WORD
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Name of the route map used to select routes to unsuppress

Default

By default, neighbor unsuppress map is disabled

Command Mode

Address Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.0.70 unsuppress-map mymap
```

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 unsuppress-map map2
```

© 2021 IP Infusion Inc. Proprietary

neighbor update-source

Use this command to allow internal BGP sessions to use any operating interface for TCP connections.

A loopback interface is most commonly used with this command. The use of loopback interface eliminates a dependency and BGP does not have to rely on the availability of a particular interface for making TCP connections.

Use the `no` parameter with this command to restore the interface assignment to the closest interface.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) update-source WORD
no neighbor (A.B.C.D|X:X::X:X|WORD) update-source
```

For BGP unnumbered mode:

```
neighbor WORD update-source WORD
no neighbor WORD update-source
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Interface name

Default

By default, neighbor update source is disabled

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 update-source myif
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 update-source myif
```


© 2021 IP Infusion Inc. Proprietary

neighbor version

Use this command to accept only a particular BGP version.

By default, the system uses BGP version 4 and on request dynamically negotiates down to version 2. Using this command disables the router's version-negotiation capability and forces the router to use only a specified version with the neighbor.

Use the `no` parameter with this command to use the default version level of a neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) version 4
no neighbor (A.B.C.D|X:X::X:X|WORD) version
```

For BGP unnumbered mode:

```
neighbor WORD version 4
no neighbor WORD version
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`4`	BGP version number

Default

By default, the system uses BGP version 4 and on request dynamically negotiates down to version 2

Command Mode

Router mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 version 4

(config)#router bgp 12
(config-router)#no neighbor 10.10.10.10 version
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 version 4
```

neighbor weight

Use this command to specify a weight value, per address-family, for all routes learned from a neighbor.

The route with the highest weight gets preference when the same prefix is learned from more than one peer. Unlike the local-preference attribute, the weight attribute is relevant only to the local router. The weights assigned using the `set weight` command override the weights assigned using this command.

Use this command in router mode to specify a weight value for all address families. Use this command in address family mode to specify a weight value per IPv4/IPv6/VPNv4/6PE address family,

When the weight is set for a peer group, all members of the peer group get the same weight. This command can also be used to assign a different weight to an individual peer-group member. When an individually-configured weight of a peer-group member is removed, its weight is reset to its peer group's weight.

Use the `no` parameter with this command to remove a weight assignment.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) weight <0-65535>
no neighbor (A.B.C.D|X:X::X:X|WORD) weight
no neighbor (A.B.C.D|X:X::X:X|WORD) weight <0-65535>
```

For v4-unnumbered mode:

```
neighbor WORD weight <0-65535>
no neighbor WORD weight
no neighbor WORD weight <0-65535>
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<0-65535>`	Weight value

Default

By default, neighbor weight value is 0

Command Mode

Router Address-Family mode and v4-unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.10.10 weight 60
```


© 2021 IP Infusion Inc. Proprietary

```
(config-router-af)#no neighbor 10.10.10.10 weight 60
```

For unnumbered peer, IPv4 unicast mode commands are configured under v4-unnumbered-mode.

```
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#neighbor eth1 weight 44
```

neighbor WORD peer-group

Use this command to create a peer group.

Use the `no` parameter with this command to remove a peer group.

Command Syntax

```
neighbor WORD peer-group
no neighbor WORD peer-group
```

Parameters

`WORD`	Name of BGP peer group

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to create a peer group named `group1`.

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor group1 peer-group
```


© 2021 IP Infusion Inc. Proprietary

network

Use this command to specify the networks to be advertised by the BGP routing process. A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

Use the `backdoor` parameter to specify a backdoor route to a BGP border router that will provide better information about the network. For data to be advertised by BGP, its routing table must include a route to the specified network. This command specifies the networks to be advertised. The network command works if the network being advertised is known to the router.

The `backdoor` parameter enables a route to be the preferred route even if it has a greater distance. A network that is specified as a backdoor network is dynamically assigned an administrative distance of 200 ensuring that IGP learned routes are preferred. If a backdoor network is not sourced by the local router, the network is learned from the external routers. If the route is learned from eBGP for a backdoor network, the distance is set to 20 or 200.

Use the `no` form of this command to remove a network route entry.

Command Syntax

```
network A.B.C.D (backdoor|)
network A.B.C.D/M (backdoor|)
network A.B.C.D mask A.B.C.D (backdoor|)
network A.B.C.D mask A.B.C.D route-map WORD (backdoor|)
network A.B.C.D route-map WORD (backdoor|)
network A.B.C.D/M route-map WORD (backdoor|)
no network A.B.C.D
no network A.B.C.D/M
```

Parameters

`A.B.C.D`	IP prefix <network>, for example, 35.0.0.0
`A.B.C.D/M`	IP prefix <network>/<length>, for example., 35.0.0.0/8
`backdoor`	BGP backdoor route
`routemap`	Route map used to modify the attributes
`WORD`	Name of the route map
`mask`	Network mask, for example, 255.255.0.0
`A.B.C.D`	Network mask, e.g., 255.255.0.0

Default

No default value is specified

Command Mode

Router Address-family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example illustrates a Class-A address configured as a network route. The natural Class-A network prefix mask length of 8 is internally derived, that is, 2.0.0.0/8.

```
(config)#router bgp 1
(config-router)#address-family ipv4 unicast
(config-router-af)#network 2.0.0.0
```


© 2021 IP Infusion Inc. Proprietary

network synchronization

Use this command to enable IGP synchronization for BGP static network routes.

Use this no parameter with this command to disable synchronization of BGP static routes.

Command Syntax

```
network synchronization
no network synchronization
```

Parameters

None

Default

By default, network synchronization is disabled

Command Mode

Address Family mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example enables IGP synchronization of BGP static network routes in the router configuration mode.

```
#configure terminal
(config)#router bgp 11
(config-router)#address-family ipv4 unicast
(config-router-af)#network synchronization
```

The following example enables IGP synchronization of BGP static network routes in the IPv6 unicast address-family mode.

```
#configure terminal
(config)#router bgp 11
(config)#address-family ipv6 unicast
(config-router-af)#network synchronization
```

redistribute

Use this command to inject routes from one routing process into another. Redistribution is used by routing protocols to advertise routes that are learned by some other means, such as by another routing protocol or by static routes. Since all internal routes are dumped into BGP, careful filtering is applied to make sure that only routes to be advertised reach the internet, not everything. This command allows redistribution by injecting prefixes from one routing protocol into another routing protocol.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
redistribute [connected|isis|kernel|ospf|rip|static]
redistribute [connected|isis|kernel|ospf|rip|static] route-map WORD
no redistribute [connected|isis|kernel|ospf|rip|static]
no redistribute [connected|isis|kernel|ospf|rip|static] route-map
no redistribute [connected|isis|kernel|ospf|rip|static] route-map WORD
```

Parameters

`connected`	Redistribute connected routes
`isis`	Redistribute connected ISO IS-IS routes
`kernel`	Redistribute connected kernel routes
`ospf`	Redistribute OSPFv2 routes
`rip`	Redistribute RIP routes
`static`	Redistribute static routes
`route-map`	Route map reference
`WORD`	Route map entries

Default

By default, redistribute is disabled

Command Mode

Address Family mode and Address Family-vrf mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the configuration of the route-map name `rmap1` and then the use of this map name in the `redistribute route-map` command.

```
#configure terminal
(config)#route-map rmap1 permit 1
(config-route-map)#match origin incomplete
(config-route-map)#set metric 100
(config-route-map)#exit
(config)#router bgp 12
```

 © 2021 IP Infusion Inc. Proprietary

```
(config-router)#address-family ipv4 unicast
(config-router-af)#redistribute ospf route-map rmap1

(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#redistribute static

(config)#router bgp 100
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#redistribute static
```

restart bgp graceful

Use this command to enable a BGP-speaker router for graceful restart. This command stops the whole BGP process and makes OcNOS retain the BGP routes and mark them as stale. Receiving BGP speakers, retain and mark as stale all BGP routes received from the restarting speaker for all address families received in the Graceful Restart Capability exchange.

Command Syntax

```
restart bgp graceful
```

Parameters

None

Default

By default, bgp graceful is disabled

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#restart bgp graceful
```


© 2021 IP Infusion Inc. Proprietary

router bgp

Use this command to start a BGP process.

Use the `no` parameter with this command to disable an existing routing process.

Command Syntax

```
router bgp <1-4294967295>
no router bgp <1-4294967295>
```

Parameters

`<1-4294967295>`

Associate the routing process with this autonomous system number

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#
```

snmp restart bgp

Use this command to restart SNMP in Border Gateway Protocol (BGP)

Command Syntax

```
snmp restart bgp
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart bgp
```


© 2021 IP Infusion Inc. Proprietary

synchronization

Use this command to enable IGP synchronization of Internal BGP (iBGP) learned routes with the Internal Gateway Protocol (IGP) system in the router configuration mode or in the address-family configuration mode.

Synchronization is used when a BGP router should not advertise routes learned from iBGP neighbors, unless those routes are also present in an IGP (for example, OSPF). Synchronization may be enabled when all the routers in an autonomous system do not speak BGP, and the autonomous system is a transit for other autonomous systems.

The `no synchronization` command is used when BGP router can advertise routes learned from its iBGP neighbors without waiting for the IGP reachability to be present.

Command Syntax

```
synchronization
no synchronization
```

Parameters

None

Default

No default value is specified

Command Mode

Address Family modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example enables IGP synchronization of iBGP routes in Router mode.

```
#configure terminal
(config)#router bgp 11
(config-router)#address-family ipv4 unicast
(config-router-af)#synchronization
```

The following example enables IGP synchronization of iBGP routes in the IPv6-Unicast address family.

```
#configure terminal
(config)#router bgp 11
(config-router)#address-family ipv6 unicast
(config-router-af)#synchronization
```

timers bgp

Use this command to globally set or reset the keepalive and holdtime values for all the neighbors.

Use the `no` parameter with this command to reset timers to default value.

Command Syntax

```
timers bgp <0-65535> <0-65535>
no timers bgp
```

Parameters

`<0-65535>`	Frequency with which keepalive messages are sent to the neighbors
`<0-65535>`	Interval after which a neighbor is considered dead if keepalive messages are not received

Default

By default, keepalive timer value is 30 seconds

By default, holdtime value is 90 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#timers bgp 40 120
```


© 2021 IP Infusion Inc. Proprietary

v4-unnumbered-mode

Use this command to configure the unnumbered peer with all the neighbor configs applicable in IPv4 unicast address family.

Use the `exit` parameter with this command to leave IPv4 BGP unnumbered mode.

Command Syntax

```
bgp v4-unnumbered-mode
exit-v4-unnumbered-mode
```

Parameters

None

Applicability

No default value is specified

Command Mode

Address-family IPv4 Unicast Mode

Applicability

This command was introduced in OcNOS-OTN version 4.2.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#address-family ipv4 unicast
(config-router-af)#bgp v4-unnumbered-mode
(config-router-v4-unnum)#
```

undebug bgp

Use this command to disable BGP debugging options.

Command Syntax

```
undebug bgp (all|bfd|dampening|events|filters|fsm|keepalives|mpls|nht|nsm|updates)
```

Parameters

`all`	Disable all debugging for BGP
`bfd`	Disable debugging for BGP Bidirectional Forwarding Detection (BFD)
`dampening`	Disable debugging for BGP dampening
`events`	Disable debugging for BGP events
`filters`	Disable debugging for BGP filters
`fsm`	Disable debugging for BGP Finite State Machine (FSM)
`keepalives`	Disable debugging for BGP keepalives
`mpls`	Disable debugging for BGP MPLS
`nht`	Disable debugging for BGP NHT messages
`nsm`	Disable debugging for NSM messages
`updates`	Disable debugging for BGP updates

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#undebug bgp events
```


© 2021 IP Infusion Inc. Proprietary

bgp unnumbered-mode

Use this command to enter the unnumbered mode in router BGP mode allowing configuration of neighbor specific parameters. In this mode we allow creation of unnumbered peer and allow all the neighbor configuration applicable in router BGP mode.

Use no form of this command to exit unnumbered-mode and return to previous mode.

Note: ECMP with BGP unnumbered and numbered together is not supported.

Command Syntax

```
bgp unnumbered-mode
exit-unnumbered-mode
```

Parameters

None

Command Mode

Router BGP mode

Applicability

This command was introduced in OcNOS-OTN version 4.2.

Examples

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 BGP Labeled Unicast Commands

This chapter describes the BGP labeled unicast commands.

- address-family labeled-unicast
- allocate-label
- clear ip bgp A.B.C.D ipv4 labeled-unicast
- clear ip bgp peer-group WORD ipv4 labeled-unicast
- clear ip bgp * ipv4 labeled-unicast

address-family labeled-unicast

Use the address family command to enter the IPv4 or VPNv4 address family mode allowing configuration of address-family specific parameters. To leave address family mode and return to configure mode, give the exit-address-family command.

This command configures the routing exchange between Provider Edge (PE) and Customer Edge (CE) devices. The BGP sessions between PE routers can carry different types of routes (VPN-IPv4 and IPv4 routes). Address families are used to control the type of BGP session.

Use the `no` parameter with this command to disable the address-family configurations.

Command Syntax

```
address-family ipv4 labeled-unicast
address-family ipv6 labeled-unicast
```

Parameters

`ipv4` IPv4 address family

`labeled-unicast`

Enter IPv4 labeled-unicast address-family mode to advertise labeled unicast routes. When a neighbor activate command is given in this mode, the BGP speaker advertises the BGP-LU capability.

`ipv6` IPv6 address family

`labeled-unicast`

Enter IPv6 labeled-unicast address-family mode to:

Activate an IPv4 neighbor to exchange labeled routes data among ISP PE devices. When a IPv4 neighbor activate command is given in this mode, the device becomes 6PE capable.

OR:

Activate an IPv6 neighbor to advertise labeled unicast routes. When a IPv6 neighbor activate command is given in this mode, the BGP speaker advertises the BGP-LU capability.

Default

Not applicable

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS-SP version 1.0.

Example

```
(config)#router bgp 100
(config-router)#address-family ipv4 labeled unicast
(config-router-af)#neighbor 172.4.5.52 activate
(config-router-af)#exit-address-family
```


© 2021 IP Infusion Inc. Proprietary

allocate-label

Use this command to allocate MPLS labels to all/route-map permitted IPv4 prefixes present in the BGP RIB. This command enables the label allocation to IPv4 prefixes, where labeled unicast (LU) routes can be exchanged with IPv4 Peers having BGP labeled-unicast capability. This command allocates labels for all IPv4 unicast prefixes (afi:1, safi:1) and IPv4 labeled-unicast prefixes (afi:1, safi:4).

Once configured, BGP will allocate labels to IPv4 unicast prefixes after the expiry of current BGP RIB scan time (default: 60 seconds).

Use the `no` form of this command to release the labels and disable BGP from allocating label to IPv4 prefixes.

Command Syntax

```
allocate-label (all|route-map WORD)
no allocate-label
```

Parameters

`all`	All the advertised routes
`route-map`	Only those routes that match route-map
`WORD`	Route-map name

Default

Not applicable

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS-SP version 1.0.

Example

To allocate an MPLS label to IPv4 unicast prefix 1.1.1.1/32

```
(config)#router bgp 100
(config-router)#neighbor 11.0.0.2 remote-as 100
(config-router)#allocate-label all
(config-router)#address-family ipv4 unicast
(config-router-af)#network 1.1.1.1/32
(config-router-af)#exit-address-family
(config-router)#address-family ipv4 labeled-unicast
(config-router-af)#network 11.0.0.2 activate
(config-router-af)#exit-address-family
```

clear ip bgp A.B.C.D ipv4 labeled-unicast

Use this command to soft reset an IPv4 Labeled-unicast BGP neighbor.

Command Syntax

```
clear ip bgp A.B.C.D ipv4 labeled-unicast soft
clear ip bgp A.B.C.D ipv4 labeled-unicast soft in
clear ip bgp A.B.C.D ipv4 labeled-unicast soft out
```

Parameters

`A.B.C.D`	BGP neighbor address
`soft`	Soft clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#clear ip bgp A.B.C.D ipv4 labeled-unicast soft in
```


© 2021 IP Infusion Inc. Proprietary

clear ip bgp peer-group WORD ipv4 labeled-unicast

Use this command to soft reset an peer-group of ipv4 labeled-unicast peer members.

Command Syntax

```
clear ip bgp peer-group WORD ipv4 labeled-unicast soft
clear ip bgp peer-group WORD ipv4 labeled-unicast soft in
clear ip bgp peer-group WORD ipv4 labeled-unicast soft out
```

Parameters

`WORD`	Peer-group name
`soft`	Soft clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#clear ip bgp peer-group LU_GROUP ipv4 labeled-unicast soft in
```

clear ip bgp * ipv4 labeled-unicast

Use this command to soft reset all IPv4 Labeled-unicast BGP neighbors.

Command Syntax

```
clear ip bgp * ipv4 labeled-unicast soft
clear ip bgp * ipv4 labeled-unicast soft in
clear ip bgp * ipv4 labeled-unicast soft out
```

Parameters

`soft`	Soft clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#clear ip bgp * ipv4 labeled-unicast soft in
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 BGP Virtual Private Network Commands

This chapter describes the BGP Virtual Private Network (VPN) configuration commands.

- address-family (see address-family in Chapter 1, *BGP Commands*)
- bgp inbound-route-filter
- clear bgp * l2vpn vpls
- clear ip bgp * vpnv4
- clear bgp <1-4294967295> l2vpn vpls
- clear ip bgp <1-4294967295> vpnv4
- clear bgp A.B.C.D l2vpn vpls
- clear ip bgp A.B.C.D vpnv4
- debug bgp mpls
- exit-address-family (see exit-address-family in Chapter 1, *BGP Commands*)
- export map
- import map
- ip vrf
- neighbor activate (see neighbor activate in Chapter 1, *BGP Commands*)
- neighbor allow-ebgp-vpn
- neighbor allowas-in (see neighbor allowas-in in Chapter 1, *BGP Commands*)
- neighbor as-origination-interval (see neighbor as-origination-interval in Chapter 1, *BGP Commands*)
- neighbor as-override
- neighbor description (see neighbor description in Chapter 1, *BGP Commands*)
- neighbor remote-as (see neighbor remote-as in Chapter 1, *BGP Commands*)
- neighbor send-community (see neighbor send-community in Chapter 1, *BGP Commands*)
- neighbor shutdown (see neighbor shutdown in Chapter 1, *BGP Commands*)
- neighbor soo
- redistribute (see redistribute in Chapter 1, *BGP Commands*)
- rd (route distinguisher)
- route-target

© 2021 IP Infusion Inc. Proprietary

bgp inbound-route-filter

Use this command to enable the MPLS (Multiprotocol Label Switching) VPN/BGP inbound route filter. This command is used to control the installation of routing information into the BGP table.

When a router runs MPLS VPN/BGP PE, it exchanges routing information with a routing distinguisher. By default, OcNOS does not install routing information that does not match the configured routing distinguisher value. When the local box has two VRFs where each routing distinguisher value is 10:100 and 20:200, routing information with routing distinguisher 10:200 is not installed into BGP table.

When `no bgp inbound-route-filter` is configured, all of routing information is installed into the BGP table.

Command Syntax

```
bgp inbound-route-filter
no bgp inbound-route-filter
```

Parameter

None

Default

By default, the router performs the routing distinguisher value check is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp inbound-route-filter
```


© 2021 IP Infusion Inc. Proprietary

clear bgp * l2vpn vpls

Use this command to reset the session with all neighbors for VPLS address family

Command Syntax

```
clear bgp * l2vpn vpls
```

Parameters

None

Command Mode

Privileged Exec Modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear bgp * l2vpn vpls
```

clear ip bgp * vpnv4

Use this command to reset a VPNv4 BGP connection for all peers. This command clears the BGP connection and dynamically resets the outbound routing table. This frees up additional memory required for storing updates to generate new updates.

Note: The soft in or in and soft out or out in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear ip bgp * vpnv4 unicast in
clear ip bgp * vpnv4 unicast out
clear ip bgp * vpnv4 unicast soft
clear ip bgp * vpnv4 unicast soft in
clear ip bgp * vpnv4 unicast soft out
```

Parameters

`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp *
#clear ip bgp * vpnv4 unicast out
```


© 2021 IP Infusion Inc. Proprietary

clear bgp <1-4294967295> l2vpn vpls

Use this command to reset the session for the neighbors with a specific ASN number for L2VPN VPLS.

Command Syntax

```
Clear bgp <1-4294967295> l2vpn vpls
```

Parameters

`<1-4294967295>` Autonomous System number of the BGP neighbor.

Command Mode

Privileged Exec Modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear bgp 100 l2vpn vpls
```

clear ip bgp <1-4294967295> vpnv4

Use this command to reset a BGP connection for all VPN peers in a specified Autonomous System.

Note: The soft in or in and soft out or out in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear ip bgp <1-4294967295> vpnv4 unicast in
clear ip bgp <1-4294967295> vpnv4 unicast out
clear ip bgp <1-4294967295> vpnv4 unicast soft
clear ip bgp <1-4294967295> vpnv4 unicast soft in
clear ip bgp <1-4294967295> vpnv4 unicast soft out
```

Parameters

`<1-4294967295>`	Clear peers with this AS number
`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp 500 vpnv4 unicast soft out
```


© 2021 IP Infusion Inc. Proprietary

clear bgp A.B.C.D l2vpn vpls

Use this command to reset the session for neighbor with address A.B.C.D.

Command Syntax

```
clear bgp A.B.C.D l2vpn vpls
```

Parameters

A.B.C.D	BGP neighbor address.

Command Mode

Privileged Exec Modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear bgp 192.168.0.3 l2vpn vpls
```

clear ip bgp A.B.C.D vpnv4

Use this command to reset an VPNv4 BGP connection for a specific IPv4 address.

Note: The soft in or in and soft out or out in the BGP commands performs the same functionality. User can use any of the commands to soft reset.

Command Syntax

```
clear ip bgp A.B.C.D vpnv4 unicast in
clear ip bgp A.B.C.D vpnv4 unicast out
clear ip bgp A.B.C.D vpnv4 unicast soft
clear ip bgp A.B.C.D vpnv4 unicast soft in
clear ip bgp A.B.C.D vpnv4 unicast soft out
```

Parameters

`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip bgp 10.10.0.12 vpnv4 unicast soft
#clear ip bgp 10.10.0.10 vpnv4 unicast out
```


© 2021 IP Infusion Inc. Proprietary

debug bgp mpls

Use this command to enable the display of MPLS related information.

Use the `no` parameter with this command to disable this function.

Note: This command is available only when `vrf` option is enabled.

Command Syntax

```
debug bgp mpls
no debug bgp mpls
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
debug bgp mpls
```

export map

This command assigns a route map to the VRF. This map is applied for routing information exported to another PE or VRF.

Use this command when an application requires finer control over the routes exported to another VRF or PE than provided by the import and export extended communities. You can filter routes that are eligible for export to another VRF or PE through the use of a route map. The route map can deny access to selected routes from a community that is on the export list.

Note: Only match rules (deny/permit) are applied for exported routes, set rules will not apply.

Use the `no` command to remove the map.

Command Syntax

```
export map WORD
no export map
```

Parameters

`WORD`	Route map

Default

No default value is specified

Command Mode

VRF mode

Applicability

This command was introduced in OcNOS-SP version 4.1.

Examples

```
(config)#ip vrf myVRF
(config-vrf)#export map set-pref
(config-vrf)#
```


© 2021 IP Infusion Inc. Proprietary

import map

This command assigns a route map to the VRF. This map is applied for routing information imported from another PE or VRF.

Use this command when an application requires finer control over the routes imported into a VRF than provided by the import and export extended communities. You can filter routes that are eligible for import into a VRF through the use of a route map.The route map can deny access to selected routes from a community that is on the import list.

Use the `no` option with this command to remove the map.

Command Syntax

```
import map WORD
no import map
```

Parameter

`WORD`	Route map

Default

No default value is specified

Command Mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#ip vrf myVRF
(config-vrf)#import map set-pref
(config-vrf)#
```

ip vrf

Use this command to assign a VPN Routing Forwarding (VRF) instance.

Use the `no` option with this command to remove the VRF from the instance.

Command Syntax

```
ip vrf WORD
no ip vrf WORD
```

Parameter

`WORD`	Name of the VRF instance

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Command Example

```
(config)#ip vrf myVRF
(config-vrf)#
```


© 2021 IP Infusion Inc. Proprietary

neighbor allow-ebgp-vpn

Use this command to allow an eBGP neighbor to be a VPN peer. By default, BGP VPN functionality is allowed only for iBGP peers.

Use the `no` parameter with this command to remove the configuration.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) allow-ebgp-vpn
no neighbor (A.B.C.D|X:X::X:X|WORD) allow-ebgp-vpn
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in IPv4 format
`X:X::X:X`	Address of the BGP neighbor in IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, BGP VPN functionality is allowed only for iBGP peers

Command Mode

Address Family-vpnv4 mode and Address Family-vpnv6 mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router bgp 200
(config-router)#neighbor 66.66.66.66 remote-as 100
(config-router)#neighbor 66.66.66.66 update-source lo
(config-router)#address-family vpnv4 unicast
(config-router-af)#neighbor 66.66.66.66 allow-ebgp-vpn
(config-router-af)#neighbor 66.66.66.66 activate
(config-router-af)#exit-address-family
```

neighbor as-override

Use this command to configure a provider edge (PE) router to override the autonomous system number (ASN) of a site with the ASN of a provider. BGP normally ignores routes from the same autonomous system. However, this command is used so that the Customer Edge (CE) routers router accepts and installs routes from the same autonomous system.

Typically, this command is used when CE routers have the same ASN in some or all sites. As per BGP requirement, a BGP speaker rejects a route that has the same ASN as itself in the `AS_PATH` attribute. Thus the CE routers having the same ASN do not accept routes from each other. Giving this command on the PE router removes the CE neighbor's ASN from the `AS_PATH` attribute allowing CE routers with the same ASN to accept routes from each other.

Use the `no` parameter with this command to remove VPN IPv4 prefixes from a specified router.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) as-override
no neighbor (A.B.C.D|X:X::X:X|WORD) as-override
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in IPv4 format
`X:X::X:X`	Address of the BGP neighbor in IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor as override is disabled

Command Mode

Address Family-vrf mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.0.1 as-override

#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 as-override
```


© 2021 IP Infusion Inc. Proprietary

neighbor send-community

Use this command to send the extended-community attribute to a customer edge router. In VPN, the route-distinguisher and route-target are encoded in BGP extended-community.

See also neighbor send-community in Chapter 1, *BGP Commands*.

Command Syntax

```
no neighbor (A.B.C.D|X:X::X:X|WORD) send-community
no neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard)
neighbor (A.B.C.D|X:X::X:X|WORD) send-community
neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`both`	Send standard and extended community attributes
`extended`	Send extended community attributes
`standard`	Send standard community attributes

Default

By default, both communities (standard and extended) are sent to every BGP neighbor.

Command Mode

Address Family Unicast mode and Address Family VRF mode.

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.10.1 remote-as 200
(config-router-af)#no neighbor 10.10.0.1 send-community extended
```

© 2021 IP Infusion Inc. Proprietary

neighbor soo

Use this command to enable the site-of-origin (SOO) feature. If the customer AS is multi-homed to the ISP, this command ensures that the PE does not advertise the routes back to the same AS.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) soo AS:nn_or_IP:nn
no neighbor (A.B.C.D|X:X::X:X|WORD) soo
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in IPv4 format
`X:X::X:X`	Address of the BGP neighbor in IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`ASN:nn_or_IP-address:nn`	An AS number and an arbitrary number (for example, 100:1), or a 32-bit IP address and an arbitrary number (for example, 192.16.10.1:1).

Default

By default, the site-of-origin (SOO) feature is disabled.

Command Mode

Address Family VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 1.1.1.1 remote-as 200
(config-router-af)#neighbor 10.10.0.1 soo 100:1
```


© 2021 IP Infusion Inc. Proprietary

rd (route distinguisher)

Use this command to assign a route distinguisher (RD) for the VRF. The route distinguisher value must be a unique value on the router.

This command creates routing and forwarding tables and specifies the default RD for a VPN. The RD is added to the customer's IPv4 prefixes, changing them into globally unique VPN-IPv4 prefixes.

Use `no` form command to remove the RD configuration.

Note: RD configuration cannot be changed, it needs to be removed and added back with new value. When RD configuration is removed the RT configuration is also lost and needs to be reconfigured.

Command Syntax

```
rd ASN:nn_or_IP-address:nn
```

```
no rd ASN:nn_or_IP-address:nn
```

Parameters

`ASN:nn_or_IP-address:nn`

AS number and an arbitrary number (for example, 100:1). Otherwise, specify a 32-bit IP address and an arbitrary number (for example, 192.16.10.1:1).

Default

No default value is specified

Command Mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#ip vrf VRF_A
(config-vrf)#rd 100:1
```

route-target

Use this command to add a list of import and export route-target extended communities to the VRF.

This command creates lists of import and export route-target extended communities for the VRF. It specifies a target VPN extended community. Execute the command once for each community. All routes with the specific route-target extended community are imported into all VRFs with the same extended community as an import route-target.

Use the `no` parameter with this command to delete a route target.

Command Syntax

```
route-target (import|export|both) ASN:nn_or_IP-address:nn
no route-target (import|export|both) ASN:nn_or_IP-address:nn
```

Parameters

`import`	Import routing information
`export`	Export routing information
`both`	Import and export routing information
`ASN:nn_or_IP-address:nn`	AS number and an arbitrary number (for example, 100:1). Otherwise, specify a 32-bit IP address and an arbitrary number (for example, 192.16.10.1:1).

Default

No default value is specified

Command Mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#ip vrf VRF_A
(config-vrf)#route-target both 100:10

(config)#ip vrf VRF_A
(config-vrf)#route-target import 100:20
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 BGP Show Commands

This chapter describes the BGP show commands.

- show bgp
- show bgp A.B.C.D
- show bgp A.B.C.D/M
- show bgp client
- show bgp community
- show bgp community-list
- show bgp dampening dampened-paths
- show bgp dampening flap-statistics
- show bgp dampening parameters
- show bgp filter-list
- show bgp inconsistent-as
- show bgp ipv6
- show bgp l2vpn vpls
- show bgp neighbors
- show bgp neighbors advertised-routes
- show bgp neighbors received prefix-filter
- show bgp neighbors received-routes
- show bgp neighbors routes
- show bgp nexthop-tracking
- show bgp nexthop-tree-details
- show bgp paths
- show bgp prefix-list
- show bgp quote-regexp
- show bgp regexp
- show bgp route-map
- show bgp statistics
- show bgp summary
- show bgp X:X::X:X
- show bgp X:X::X:X/M longer prefixes
- show debugging bgp
- show ip bgp
- show ip bgp cidr-only
- show ip bgp community-info
- show ip bgp peer-group
- show ip bgp peer-group vrf all

© 2021 IP Infusion Inc. Proprietary

- show ip bgp rtfilter all
- show ip bgp scan
- show ip bgp vpnv4
- show ip extcommunity-list
- show ip extcommunity-list
- show ip protocols
- show ip vrf
- show running-config as-path access-list
- show running-config community-list

© 2021 IP Infusion Inc. Proprietary

show bgp

Use this command to display the status of BGP routes.

Command Syntax

```
show bgp
show bgp (ipv6)
show bgp (ipv4|ipv6) (unicast|multicast)
show ip bgp
show ip bgp ipv4 (unicast|multicast)
show bgp (vrf (VRFNAME|all|default))
show ip bgp (vrf (VRFNAME|all|default))
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip bgp
BGP table version is 1, local router ID is 12.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop      Metric    LocPrf   Weight   Path
*> 1.1.1.1/32   0.0.0.0          0         100      32768      i

Total number of prefixes 1
```

show bgp A.B.C.D

Use this command to display BGP route information for a network.

Command Syntax

```
show bgp (ipv4) (unicast|multicast) A.B.C.D
show ip bgp A.B.C.D
show ip bgp ipv4 (unicast|multicast) A.B.C.D
```

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`A.B.C.D`	IP prefix (network), for example, 35.0.0.0

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
OcNOS#show ip bgp 80.80.80.0
BGP routing table entry for 80.80.80.0/24
Paths: (1 available, no best path)
 Not advertised to any peer
 300
   15.15.15.1 (inaccessible) from 11.11.11.2 (15.15.15.2)
     Origin incomplete, metric 0, localpref 100, valid, internal
     rx path_id: 0       tx path_id: -1
     Last update: Wed May 11 15:22:36 2016
```

Table 4-148 explains the output fields.

Table 4-148: show ip bgp output details

Field	Description
Paths	The paths listed in the routing table, along with path information, and whether the path are being advertised.
Metric	If shown, the value of the inter-autonomous system metric.
LocalPref	Local preference value as set with the set local-preference route-map configuration command.
rx path_id	Autonomous system receive path to the source network. There can be one entry in this field for each autonomous system in the path.

© 2021 IP Infusion Inc. Proprietary

Table 4-148: show ip bgp output details

Field	Description
tx path_id	Autonomous system transmit path to the destination network. There can be one entry in this field for each autonomous system in the path.
Last update	Last time since the neighbor transitioned to or from the established state.

show bgp A.B.C.D/M

Use this command to display BGP route information for a network prefix.

Command Syntax

```
show bgp ipv4 (unicast|multicast) A.B.C.D/M
show ip bgp A.B.C.D/M
show ip bgp ipv4 (unicast|multicast) A.B.C.D/M
show ip bgp A.B.C.D/M (vrf (VRFNAME|all|default))
show ip bgp A.B.C.D/M longer-prefixes
show ip bgp ipv4 (unicast|multicast) A.B.C.D/M longer-prefixes
show ip bgp A.B.C.D/M longer-prefixes (vrf (VRFNAME|all|default))
```

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`A.B.C.D/M`	IP prefix (network/length), for example, 35.0.0.0/8
`longer-prefixes`	Display route and more specific routes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp ipv4 unicast 22.22.22.22/32
BGP routing table entry for 22.22.22.22/32
Paths: (2 available, best #1, table Default-IP-Routing)
  Not advertised to any peer
  Local
    11.11.11.2 from 11.11.11.2 (2.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Last update: Fri Feb 16 09:46:54 2001

  Local
    11.11.12.2 from 11.11.12.2 (2.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal
      Last update: Fri Feb 16 09:46:52 2001
```


© 2021 IP Infusion Inc. Proprietary

show bgp client

Use this command to display BGP client information.

Command Syntax

```
show bgp client
```

Parameters

None

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp client
R1#sh bgp client
BGP client ID: 11
 PIM, socket 10
  Service: AS number service, Route Service
  Messsage received 1, sent 1
  Connection time: Tue May 14 03:11:01 2019
  Last message read: Service Request
  Last message write: Service Reply
R1#
```

show bgp community

Use this command to display BGP routes that match a community.

Command Syntax

```
show bgp ip (unicast|multicast) community
show bgp ip (unicast|multicast) community (vrf (VRFNAME|all|default))
show bgp ip (unicast|multicast) community [AA:NN|local-AS|no-advertise|no-export]
  (exact-match|)
show ip bgp community
show ip bgp community [AA:NN|local-AS|no-advertise|no-export|internet] (exact-
  match|)
show ip bgp community (vrf (VRFNAME|all|default))
show ip bgp community [AA:NN|local-AS|no-advertise|no-export|internet] (exact-
  match|)
show ip bgp community-list WORD (exact-match|) (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) community
show ip bgp ipv4 (unicast|multicast) community (vrf (VRFNAME|all|default))
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF
`AA:NN`	Community number
`local-AS`	Do not send outside local AS (well-known community)
`no-advertise`	Do not advertise to any peer (well-known community)
`no-export`	Do not export to next AS (well-known community)
`internet`	Internet community (well-known community)
`exact-match`	Exact match of the communities

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

© 2021 IP Infusion Inc. Proprietary

Example

```
#show bgp community
BGP table version is 1, local router ID is 102.67.98.95
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network                Next H     Metric    LocPrf     Weight    Path
*> 2001:43f8:bb1::/64   ::          0        100       32768      ?

Total number of prefixes 1
```

show bgp community-list

Use this command to display BGP routes that match a community list.

Command Syntax

```
show bgp community-list WORD (exact-match|)
show bgp ip (unicast|multicast) community-list WORD (exact-match|)
show bgp ip (unicast|multicast) community-list WORD (exact-match|)
show bgp (ipv4|ipv6) (unicast|multicast) community-list WORD (exact-match|)
show bgp (ipv6) community-list WORD (exact-match|)
show ip bgp community-list WORD (exact-match|)
show ip bgp ipv4 (unicast|multicast) community-list WORD (exact-match|)
```

Parameters

`WORD`	Community list name
`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`exact-match`	Only routes that exactly match the community

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp community-list Originate
Named Community expanded list Originate
    permit 37721:1[0-2]0[05]$
    permit 37721:1[0-2]0[05]
```


© 2021 IP Infusion Inc. Proprietary

show bgp dampening dampened-paths

Use this command to display detailed information about paths suppressed due to dampening.

Command Syntax

```
show bgp dampening dampened-paths
show bgp (ipv4|ipv6) (unicast|multicast) dampening dampened-paths
show bgp (ipv6) dampening dampened-paths
show ip bgp dampening dampened-paths
show ip bgp dampening dampened-paths (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) dampening dampened-paths
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp dampening dampened-paths
```

show bgp dampening flap-statistics

Use this command to display BGP dampening flap statistics.

Command Syntax

```
show bgp dampening flap-statistics
show bgp (ipv4|ipv6) (unicast|multicast) dampening flap-statistics
show bgp (ipv6) dampening flap-statistics
show ip bgp dampening flap-statistics
show ip bgp dampening flap-statistics (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) dampening flap-statistics
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This sample output shows that the internal route (`i`), has flapped 3 times and is now categorized as history (`h`).

```
#show ip bgp dampening flap-statistics
BGP table version is 1, local router ID is 30.30.30.77
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From            Flaps  Duration  Reuse    Path
hi1.1.1.0/24     10.100.0.62       3  00:01:20       i
```

Header

```
BGP table version is 1, local router ID is 30.30.30.77
```

- BGP table version
- BGP router ID is `30.30.30.77`

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S stale
```


© 2021 IP Infusion Inc. Proprietary

Table 4-148 shows the status codes displayed at the start of a route entry.

Table 4-149: status details

Status Code	Description	Comments
s	suppressed	Whether the route is suppressed and is not advertised to neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
p	stale	When the BGP neighbor from which a route is learned is in graceful restart, the route is retained in the BGP routing table, but marked as stale .
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The selected route to be installed in the kernel routing table.
i	internal	The prefix was learned from an iBGP peer.

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Table 4-150 shows the codes at the end of each route entry that indicate where the route originated.

Table 4-150: origin details

Origin Code	Description	Comments
i	IGP	The route is from an Interior Gateway Protocol.
e	EGP	The route is from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an IGP.

Table 4-151 explains the output fields.

Table 4-151: show bgp dampening flap-statistics output details

Field	Description
Network	Internet address of a network.
From	IP address of the advertising peer.
Flaps	Number of times this route has failed and returned (flapped).

Table 4-151: show bgp dampening flap-statistics output details

Field	Description
Duration	Elapsed time since the first penalty points were assessed.
Reuse	The amount of time remaining until this route will be un-suppressed and can be used again.

© 2021 IP Infusion Inc. Proprietary

show bgp dampening parameters

Use this command to display the BGP dampening parameters.

Command Syntax

```
show bgp dampening parameters
show bgp (ipv4|ipv6) (unicast|multicast) dampening parameters
show bgp (ipv6) dampening parameters
show ip bgp dampening parameters
show ip bgp ipv4 (unicast|multicast) dampening parameters (vrf
  (VRFNAME|all|default))
show ip bgp dampening parameters (vrf (VRFNAME|all|default))
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip bgp dampening parameters
 dampening 5 750 2000 60 15
 Dampening Control Block(s):
  Reachability Half-Life time    : 5 min
  Reuse penalty                  : 750
  Suppress penalty               : 2000
  Max suppress time              : 60 min
  Un-reachability Half-Life time : 15 min
  Max penalty (ceil)             : 11999
  Min penalty (floor)            : 375
#
```

Table 4-152 explains the output fields.

Table 4-152: show ip bgp dampening parameters output details

Field	Description
Dampening Control Block(s)	Flap damping reduces the number of update messages by marking routes as ineligible for selection as the active or preferable route.
Reachability Half-Life time	Number of minutes after which an arbitrary value is halved if a route stays stable.
Reuse penalty	Reuse threshold—Arbitrary value below which a suppressed route can be used again.
Suppress penalty	Cutoff (suppression) threshold—Arbitrary value above which a route can no longer be used or included in advertisements.
Max suppress time	Maximum hold-down time for a route, in minutes.
Un-reachability Half-Life time	Number of minutes after which an arbitrary value is not halved if a route stays stable.
Max penalty (ceil)	Maximum penalty corresponds to the time it would take max-suppress to decay and reach the reuse level (ceil).
Min penalty (floor)	Maximum penalty corresponds to the time it would take max-suppress to decay and reach the reuse level (floor).

© 2021 IP Infusion Inc. Proprietary

show bgp filter-list

Use this command to display routes that match a regular expression filter list.

Command Syntax

```
show bgp filter-list WORD
show bgp (ipv4|ipv6) (unicast|multicast) filter-list WORD
show bgp (ipv6) filter-list WORD
show ip bgp filter-list WORD
show ip bgp ipv4 (unicast|multicast) filter-list WORD
show ip bgp filter-list WORD (exact-match)
show ip bgp filter-list WORD (exact-match) (vrf (VRFNAME|all|default))
show ip bgp filter-list WORD (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) filter-list WORD (exact-match)(vrf
  (VRFNAME|all|default))
```

Parameters

`WORD`	Regular-expression filter list
`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`exact-match`	Exact match of the filter list
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF
`vrf`	VPN Routing/Forwarding instance name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp filter-list bgp-local-only
BGP table version is 1, local router ID is 102.67.98.95
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network                Next Hop        Metric    LocPrf      Weight   Path
*> 2001:43f8:bb1::/6     ::              0        100         32768     ?
```

```
    Total number of prefixes 1
```

 © 2021 IP Infusion Inc. Proprietary

show bgp inconsistent-as

Use this command to display routes with inconsistent AS paths.

Command Syntax

```
show bgp inconsistent-as
show bgp (ipv4|ipv6) (unicast|multicast) inconsistent-as
show bgp (ipv6) inconsistent-as
show ip bgp inconsistent-as
show ip bgp ipv4 inconsistent-as
show ip bgp ipv4 (unicast|multicast) inconsistent-as
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp inconsistent-as

BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network        Next Hop              Metric         LocPrf   Weight   Path
*> 10.1.0.0   172.29.232.55            0             0         100      ?
```

show bgp ipv6

Use this command to display the BGP routing table.

Command Syntax

```
show bgp ipv6 (unicast|multicast|labeled|)
show bgp ipv6 (unicast|multicast|labeled|) X:X::X:X/M
```

Parameters

`multicast`	IPv6 multicast address prefixes
`unicast`	IPv6 unicast address prefixes
`labeled`	Labeled IPv6 routes
`X:X::X:X/M`	IPv6 prefix network/length, such as 3ffe:a::/64

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example: iBGP and eBGP Routes

This example shows routes learned from both iBGP and eBGP.

```
#show bgp ipv6
BGP table version is 0, local router ID is 10.100.0.77
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal S stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network                                Metric LocPrf Weight  Path
*> 2001:58::/32                                              0  20 ?
     fe80::202:b3ff:fec8:9fdb
*> 2002:58::/32                                              0  20 i
     fe80::202:b3ff:fec8:9fdb
*>i2003:58::/32                                   100        0  i
     fe80::208:a1ff:fe16:797d
```

Header

```
BGP table version is 0, local router ID is 10.100.0.77
```

- BGP table version
- BGP router ID is `10.100.0.77`

```
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i - internal
```


© 2021 IP Infusion Inc. Proprietary

Table 4-153 shows the status codes displayed at the start of a route entry.

Table 4-153: status details

Status Code	Description	Comments
s	suppressed	Whether the route is suppressed and is not advertised to neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
p	stale	When the BGP neighbor from which a route is learned is in graceful restart, the route is retained in the BGP routing table, but marked as stale .
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The selected route to be installed in the kernel routing table.
i	internal	The prefix was learned from an iBGP peer.

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Table 4-154 shows the codes at the end of each route entry that indicate where the route originated.

Table 4-154: origin codes

Origin Code	Description	Comments
i	IGP	The route is from an Interior Gateway Protocol.
e	EGP	The route is from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an IGP.

Route Entry Examples

```
*> 2002:58::/32     fe80::202:b3ff:fec8:9fdb                              0 20 i
```

- This route entry shows that this route is learned from eBGP.
- The origin code “i” means that the prefix is added by the network statement at originating AS.
- The path 20 indicates that the prefix advertisement originated from AS20.
- The administrative weight parameter applies only to routes within an individual router.
- Since this route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.

```
*> 2001:58::/32      fe80::202:b3ff:fec8:9fdb                              0 20 ?
```

- This route entry shows that the prefix is learnt from eBGP.The origin code i indicates that the prefix is added by network statement at originating AS.The path attribute 20 indicates that the route advertisement originated from AS20.The administrative weight parameter applies only to routes within an individual router. Since this

route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.The origin code “?” means the route was learned through redistribution.

```
*>i2003:58::/32     fe80::208:a1ff:fe16:797d                    100     0 i
```

- The status code “i” means that the route was learned through iBGP. The Local Preference attribute of the route, which is used only with the local AS, is set to 100 (the default value).

Example: IPv6 Prefix Routes

This example shows labeled routes for a given IPv6 prefix:

```
#show bgp ipv6 labeled 3ffe:a::/64
           BGP routing table entry for 3ffe:a::/64
           Paths: (1 available, best #1, table Default-IP-Routing-Table)
           Not advertised to any peer
           Local
           ::ffff:114:1414 from 20.20.20.1 (92.92.92.92)
          Origin incomplete metric 0, localpref 100, label    5420,
           valid, internal, best
           Last update: Mon May 26 17:48:18 2008
```

Table 4-155 explains the output fields.

Table 4-155: show bgp ipv6 output details

Field	Description
Paths	The paths listed in the routing table, along with path information, and whether the path are being advertised.
Metric	If shown, the value of the inter-autonomous system metric.
Local Pref	Local preference value as set with the set local-preference route-map configuration command.
rx path_id	Autonomous system receive path to the source network. There can be one entry in this field for each autonomous system in the path.
tx path_id	Autonomous system transmit path to the destination network. There can be one entry in this field for each autonomous system in the path.
Last update	Last time since the neighbor transitioned to or from the established state.

© 2021 IP Infusion Inc. Proprietary

show bgp ipv6 peer-group

Use this command to list the BGP peer group information in ipv6 unicast.

Command Syntax

```
show bgp ipv6 peer-group (WORD|)
```

Parameters

WORD	Name of the peer group

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.2.

Example

```
#show bgp ipv6 peer-group p2
BGP dynamic peer-group is p2, IBGP, remote AS 42949672
  BGP dynamic peer-group p2 listen range group members:
  5ffe:3::/64
  BGP version 4
Minimum time between advertisement runs is 5 seconds
For address family: IPv6 Unicast
  Peer-group member:
  *5ffe:3::1
  Index 2, Offset 0, Mask 0x4
  0 accepted prefixes, 0 announced prefixes
#
```

show bgp l2vpn vpls

Command Syntax

```
show bgp l2vpn vpls (rr|) (detail|)
```

Parameters

`rr`	Display the information of auto-discovered peers at Route reflector node.
`detail`	Display the detailed information of auto-discovered peers.

Command Mode

Exec and Privileged Exec Modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp l2vpn vpls
VPLS-ID   VE-ID    Discovered-Peers   Route-Target
10        3        1                   10:100


#show bgp l2vpn vpls  detail

VPLS ID: 10
VE-ID: 3
Discovered Peers: 1
Route-Target: 10:100
Local RD: 10:100
 Mesh Peers:
  Address:3.3.3.3, RD:10:100, VE-ID:4
  VC Details: VC-ID:34
  Remote (LB:52480,VBO:1,VBS:64)  Local (LB:52480,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:52483, Out Label:52482
  PW Status:Established
```

Table 4-156 explains the output fields.

Table 4-156: show bgp l2vpn vpls output details

Field	Description
VPLS-ID	L2VPN address family database information for the Virtual Private LAN Service (VPLS).
VE-ID	L2VPN address family database information for the Virtual Expansion.
Discovered Peers	Peer discovery is used to find peers that are available for data using LLDP.
Route-Target	An identifier prepended to IP addresses to assure the uniqueness of the address.

© 2021 IP Infusion Inc. Proprietary

Table 4-156: show bgp l2vpn vpls output details

Field	Description
Local RD	The Local Route Descriptor – the first two numbers of the Route-Target.
Mesh Peers	Internal BGP peers – devices that do not re-advertise routes to other IBGP devices.
Address	Mesh session information for the peer specified with the ip-address argument.
RD	Mesh peer's Route-Descriptor.
VC Details	The virtual circuit session information with the ip-address for the Provider Edge (PE) routers.
Remote	• LB (Label Base) – the first label value of a free set of labels that can be reserved by the PE router to be used for this VPLS domain. • VBO (VE Block Offset) – the offset value to be used when multiple label blocks must be created by a PE router. • VBS (VE Block Size) – the size of the label block.
Local	• LB (Label Base) – the first label value of a free set of labels that can be reserved by the PE router to be used for this VPLS domain. • VBO (VE Block Offset) – the offset value to be used when multiple label blocks must be created by a PE router. • VBS (VE Block Size) – the size of the label block.
LB sent on known VEID	Whether the Label Base came on a known Virtual Expansion Identifier – yes or no.
In Label	The ingress (incoming interface) label for this segment.
Out Label	Label received from downstream neighbor for route.
PW Status	The status of the VPLS Pseudo-Wire. Values can be: Idle, Active, Open, or Established.

```
#show bgp l2vpn vpls rr
RD        RR-Clients     Non-Clients           Route-Target
10:100     2                  0                  10:100
10:100     2                  0                  10:100


#show bgp l2vpn vpls rr detail

Route-Target: 10:100
  Peer:1.1.1.1
    RR Client  : Yes
    VE-ID:3  LB:52480  VBO:1  VBS:64

Route-Target: 10:100
  Peer:3.3.3.3
    RR Client  : Yes
    VE-ID:4  LB:52480  VBO:1  VBS:64
```

Table 4-157 explains the output fields.

Table 4-157: show bgp l2vpn vpls rr output details

Field	Description
Route-Target	An identifier prepended to IP addresses to assure the uniqueness of the address.
Peer	Internal BGP peers – devices that do not re-advertise routes to other IBGP devices.
RR Client	Device is a client of the Route Reflector – yes or no.
VE-ID	L2VPN address family database information for the Virtual Expansion.
LB	LB (Label Base) – the first label value of a free set of labels that can be reserved by the PE router to be used for this VPLS domain.
VBO	VBO (VE Block Offset) – the offset value to be used when multiple label blocks must be created by a PE router.
VBS	VBS (VE Block Size) – the size of the label block.

© 2021 IP Infusion Inc. Proprietary

show bgp neighbors

Use this command to display information about BGP neighbor connections.

Command Syntax

```
show bgp neighbors
show bgp neighbors (A.B.C.D|X:X::X:X|WORD)
show bgp ipv6 neighbors
show ip bgp ipv4 (unicast|multicast) neighbors
show ip bgp neighbors
show ip bgp neighbors (A.B.C.D|X:X::X:X)(advertised-routes|)
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X|WORD)
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) (hold-time|keepalive-
  interval|connection-retrytime)
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) (sent-msgs|rcvd-
  msgs|notification|update|open|keepalive)
```

Parameters

`ipv4`	IPv4 neighbors
`ipv6`	IPv6 neighbors
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`A.B.C.D`	IPv4 neighbor
`X:X::X:X`	IPv6 neighbor
`WORD`	Interface name
`advertised-routes`	Routes advertised to a BGP neighbor
`hold-time`	Hold time
`keepalive-interval`	Keepalive interval
`connection-retrytime`	Connection retry time
`sent-msgs`	Sent packets
`rcvd-msgs`	Received packets
`notification`	Notification messages
`update`	Update messages
`open`	Open messages
`keepalive`	Keepalive messages

Command Mode

Privileged Exec and Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group myPeer for session parameters
  BGP version 4, remote router ID 10.12.7.155
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  myPeer peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 2.2.2.1, Local port: 33865
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: 1111::1
Nexthop local: fe80::a00:27ff:fecc:47a6
BGP connection: non shared network
Last Reset: 00:32:48, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

BGP Neighbor Fields

Table 4-158 explains the output fields.

Table 4-158: show bgp neighbor output details

Field	Description
BGP neighbor	BGP session information for the neighbor with the ip-address argument.
remote AS	Remote Autonomous system used to exchange exterior routing information between neighboring ASs.

© 2021 IP Infusion Inc. Proprietary

Table 4-158: show bgp neighbor output details

Field	Description
local AS	Local Autonomous system used to exchange internal routing information within AS.
internal link external link	Internal link is used to forward route advertisements received from an external BGP router through the internal network (in the same AS). External link is used for exchanging routing information between Autonomous Systems (AS) and routing traffic across the Internet (eBGP neighbor).
member of peer-group	Peer group information for the peer group specified with the peer-group argument.
BGP version	Negotiated BGP version for this session.
remote router ID	IP address of the neighbor. BGP uses the highest loopback address as the Router ID. If no loopback interface is configured, BGP uses the highest configured IP address on a system.
BGP state	Session state as explained in Table 4-163. The exchange of routing information begins between peers only after the neighbor session is in an Established state.
up for	Time that the underlying TCP connection has been up.
last read	Time since BGP last received a message from this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages. The maximum time that can elapse between successive messages from this neighbor is 180 seconds. If no message is received for 180 seconds, this neighbor will be declared dead.
last write	Time since BGP last sent a message to this neighbor.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor. The time interval between successive keepalive messages is 60 seconds. Typically, the hold time value is set to three times the keepalive interval.
neighbor capabilities	BGP capabilities advertised and received from this neighbor. “Advertised and received” is displayed when a capability is successfully exchanged between two routers.
received	Total number of received messages. notifications: Number of notification (error) messages received. in queue: Number of messages in the input queue
sent	Total number of sent messages. notifications: Number of notification (error) messages sent. in queue: Number of messages in the output queue
route refresh request	Number of route refresh request messages sent and received.
minimum time between advertisement runs.	The minimum time gap, in seconds, between successive route updates sent to the neighbor. Generally, a jitter (of 25%) is applied to this time interval, which means that if the time between advertisements is configured as 30, successive advertisements can have a time gap of as low as 22.5 (after applying a 25% jitter to the 30 seconds, which is 7.5 seconds).
for address family	The peers have exchanged address family capability.
BGP table version	For each of the address families agreed upon, BGP maintains a separate table.
neighbor version	Tracks prefixes that have been sent and those that need to be sent.

Table 4-158: show bgp neighbor output details

Field	Description
connections established	The number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other. “Dropped” means the number of time the connection has failed or gone down.
local host foreign host	Local host is the IP address and the port number of the local system used for the peering session. Foreign host is the IP address and the port of the neighbor. BGP always uses the TCP port number 179 for the peer originating the session.
nexthop	The IP address of the next hop used to reach the neighbor. eBGP or iBGP peers do not need to be directly connected. Peering sessions can be set up across multiple hops. If the neighbors are directly connected, the IP address of the local system is listed as the next hop.
nexthop global	The global IPv6 address of the next hop
nexthop local	The link-local IPv6 address of the next hop
non shared network	The peering session is running on a non shared network.
last reset	Time since this peering session was last reset. The reason for the reset is displayed on this line.
notification error message	Last error message sent.

© 2021 IP Infusion Inc. Proprietary

show bgp neighbors advertised-routes

Use this command to display the routes advertised to a BGP neighbor.

Command Syntax

```
show bgp neighbors (A.B.C.D|X:X::X:X|WORD) advertised-routes
show ip bgp neighbors (A.B.C.D|X:X::X:X) advertised-routes (vrf
  (VRFNAME|all|default))
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) advertised-routes
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) routes advertised
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X|WORD) advertised-
  routes
```

Parameters

`A.B.C.D`	IPv4 neighbor
`X:X::X:X`	IPv6 neighbor
`WORD`	Interface name
`ipv4`	IPv4 addresses
`multicast`	Multicast prefixes
`unicast`	Unicast prefixes
`vrf`	VPN Routing/Forwarding instance name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp neighbors 11.11.11.2 advertised-routes
BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network              Next Hop            Metric    LocPrf       Weight   Path
*>i 33.33.33.33/32   11.11.11.1           0         100         32768     i

Total number of prefixes 1
```

show bgp neighbors received prefix-filter

Use this command to display the prefix list filter.

Command Syntax

```
show bgp neighbors (A.B.C.D|X:X::X:X|WORD) advertised-routes
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) received prefix-filter
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X) received prefix-
  filter
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`WORD`	Interface name
`ipv4`	IPv4 addresses
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp neighbors 100.1.1.1 received prefix-filter
Address family: IPv4 Unicast
ip prefix-list 100.1.1.1.1.1: 1 entries
   seq 5 permit 1.1.1.1/32
```


© 2021 IP Infusion Inc. Proprietary

show bgp neighbors received-routes

Use this command to display the received routes from a neighbor.

To display all the received routes from a neighbor, perform a BGP soft reconfigure first.

Command Syntax

```
show bgp neighbors (A.B.C.D|X:X::X:X|WORD) received-routes
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X) received-routes
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) received-routes
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) routes received
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`WORD`	Interface name
`ipv4`	IPv4 addresses
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp neighbors 11.11.11.1 received-routes
BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network              Next Hop       Metric    LocPrf       Weight   Path
*>i 33.33.33.33/32   11.11.11.1      0         100          0        i

Total number of prefixes 1
```

show bgp neighbors routes

Use this command to display all accepted routes learned from neighbors.

Command Syntax

```
show bgp neighbors (A.B.C.D|X:X::X:X|WORD) routes
show ip bgp neighbors (A.B.C.D|X:X::X:X|WORD) routes
show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X|WORD) routes
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`WORD`	Interface name
`ipv4`	IPv4 addresses
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following output displays detailed information about the neighbor.

```
#show bgp neighbors 10.10.10.2 routes
BGP neighbor is fe80::203:47ff:feb0:d72b, remote AS 10, local AS 10, internal
link
  BGP version 4, remote router ID 10.10.10.50
  BGP state = Established, up for 00:02:01
  Last read 00:00:01, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
  Sent 5 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
```


© 2021 IP Infusion Inc. Proprietary

Table 4-159 explains the output fields.

Table 4-159: show bgp neighbors routes output details

Field	Description
BGP neighbor	Neighbor identifier along with the local and remote Autonomous System numbers.
BGP version	The version of BGP being used by the neighbor device, along with the remote router ID number.
BGP state	The current state of the neighbor connection and length of time within the current state. Possible states are: Idle, Connect, Active, and Established.
Last read	The amount of time in Hours**:** Minutes**:** Seconds since this device last checked the Hold Time parameters.
hold time	The amount of time this device waits for a Keepalive or Update message before the BGP connection is closed.
Keepalive interval	KEEPALIVE messages are sent periodically to ensure that the connection is live.
Neighbor capabilities	New or optional parameters called “Capabilities.” Provides a graceful way to advertise new or unique options without causing peering to terminate. The capabilities are communicated in TLV fields. (see RFC 3392). In the example output above, the following capabilities were advertised by the neighbor and were received and understood by this device: • Route refresh • Address family IPv4 Unicast • Address family IPv6 Unicast
Route refresh	This helps to identify that and synchronize the peers without a hard reset.
For address family	Address Family Identifier (AFI) IPv4 Unicast.
Received messages	Information received from the neighbors.
notifications	Passes information to a router about sessions.
in que	Number of messages currently residing in the queue awaiting action.
Route refresh request	Information received and sent.
Minimum time between advertisement runs	Interval between exchange of messages.
For address family: IPv4 Unicast	The following three values are subordinate to the IPv4 Unicast Address Family.
Community attributes sent to this neighbor	Both the standard and the extended community information has been sent to the neighbor.
accepted prefixes	Configure a limit to the number of prefixes that can be accepted in a BGP peer session.
announced prefixes	A prefix announced in BGP consists of the IPV4 or IPV6 address block being announced.

show bgp nexthop-tracking

Use this command to display BGP nexthop-tracking status.

Command Syntax

```
show bgp nexthop-tracking
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp nexthop-tracking

Configured NHT: ENABLED
NHT Delay time-interval : 6
BGP VRF: (Default) VRF_ID 0
BGP Instance: (Default), AS: 100, router-id 4.4.4.40
NHT is Enabled
Recvd Msg count from RIB: 0
NHT delay-timer remaining seconds: 0
BGP nexthop(s):
Total number of IPV4 nexthops : 0
Total number of IPV6 nexthops : 0

BGP VRF: VRF_A VRF_ID 2
BGP Instance: (Default), AS: 100, router-id 4.4.4.40
NHT is Enabled
Recvd Msg count from RIB: 0
NHT delay-timer remaining seconds: 0
BGP nexthop(s):
Total number of IPV4 nexthops : 0
Total number of IPV6 nexthops : 0
```

Table 4-160 explains the output fields.

Table 4-160: show bgp nexthop-tracking output details

Field	Description
Configured NHT	Whether Next Hop Tracking (NHT) is enabled or disabled.
NHT Delay time-interval	A delay timer that indicates how long this device waits before checking its RIB for changes.

© 2021 IP Infusion Inc. Proprietary

Table 4-160: show bgp nexthop-tracking output details

Field	Description
BGP VRF	Name and ID number of this BGP VRF.
BGP Instance	Autonomous System number and router ID.
NHT is Enabled	NHT Network enables the measurement and comparison of performance.
Recvd Msg count from RIB	Number of received change-messages from the RIB.
NHT delay-timer remaining seconds	Time remaining until the next decision cycle.
BGP nexthop(s)	Nexthop in the BGP to reach a certain destination.
Total number of IPV4 nexthops	Number of nexthops in the IPv4 Address Family.
Total number of IPV6 nexthops	Number of nexthops in the IPv6 Address Family.

show bgp nexthop-tree-details

Use this command to display BGP nexthop-tree details.

Command Syntax

```
show bgp nexthop-tree-details
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp nexthop-tree-details
BGP Instance: (Default), AS: 65534, router-id 51.1.1.3
AFI_IP Nexthop count : 0
AFI_IP6 Nexthop count : 0

BGP Instance: (Default), AS: 0, router-id 51.1.1.3
AFI_IP Nexthop count : 0
AFI_IP6 Nexthop count : 0
```

Table 4-161 explains the output fields.

Table 4-161: show bgp nexthop-tree-details output details

Field	Description
Bgp Instance	The Autonomous System number and router ID.
AFI_IP Nexthop count	Nexthop count for the IPv4 Address Family
AFI_IP6 Nexthop count	Nexthop count for the IPv6 Address Family

© 2021 IP Infusion Inc. Proprietary

show bgp paths

Use this command to display BGP path information.

Command Syntax

```
show bgp paths
show bgp (ipv6) paths
show ip bgp paths
show ip bgp ipv4 (unicast|multicast) paths
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp paths

Address         Refcnt    Path
[0x1af8ee0:0]    (21)
[0x1b3ceb0:345] (14)      64602
[0x1c71d40:821] (12008)   64602 65500
[0x1d03fb0:822] (12008)   64602 65501
```

Table 4-162 explains the output fields.

Table 4-162: show bgp paths output details

Field	Description
Address	Hash and hash key separated by the colon character.
Refcnt	Number of routed using that path.
Path	Autonomous System Number (ASN) for the route.

show bgp prefix-list

Use this command to display routes matching the prefix-list.

Command Syntax

```
show bgp prefix-list WORD
show bgp (ipv4|ipv6) (unicast|multicast|) prefix-list WORD (vrf
  (VRFNAME|all|default|))
show ip bgp prefix-list WORD
show ip bgp prefix-list WORD (exact-match)
show ip bgp prefix-list WORD (exact-match) (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) prefix-list WORD
show ip bgp ipv4 (unicast|multicast) prefix-list WORD (exact-match)
```

Parameters

`WORD`	Name of the IP prefix list
`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`exact-match`	Exact match of the prefix list
`vrf`	VPN Routing/Forwarding instance
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp prefix-list Route1
BGP table version is 1, local router ID is 12.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network        Next Hop          Metric    LocPrf       Weight   Path
*>1.1.1.1/32   0.0.0.0            0         100         32768      i

Total number of prefixes 1
```


© 2021 IP Infusion Inc. Proprietary

show bgp quote-regexp

Use this command to display route matching an AS path quoted regular expression.

Command Syntax

```
show bgp quote-regexp WORD
show bgp (ipv4|ipv6) (unicast|multicast|) quote-regexp WORD
show ip bgp quote-regexp WORD
show ip bgp ipv4 (unicast|multicast) quote-regexp WORD
```

Parameters

`WORD`	A regular expression to match the AS paths. Use quotes to enclose the regular expression.
`ipv4`	IPv4 route information
`ipv6`	IPv6 route information
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp quote-regexp ^$
BGP table version is 1, local router ID is 102.67.98.95
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network               Next Hop     Metric    LocPrf       Weight    Path
*> 2001:43f8:bb1::/64    :            0        100         32768      ?

Total number of prefixes 1
```

show bgp regexp

Use this command to display routes matching the AS path regular expression.

Command Syntax

```
show bgp regexp LINE
show bgp (ipv4|ipv6) (unicast|multicast) regexp LINE
show bgp (ipv6) regexp LINE
show ip bgp regexp LINE
show ip bgp regexp LINE (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) regexp LINE
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`LINE`	A regular expression to match the AS paths
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp regexp ^$
BGP table version is 1, local router ID is 102.67.98.95
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network                Next Hop   Metric    LocPrf       Weight   Path
*> 2001:43f8:bb1::/64     ::        0        100          32768     ?

Total number of prefixes 1
```


© 2021 IP Infusion Inc. Proprietary

show bgp route-map

Use this command to display routes that match the specified route map.

Command Syntax

```
show bgp route-map WORD
show bgp (ipv4|ipv6) (unicast|multicast) route-map WORD
show bgp (ipv6) route-map WORD
show ip bgp route-map WORD
show ip bgp route-map WORD (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) route-map WORD
```

Parameters

`WORD`	Routes matching the route-map
`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`vrf`	VPN routing/forwarding instance
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp prefix-list Route1
BGP table version is 1, local router ID is 12.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric    LocPrf       Weight  Path
*>1.1.1.1/32     0.0.0.0               0         100         32768    i
```

show bgp statistics

Use this command to display BGP statistics.

Command Syntax

```
show bgp statistics
```

Parameters

None

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp statistics

============================================================
BGP VRF default statistics
============================================================
Neighbor aggregated statistics (sent/received)
Msgs          Bytes           Opens          Updates
16/17           394/0           1/2           0/0
Keepalives  Notifications  Route-refresh  Capabilities
15/15            0/0           0/0           0/0
BGP I/O Information
Active Open attempts            : 0
Passive Open attempts           : 0
BGP I/O Open loops              : 0
BGP I/O Open calls              : 0
BGP I/O Open recv calls         : 0
BGP I/O Send calls              : 0
BGP I/O Recv calls              : 0
BGP I/O Write calls             : 0
BGP I/O Write loops             : 0
BGP I/O Write loop yields       : 0
BGP I/O Read calls              : 0
BGP I/O Read loops              : 0
BGP I/O Read loop yields        : 0
BGP I/O process nlri yields     : 0
BGP I/O process withdraw yields : 0
BGP Read time exceeded          : 0
BGP Update send pending         : 0
BGP Update buffer not available : 0
BGP Update walk suspended       : 0
BGP Yielded in updates          : 0
BGP Yielded in packing          : 0
BGP No sendbuf for peer         : 0
BGP No withdraw buf for peer    : 0
BGP Yields in update peer loop  : 0
```


© 2021 IP Infusion Inc. Proprietary

```
No updates pending or no buffers: 0
No data to write                : 0
Msg queue recv errors           : 0
Sockets create/accept/close     : 2/1/2
Sockets create retries/failures : 1/0
Socket fd-close session         : 0
MemPool - Advertise             : | Total (0/0) blk_size:64
MemPool - AdjOut                : | Total (0/0) blk_size:12
MemPool - Advertise Attr        : | Total (0/0) blk_size:24
MemPool - BGP Info              : | Total (0/0) blk_size:216
MemPool - BGP Attr              : | Total (0/0) blk_size:224
MemPool - BGP Node IPv4         : | Total (0/0) blk_size:128
MemPool - BGP Node IPv6         : | Total (0/0) blk_size:136
MemPool - BGP Node EVPN         : | Total (0/0) blk_size:160
MemPool - BGP Node Max KeyLen   : | Total (0/0) blk_size:176
MemPool - BGP RIB msg4          : | Total (0/0) blk_size:4440
MemPool - BGP RIB msg6          : | Total (0/0) blk_size:424
MemPool - BGP MPLS REQ          : | Total (0/0) blk_size:32
#
```

© 2021 IP Infusion Inc. Proprietary

show bgp summary

Use this command to display a summary of BGP neighbor status.

Command Syntax

```
show bgp summary
show bgp (ipv4|ipv6) (unicast|multicast|) summary
show ip bgp summary
show ip bgp summary (vrf (VRFNAME|all|default))
show ip bgp ipv4 (unicast|multicast) summary
```

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp summary

BGP router identifier 6.6.6.6, local AS number 64601

BGP table version is 1

1 BGP AS-PATH entries

0 BGP community entries

Neighbor V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/PfxRcd

*12.1.1.24 64902    7          7       1      0      0   00:02:54       0

* Dynamically created based on a listen range command

BGP dynamic peer-group: group1
```


© 2021 IP Infusion Inc. Proprietary

```
listen range:  12.1.0.0/16
Total number of dynamically created neighbors/limit: 1/(200)
Total number of dynamically created neighbors: 1
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
Total number of neighbors 1
Total number of Established sessions 1

BGP dynamic peer-group: group2
listen range:  12.2.0.0/16
Total number of dynamically created neighbors/limit: 0/(200)
Total number of dynamically created neighbors: 0
Total number of activated dynamic peer-groups for IPv4 Unicast address-family: 1
```

Header

```
BGP router identifier 10.10.15.50, local AS number 65000
1 BGP AS-PATH entries
0 BGP community entries
```

- The BGP router identifier is 10.10.15.50 and the local router AS number is 65000.
- The BGP table version tracks the local BGP table version. Any time the BGP best path algorithm executes, the table version increments.
- There is one BGP AS-PATH entry and no community entries.

Neighbor Entry Fields

Table 4-163 explains the fields for each neighbor entry.

Table 4-163: neighbor entry fields

Field	Description
Neighbor	IP address of peer.
V	BGP version of peer.
AS	Autonomous system number of peer.
MsgRcvd	Messages received since the BGP connection was established.
MsgSent	Messages sent since the BGP connection was established.
TblVer	Last version of the local router's BGP database advertised to the peer.
InQ	Received messages waiting in the input queue for further processing.
OutQ	Messages waiting in the output queue to be sent.

Table 4-163: neighbor entry fields (Continued)

Field	Description
Up/Down	Connection up time and down time.
State/PfxRcd	If the TCP session is up and the BGP peers have formed an adjacency, this field shows how many prefixes have been received from the remote neighbor. Other states: Idle: The local router has not allocated resources for the peer connection, so incoming connection requests are refused Idle (Admin): The peer has shut down Idle (PfxCt): Prefix overflow Idle (G-shut): Graceful shutdown Connect: BGP is waiting for the TCP connection to complete Active: the local router is trying to establish a TCP connection to the remote peer. You might see this if the local peer has been configured, but the remote peer is unreachable or has not been configured. OpenSent: BGP is waiting for an open message from its peer OpenConfirm: BGP received an open message from the peer and is now waiting for a keepalive or notification message. If BGP receives a keepalive message from the peer, the state changes to established. If the message is a notification, the state changes to idle. Established: BGP is ready to exchange update, notification, and keepalive messages with its peer Invalid: The session state is invalid

Neighbor Entry Example

```
10.10.14.51   4   100  93       120     0      0    0     00:42:16        0
```

- The neighbor has the IP address 10.10.14.51 and AS number 100.
- The neighbor uses BGP version 4.
- 93 messages have been received.
- 120 messages have been sent.
- The BGP routing table version is 0.
- There are no received messages waiting in the input queue for further processing.
- There are no messages waiting in the output queue to be sent.
- The connection has been up for 0 hours, 42 minutes and 53 seconds.
- The local router has received no prefixes from this neighbor.

© 2021 IP Infusion Inc. Proprietary

show bgp X:X::X:X

Use this command to display BGP network information in an IPv6 environment.

Command Syntax

```
show bgp X:X::X:X
show bgp (ipv6) X:X::X:X
show bgp (ipv6) (unicast|multicast) X:X::X:X
```

Parameters

`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`X:X::X:X`	IPv6 prefix (network), for example, 2003::

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp ipv6 6666::/64
BGP routing table entry for 6666::/64
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to peer-groups:
  Book-v6
  Local
    :: from :: (102.67.98.95)
      Origin incomplete,metric 0, localpref 100, weight 32768      valid,
sourced, best, source safi: 0
      Community: 37721:2000
      Last update: Thu Feb  4 09:00:50 2021
```

show bgp X:X::X:X/M longer prefixes

Use this command to display BGP network information along with mask information.

Command Syntax

```
show bgp X:X::X:X/M longer-prefixes
```

Parameters

`X:X::X:X/M`	IPv6 prefix (network/length), for example, 2003::/16

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bgp 2001:43f8:bb1::/64 longer-prefixes
BGP table version is 1, local router ID is 102.67.98.95
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network               Next Hop   Metric    LocPrf       Weight  Path
*>2001:43f8:bb1::/64    ::         0         100         32768     ?

Total number of prefixes 1
```


© 2021 IP Infusion Inc. Proprietary

show debugging bgp

Use this command to display BGP debugging options.

Command Syntax

```
show debugging bgp
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the show debugging bgp command.

```
#show debugging bgp
BGP debugging status:
 BGP debugging is on
 BGP events debugging is on
 BGP updates debugging is on
 BGP fsm debugging is on
```

show ip bgp

Use this command to display BGP routes.

Command Syntax

```
show ip bgp
show ip bgp ipv4 (unicast|multicast)(vrf (VRFNAME|all|default))
```

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows routes learned from both iBGP and eBGP peers.

```
#show ip bgp
BGP table version is 0, local router ID is 10.100.0.77
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S stale,
      Origin codes: i - IGP, e - EGP,? - incomplete
       Network             Next Hop      Metric LocPrf   Weight   Path
   *> 172.16.1.0/24     10.10.10.78                          0       1 4 i
   *> 192.16.1.0        10.10.10.78       200                0       1 4 ?
   *                    10.100.0.62       100                0       3 4 ?
   *>i 192.17.1.0       10.100.0.62                 100      0       i

Total number of prefixes 2
```

Header

```
BGP table version is 0, local router ID is 10.100.0.77
```

- The BGP table version tracks the local BGP table version. Any time the BGP best path algorithm executes, the table version increments.
- The Router ID of the local router is `10.100.0.77`.

```
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i - internal
```


© 2021 IP Infusion Inc. Proprietary

Table 4-164 explains the status codes in the header.

Table 4-164: status codes

Status code	Description	Comments
s	suppressed	Whether the route is suppressed and will not be advertised to the neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
p	stale	When the BGP neighbor from which a route is learned is in graceful restart, the route is retained in the BGP routing table, but marked as stale.
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The route selected as the best path and installed in the kernel routing table.
i	internal	Whether the route is learned from an iBGP peer. If this symbol is not present, the route was learned from an eBGP peer.

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Table 4-165 explains the codes are at the end of each routing entry that show where the route originated.

Table 4-165: origin codes

Origin code	Description	Comments
i	IGP	The route originated from an Interior Gateway Protocol.
e	EGP	The route originated from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an Interior Gateway Protocol.

Route Entry Fields

Table 4-166 explains the fields shows for each route.

Table 4-166: route entry fields

Field	Description
Network	Network prefix installed in BGP. If multiple routes exist for the same prefix, only the first prefix is identified and others have blank spaces. The status codes are explained in Table 4-164.
Next Hop	IP address of the nexthop for this route.

Table 4-166: route entry fields (Continued)

Field	Description
Metric	Multiple-Exit Discriminator (MED). If there are multiple paths to the same destination from a single routing protocol, then the multiple paths have the same administrative distance and the best path is selected based on this metric. The path with the lowest metric is selected as the optimal path and installed in the routing table.
LocPrf	Local preference set with the `set local-preference` command. This value is used only with iBGP sessions within the local autonomous system to determine if a route towards a destination is the “best” one. The path with the highest local preference is preferred.
Weight	This field applies only to routes within an individual router. If a route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.
Path and origin	The autonomous systems through which the prefix advertisement passed. The origin codes are explained in Table 4-165

Route Entry Examples

```
*> 172.16.1.0/24    10.10.10.78                          0    1 4 i
```

- The absence of status code “i” means the route is external and was learned from an eBGP peer.
- The “>” means this route is selected to be installed in the kernel routing table. Its network address is 172.16.1.0/24.
- The IP address of the nexthop for this route is 10.10.10.78.
- This route was learned from a peer, so it has a default weight of 0.
- The path “1 4” means the prefix advertisement passed through AS1 and AS4.
- The origin code “i” means the prefix was added by a network statement at an originating AS.

```
*> 192.16.1.0       10.10.10.78            200            0    1 4 ?
*                   10.100.0.62            100            0    3 4 ?
```

- The same prefix was learned from two different ASs, AS1 and AS3.
- The route learned from AS1 is chosen as the best route because AS1 has a lower Router ID (10.10.10.78) than AS2 (10.100.0.62). Although the metric of the route learned from AS1 is higher (200) than the route learned from AS3 (100), this attribute is not used in the best path selection decision because the metrics are compared only if the first (neighboring) AS is the same in the two paths.
- The origin code “?” indicates that the routes were learned through redistribution.

```
*>i192.17.1.0       10.100.0.62                    100     0    i
```

- The route is learned through an iBGP peer as indicated by the status code “i”.
- The preference of the route, used only with the local AS, is 100 (the default value).

© 2021 IP Infusion Inc. Proprietary

show ip bgp cidr-only

Use this command to display routes with non-natural network masks.

Command Syntax

```
show ip bgp cidr-only
show ip bgp ipv4 (unicast|multicast) cidr-only
```

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the `show ip bgp cidr-only` command.

```
#show ip bgp cidr-only
BGP table version is 0, local router ID is 10.10.10.50
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 3.3.3.0/24       10.10.10.10                              0 11 i
Total number of prefixes 2
```

Table 4-167 explains the status codes in the header.

Table 4-167: status codes

Status code	Description	Comments
s	suppressed	Whether the route is suppressed and will not be advertised to the neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
p	stale	When the BGP neighbor from which a route is learned is in graceful restart, the route is retained in the BGP routing table, but marked as stale.

Table 4-167: status codes (Continued)

*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The route selected as the best path and installed in the kernel routing table.
i	internal	Whether the route is learned from an iBGP peer. If this symbol is not present, the route was learned from an eBGP peer.

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Table 4-168 explains the codes are at the end of each routing entry that show where the route originated.

Table 4-168: origin codes

Origin code	Description	Comments
i	IGP	The route originated from an Interior Gateway Protocol.
e	EGP	The route originated from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an Interior Gateway Protocol.

Route Entry Fields

Table 4-169 explains the fields shows for each route.

Table 4-169: route entry fields

Field	Description
Network	Network prefix installed in BGP. If multiple routes exist for the same prefix, only the first prefix is identified and others have blank spaces. The status codes are explained in Table 4-167.
Next Hop	IP address of the nexthop for this route.
Metric	Multiple-Exit Discriminator (MED). If there are multiple paths to the same destination from a single routing protocol, then the multiple paths have the same administrative distance and the best path is selected based on this metric. The path with the lowest metric is selected as the optimal path and installed in the routing table.
LocPrf	Local preference set with the `set local-preference` command. This value is used only with iBGP sessions within the local autonomous system to determine if a route towards a destination is the “best” one. The path with the highest local preference is preferred.
Weight	This field applies only to routes within an individual router. If a route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.
Path and origin	The autonomous systems through which the prefix advertisement passed. The origin codes are explained in Table 4-168

© 2021 IP Infusion Inc. Proprietary

show ip bgp community-info

Use this command to list all BGP community information.

Command Syntax

```
show ip bgp community-info
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp community-info
Address Refcnt Community
[0x262a4c0] (1) 1:1
```

show ip bgp peer-group

Use this command to list the BGP peer group information in ipv4 unicast.

Command Syntax

```
show ip bgp peer-group (WORD|)
```

Parameters

NAME	Name of the peer group.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp peer-group group1
BGP dynamic peer-group is group1, EBGP, remote AS 64902
  BGP dynamic peer-group group1 listen range group members:
  12.1.0.0/16
  BGP version 4
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
  Peer-group member:
  *12.1.1.2
  Index 0, Offset 0, Mask 0x1
  0 accepted prefixes, 0 announced prefixes
```


© 2021 IP Infusion Inc. Proprietary

show ip bgp peer-group vrf all

Use this command to list all BGP peer group VRF information.

Command Syntax

```
show ip bgp peer-group vrf all
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp peer-group vrf all
% VRF: VRF1

BGP dynamic peer-group is group2, EBGP, remote AS 64902
  BGP dynamic peer-group group2 listen range group members:
  12.2.0.0/16
  BGP version 4
Minimum time between advertisement runs is 30 seconds
% VRF: management
Peer-Group not found

% VRF: default

BGP dynamic peer-group is group1, EBGP, remote AS 64902
  BGP dynamic peer-group group1 listen range group members:
  12.1.0.0/16
  BGP version 4
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
  Peer-group member:
  *12.1.1.2
  Index 0, Offset 0, Mask 0x1
  0 accepted prefixes, 0 announced prefixes
```

show ip bgp rtfilter all

Use this command to display route target filters sent and received.

Command Syntax

```
show ip bgp rtfilter all
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp rtfilter all
RTFilter's Received
********************
peer-ip 1.1.1.1
RTFilter's Sent
********************
peer-ip 1.1.1.1
```


© 2021 IP Infusion Inc. Proprietary

show ip bgp scan

Use this command to display BGP scan status.

Command Syntax

```
show ip bgp scan
```

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip bgp scan
BGP VRF: (Default) VRF_ID 0
BGP scan interval is 60 secs
scan remain-time: 3 secs
Current BGP nexthop cache:
BGP connected route:
 10.10.10.0/24
 10.10.11.0/24
```

show ip bgp vpnv4

Use this command to display information relating to VPNv4.

Command Syntax

```
show ip bgp vpnv4 all
show ip bgp vpnv4 all A.B.C.D
show ip bgp vpnv4 all neighbors
show ip bgp vpnv4 all neighbors A.B.C.D
show ip bgp vpnv4 all summary
show ip bgp vpnv4 all tags
show ip bgp vpnv4 rd WORD
show ip bgp vpnv4 rd WORD A.B.C.D
show ip bgp vpnv4 rd WORD label
show ip bgp vpnv4 rd WORD neighbors
show ip bgp vpnv4 rd WORD neighbors A.B.C.D
show ip bgp vpnv4 rd WORD summary
show ip bgp vpnv4 view WORD all
show ip bgp vpnv4 vrf NAME
show ip bgp vpnv4 vrf NAME A.B.C.D
show ip bgp vpnv4 vrf NAME label
show ip bgp vpnv4 vrf NAME summary
```

Parameters

`all`	Displays information about all VPNv4 NLRIs
`A.B.C.D`	Network
`neighbors`	TCP and BGP neighbor connections
`A.B.C.D`	Network
`summary`	Summary display
`tags`	BGP tags for prefixes
`rd`	Route distinguisher
`WORD`	BGP view name
`A.B.C.D`	Network
`label`	MPLS Labels for prefixes
`neighbors`	TCP and BGP neighbor connections
`A.B.C.D`	Network
`summary`	Summary display
`view`	VPNv4 NLRI-specific information
`WORD`	BGP view name

© 2021 IP Infusion Inc. Proprietary

`vrf`	VRF VPNv4 NLRIs
`NAME`	VPN Routing/Forwarding instance name
`A.B.C.D`	Network
`label`	MPLS Labels for prefixes
`summary`	Summary display

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output from the `show ip bgp vpnv4 all` command displaying VPNv4 specific information

```
#show ip bgp vpnv4 all
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (VRF1)
* i 10.10.9.0/24     10.10.0.1                0   141      0  65000 ?
*>  10.10.9.0/24     10.10.14.50              0            0  65000 ?
*>  10.10.10.0/24    10.10.14.50                           0  65000 ?
* i 10.10.15.0/24    10.10.0.1                    141      0  65000 ?
*>  10.10.15.0/24    10.10.14.50              0            0  65000 ?

#show ip bgp vpnv4 all neighbors

BGP neighbor is 24.10.10.2, remote AS 65000, local AS 65000, internal link
  BGP version 4, remote router ID 179.112.0.1
  BGP state = Established, up for 10:04:14
  Last read 10:04:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Multicast: received
    Address family IPv6 Unicast: received
  Received 1641 messages, 0 notifications, 0 in queue
  Sent 1280 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 676, neighbor version 676
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  60000 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 24.10.10.1, Local port: 179
Foreign host: 24.10.10.2, Foreign port: 32959
Nexthop: 24.10.10.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

Table 4-170 explains the fields shows for each route.

Table 4-170: show ip bgp vpnv4 all neighbors output details

Field	Description
BGP neighbor	Router ID of the BGP neighbor.
remote AS	Autonomous system number of the neighbor.
local AS	Autonomous system number of the local system.
internal link	internal link: iBGP neighbor (in the same AS).
BGP version	The version of BGP being used by the neighbor device.
BGP state	The current state of the neighbor connection and length of time within the current state.Possible states are: Idle, Connect, Active, and Established.
Last read	The amount of time in Hours **:** Minutes **:** Seconds since this device last checked the Hold Time parameters.
hold time	The amount of time this device waits for a Keepalive or Update message before the BGP connection is closed.
Keepalive interval	KEEPALIVE messages are sent periodically to ensure that the connection is live.
Neighbor capabilities	New or optional parameters called “Capabilities.” Provides a graceful way to advertise new or unique options without causing peering to terminate. The capabilities are communicated in TLV fields. (see RFC 3392). In the example output above, the following capabilities were advertised by the neighbor and were received and understood by this device: • Route refresh • Address family IPv4 Unicast • Address family IPv6 Unicast
Received	Message count, notification count, number of messages waiting in the queue.
Sent	Message count, notification count, number of messages waiting in the queue.
Route refresh request	Route requests sent and received.
For address family	As stated – in this case IPv4 Unicast.
BGP table version	For each of the address families agreed upon, BGP maintains a separate table.
neighbor version	Tracks prefixes that have been sent and those that need to be sent.
connections established	The number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other. “Dropped” means the number of time the connection has failed or gone down.
local host foreign host	Local host is the IP address and the port number of the local system used for the peering session. Foreign host is the IP address and the port of the neighbor. BGP always uses the TCP port number 179 for the peer originating the session.

© 2021 IP Infusion Inc. Proprietary

Table 4-170: show ip bgp vpnv4 all neighbors output details (Continued)

Field	Description
nexthop	The IP address of the next hop used to reach the neighbor. eBGP or iBGP peers do not need to be directly connected. Peering sessions can be set up across multiple hops. If the neighbors are directly connected, the IP address of the local system is listed as the next hop.
nexthop global	The global IPv6 address of the next hop
nexthop local	The link-local IPv6 address of the next hop
non shared network	The peering session is running on a non shared network.
last reset	Time since this peering session was last reset. The reason for the reset is displayed on this line.
notification error message	Last error message sent.

show ip extcommunity-list

Use this command to display BGP routes that match an extended community list.

Command Syntax

```
show ip extcommunity-list (WORD | )
show ip extcommunity-list (<1-199>|WORD)
show ip bgp extcommunity-list WORD (exact-match|)(vrf VRFNAME|)
```

Parameters

WORD	Name of extended community list
<1-199>	Number of extended community list
VRFNAME	VPN routing/forwarding instance name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip extcommunity-list test
Named extended community expanded list test
    permit rt 100:100
```


© 2021 IP Infusion Inc. Proprietary

show ip protocols

Use this command to display information about the IP protocols such as IP routing process parameters and statistics.

Command Syntax

```
show ip protocols
show ip protocols bgp
```

Parameters

bgp	BGP information

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip protocols bgp
Routing Protocol is "bgp 100"
Sending updates every 30 seconds with +/-50%, next due in 12 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing: connected static
Default version control: send version 2, receive version 2
Interface        Send  Recv   Key-chain
   eth0                2     2
Routing for Networks:
  10.10.0.0/24
Routing Information Sources:
  Gateway          BadPackets BadRoutes  Distance Last Update
 Distance: (default is 120)
```

Table 4-171 explains the fields shows for each route.

Table 4-171: show ip protocols output details

Field	Description
Routing Protocol is "bgp 100"	Specifies the routing protocol used.
Sending updates every 30 seconds	Specifies the time between sending updates.
Next due in 12 seconds	Precisely when the next update is due to be sent.
Timeout after 180 seconds	Specifies the value of the timeout parameter.
Redistributing	Lists the protocol that is being redistributed.

Table 4-171: show ip protocols output details

Field	Description
Routing for Networks	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the IP Infusion software is using to build its routing table.

© 2021 IP Infusion Inc. Proprietary

show ip vrf

Use this command to display the routing information of the VRF, such as interface, route distinguisher, route-target, and so on.

Command Syntax

```
show ip vrf
show ip vrf WORD
```

Parameter

WORD	VRF name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip vrf VRF_A
VRF VRF_A; (table=1)
```

show running-config as-path access-list

Use this command to show the running system status and configuration details for access lists based on autonomous system paths.

Command Syntax

```
show running-config as-path access-list
```

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#show running-config as-path access-list
!
ip as-path access-list wer permit knsmk
!
(config)#
```


© 2021 IP Infusion Inc. Proprietary

show running-config community-list

Use this command to show the running system status and configuration details for community lists.

Command Syntax

```
show running-config community-list
```

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
(config)#show running-config community-list
!
ip community-list standard aspd permit internet
ip community-list expanded cspd deny ljj
ip community-list expanded cspd permit dcv
ip community-list expanded wde permit njhd
ip community-list expanded wer deny sde
(config)#
```

© 2021 IP Infusion Inc. Proprietary

Appendix 5 Regular Expressions

Table 5-172 shows the regular expression special characters used in BGP commands. You can use these characters in combination to build complex regular expressions.

Table 5-172: Regular expression characters

Symbol	Character	Meaning
^	Caret	Matches the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign	Matches the end of the input string.
.	Period	Matches a single character (including white spaces).
*	Asterisk	Matches none or more sequences of a pattern.
+	Plus sign	Matches one or more sequences of a pattern.
?	Question mark	Matches none or one occurrence of a pattern.
_	Underscore	Matches spaces, commas, braces, parenthesis, or the beginning and end of an input string.
[]	Brackets	A range of single-characters.
-	Hyphen	Separates the end points of a range.

© 2021 IP Infusion Inc. Proprietary

Intermediate System to Intermediate System Command Reference

Contents

This document contains these chapters:

- Chapter 1, *IS-IS Commands*
- Chapter 2, *IS-IS Graceful Restart Commands*
- Chapter 3, *IS-IS Show Commands*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 IS-IS Commands

This chapter describes the IS-IS commands:

- accept-lifetime
- address-family ipv6
- adjacency-check
- area-password
- authentication key-chain
- authentication mode
- authentication send-only
- bfd all-interfaces
- capability cspf
- clear clns neighbors
- clear clns is-neighbors
- clear ip isis route
- clear isis adjacency
- clear isis counter
- clear isis interface counter
- clear isis process
- debug isis
- default-information originate
- distance (IPv4)
- distance (IPv6)
- domain-password
- dynamic-hostname
- fast-reroute per-prefix
- fast-reroute terminate-hold-on interval
- fast-reroute tie-break
- ignore-lsp-errors
- ip router isis
- ipv6 router isis
- isis authentication key-chain
- isis authentication mode md5
- isis authentication send-only
- isis bfd
- isis circuit-type
- isis csnp-interval
- isis fast-reroute per-prefix candidate disable

- isis hello-interval
- isis hello-multiplier
- isis hello padding
- isis lsp-interval
- isis mesh-group
- isis metric
- isis network
- isis password
- isis priority
- isis retransmit-interval
- ispf
- isis wait-timer
- isis wide-metric
- isis tag
- isis te-metric
- is-type
- key chain
- key
- key-string
- key-string encrypted
- lsp-gen-interval
- lsp-mtu
- lsp-refresh-interval
- max-area-address
- max-lsp-lifetime
- metric-style
- mpls traffic-eng
- mpls traffic-eng router-id
- net
- passive-interface
- prc-interval-exp
- redistribute
- redistribute isis
- redistribute isis WORD
- router isis
- send-lifetime
- snmp restart isis
- spf-interval-exp
- summary-address

© 2021 IP Infusion Inc. Proprietary

- summary-prefix

accept-lifetime

Use this command to specify the time period during which the authentication on a key chain is received as valid.

Use the `no` parameter with this command to negate this command.

Command Syntax

```
accept-lifetime HH:MM:SS MONTH <01-31> <1993-2035> HH:MM:SS MONTH <01-31> <1993-2035>
accept-lifetime HH:MM:SS MONTH <01-31> <1993-2035> infinite
accept-lifetime HH:MM:SS MONTH <01-31> <1993-2035> duration <1-2147483646>
no accept-lifetime
```

Parameters

`HH:MM:SS`	Specify the start time of accept-lifetime in hours, minutes and seconds.
`<01-31>`	Specify the day of the month to start. If the day is a single-digit, the leading 0 must be added, example: 01, 02, 03, etc.
`MONTH`	Specify the month of the year to start as the first three letters of the month with first letter in upper case, for example, Jan. (case sensitive).
`<1993-2035>`	Specify the year to start.
`HH:MM:SS`	Specify the end time of accept-lifetime in hours, minutes and seconds.
`<01-31>`	Specify the day of the month to end. If the day is a single-digit, the leading 0 must be added, example: 01, 02, 03, etc.
`MONTH`	Specify the month of the year to end as the first three letters of the month with first letter in caps, for example, Jan. (case sensitive).
`<1993-2035>`	Specify the year to end.
`duration`	Indicate the duration parameter.
`<1-2147483646>`	Specify the actual end time duration of a key in seconds.
`infinite`	Specify the end time to never expire.

Default

By default, accept-lifetime command is disabled

Command Mode

Keychain-key mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the setting of accept-lifetime for key1 on the key chain named mychain.

```
#configure terminal
(config)#key chain mychain
```


© 2021 IP Infusion Inc. Proprietary

```
(config-keychain)#key 1
(config-keychain-key)#accept-lifetime 03:03:01 Dec 03 2004 04:04:02 Oct 06
2006
```

address-family ipv6

Use this command to enter 'address-family ipv6' mode, where users can configure IPv6 routing specific configuration.

Use the no parameter with this command to remove all configuration under 'address-family ipv6'.

Command Syntax

```
address-family ipv6 (unicast|)
no address-family ipv6 (unicast|)
```

Parameters

`unicast`	Specify unicast routing for IPv6.

Default

Unicast routing is not configured.

Command Mode

Router mode

Example

```
#configure terminal
(config)#router isis bb
(config-router)#address-family ipv6 unicast
```


© 2021 IP Infusion Inc. Proprietary

adjacency-check

Use this command to check ISIS neighbor protocol support.

Use the `no` parameter with this command to uncheck ISIS neighbor protocol support.

Command Syntax

```
adjacency-check
no adjacency-check
```

Parameters

None

Default

By default, adjacency-check command is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router isis bb
(config-router)#adjacency-check

(config-router)#no adjacency-check
```

area-password

Use this command to set the authentication password for the Level-1 area and to set authentication on Level-1 sequence number PDUs. This command enables authentication when receiving and sending link-state and sequence number PDUs in Level-1 areas. The password must be the same for all the ISIS routers in the same area.

Use the `no` parameter with this command to clear the area password.

Command Syntax

```
area-password WORD
area-password WORD authenticate snp (send-only|validate)
no area-password
```

Parameters

`WORD`	Password string.
`authenticate`	Insert the password into Level-1 SNP PDUs.
`snp`	Sequence number PDUs.
`send-only`	Only insert the password into the Level-1 sequence number PDUs, but not check the password in sequence number PDUs that it receives. Use this keyword during a software upgrade to ease the transition.
`validate`	Insert the password into Level-1 sequence number PDUs and check the password in sequence number PDUs that it receives.

Default

By default, the area password is not configured

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router isis bb
(config-router)#area-password mypasswd

(config)#router isis bb
(config-router)#area-password myPass authenticate snp send-only

(config)#router isis bb
(config-router)#no area-password
```


© 2021 IP Infusion Inc. Proprietary

authentication key-chain

Use this command to set the key chain to be used for authentication at the instance level. Authentication mode must be set to `md5` to configure the key chain. If no key chain is configured with the key-chain command, no key-chain authentication is performed.

Only one authentication key-chain is applied to an ISIS interface at a time. That is, issuing a second `isis authentication key-chain` command overrides the first `isis authentication key-chain` command. If neither the `level-1` nor the `level-2` keyword is configured, the chain applies to both levels. Authentication can be specified for an individual ISIS interface using the `isis authentication key-chain` command.

Use the `no` parameter with this command to unset the key chain used for authentication.

Command Syntax

```
authentication key-chain WORD (level-1|level-2|)
no authentication key-chain (level-1|level-2|)
```

Parameters

`WORD`	Specify the chain name (valid authentication keys).
`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

The key chain applies to the level(s) on which authentication mode is configured as MD5 if no level is specified.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router isis 1
(config-router)#authentication key-chain myKey level-1
```

authentication mode

Use this command to set the authentication mode at the instance level.

If clear-text authentication was configured using the `area-password` or `domain-password` commands, the `authentication mode` command overrides both of those commands (based on the level at which MD5 is configured). If the `authentication mode` command was used first, and subsequently an attempt is made to use the `area-password` or `domain-password` commands, the attempt fails. To configure clear-text authentication using the `area-password` or `domain-password` commands, first use the `no authentication mode` command.

The type of authentication and the level to which it applies can be specified for a single ISIS interface, rather than per ISIS instance, using the `isis authentication mode` command.

Use the `no` parameter with this command to unset the authentication mode.

Command Syntax

```
authentication mode {md5|text} (level-1|level-2|)
no authentication mode {md5|text} (level-1|level-2|)
```

Parameters

`md5`	Keyed message digest
`text`	Text mode
`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

The authentication mode is set to MD5 for both levels if no level is specified.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis 1
(config-router)#authentication mode md5 level-1

(config-router)#no authentication mode md5 level-1
```


© 2021 IP Infusion Inc. Proprietary

authentication send-only

Use this command to set the send-only option at the instance level.

Use this command before configuring the authentication mode and authentication key-chain, so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all routers that must communicate are configured with this command, enable the authentication mode and key chain on each router. Then, specify the `no authentication send-only` command to disable the send-only feature.

If the `level-1-2` keyword is configured, the send-only feature applies to both levels.

Use the `no` parameter with this command to unset the send-only option.

Command Syntax

```
authentication send-only (level-1-only|level-2-only|level-1-2)
no authentication send-only
```

Parameters

`level-1-only`	Set send-only option for level-1 only.
`level-2-only`	Set send-only option for level-2 only.
`level-1-2`	Set send-only option for level-1-2 only.

Default

By default, authentication send only is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis 1
(config-router)#authentication send-only level-1-only

(config-router)#no authentication send-only
```

bfd all-interfaces

Use this command to enable the Bidirectional Forwarding Detection (BFD) feature on the interfaces enabled with this ISIS instance.

This command sets BFD fall-over check for all the neighbors under specified process. To disable BFD checking on particular interface use `isis bfd disable` command at interface mode.

Use the no parameter with this command to disable BFD functionality for an ISIS instance.

Command Syntax

```
bfd all-interfaces
no bfd all-interfaces
```

Parameters

None

Default

By default, the BFD feature is disabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router isis aa
(config-router)#bfd all-interfaces

(config-router)#no bfd all-interfaces
```


© 2021 IP Infusion Inc. Proprietary

capability cspf

Use this command to enable the constrained shortest path first (CSPF) feature in the ISIS module. CSPF calculates optimum explicit route (ER), using Traffic Engineering Database and (TED) and pre-existing Label Switched Path (LSP). The resulting ER is used by a signaling protocol (RSVP-TE) to set up LSPs. Use the no parameter with this command to disable CSPF functionality for an ISIS instance.

Command Syntax

```
capability cspf
no capability cspf
```

Parameters

None

Default

If this command is not used, the CSPF feature is disabled.

Command Mode

Router mode

Example

```
(config)#router isis aa
(config-router)#capability cspf
```

clear clns neighbors

Use this command to clear CLNS neighbor adjacencies.

Command Syntax

```
clear clns neighbors
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>ena
#clear clns neighbors
```


© 2021 IP Infusion Inc. Proprietary

clear clns is-neighbors

Use this command to clear IS neighbor adjacencies.

Command Syntax

```
clear clns is-neighbors System-ID
```

Parameters

`System-ID`	Neighbor system ID in XXXX.XXXX.XXXX format.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#clear clns is-neighbors 1111.1111.1111.1111
```

clear ip isis route

Use this command to clear IPv4 routes.

Command Syntax

```
clear ip isis (WORD|) route (redistribution|all)
```

Parameters

`WORD`	Name that identifies the IS-IS area.
`redistribution`	Clear IS-IS local redistribution routes.
`all`	Clear all of the IS-IS routing tables.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>ena
#clear ip isis route redistribution
```


© 2021 IP Infusion Inc. Proprietary

clear isis adjacency

This command is used to remove the entries from the IS-IS adjacency database. Clears all adjacencies for the specified routing instance or specified interface or particular system ID.

Command Syntax

```
clear isis adjacency (*|IFNAME|system-id XXXX.XXXX.XXXX|) (vrf VRFNAME|)
```

Parameters

`*`	Clear all neighbors.
`IFNAME`	Interface name.
`XXXX.XXXX.XXXX`	Neighbor System-ID.
`VRFNAME`	VRF name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear isis adjacency *
```

clear isis counter

Use this command to clear system-wide IS-IS counters (IsisSystemCounterEntry in RFC 4444).

Command Syntax

```
clear isis counter
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear isis counter
```


© 2021 IP Infusion Inc. Proprietary

clear isis interface counter

Use this command to clear interface counters. If you do not specify a parameter, then counters for all interfaces are cleared.

Command Syntax

```
clear isis interface counter (IFNAME|)
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear isis interface counter
```

clear isis process

Use this command to restart ISIS processes. If you do not specify a parameter, then all ISIS processes are restarted.

Command Syntax

```
clear isis (WORD|) process
```

Parameters

WORD	Name that identifies the IS-IS area.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear isis process
```


© 2021 IP Infusion Inc. Proprietary

debug isis

Use this command to turn on debugging for specified criteria. Debug commands enable to show some debugging information about specified criteria into file or terminal.

Use the `no` parameter to turn off debugging for specified criteria.

Command syntax

```
debug isis (all|)
debug isis (authentication|bfd|checksum|events|hello|mpls (interface IFNAME |
  System-ID|)|ifsm|local-updates|lsp|nfsm|nsm|pdu|protocol-errors|rib|spf)
no debug isis (all|)
no debug all
no debug all isis
undebug all
undebug isis (all|)
undebug all isis
no debug isis (authentication|bfd|checksum|events|hello|mpls (interface IFNAME |
  System-ID|)|ifsm|local-updates|lsp|nfsm|nsm|pdu|protocol-errors|rib|spf)
undebug isis (authentication|bfd|checksum|events|hello|mpls (interface IFNAME |
  System-ID|)|ifsm|local-updates|lsp|nfsm|nsm|pdu|protocol-errors|rib|spf)
```

Parameters

`all`	Enables all debugging.
`authentication`	Debugging for authentication.
`checksum`	Debugging for checksums.
`bfd`	Debugging for bidirectional forwarding detection.
`events`	Debugging for internal events.
`hello`	Debugging for hello processing.
`interface`	Interface.
`IFNAME`	Interface name.
`System-ID`	System identifier.
`ifsm`	Debugging for interface finite state machine.
`local-updates`	Debugging for local updates.
`lsp`	Debugging for link-state packet.
`nfsm`	Debugging for neighbor finite state machine.
`nsm`	Debugging for NSM messages.
`pdu`	Debugging for protocol data unit.
`protocol-errors`	Debugging for protocol errors.
`rib`	Debugging for RIB information.

`spf`	Debugging for shortest path first route calculation.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug isis pdu

#configure terminal
(config)#debug isis nsm
```


© 2021 IP Infusion Inc. Proprietary

default-information originate

Use this command to originate reachability information to a default route into link-state packets.

There is no default information in a Level-2 domain by default, while a Level-1 router calculates a default to L1L2 route during SPF calculation. This command originates a default route into a Level-2 domain.

Use the `no` parameter with this command to withdraw reachability information to a default route from link-state packets.

Command Syntax

```
default-information originate (always| level-1|) (route-map WORD|)
no default-information originate (always| level-1|)
```

Parameters

`originate`	Specify to distribute a default route
`always`	The default route is advertised even if there is no default route in the router's routing table.
`level-1`	Distribute in level-1.
`route-map`	Identifies other filtering options via a route map.

Default

There is no default information in Level-2 domain by default, while Level-1 router calculates default to L1L2 route during SPF calculation. This command enables to originate default route into Level-2 domain. As an added option, if the user wants to originate the default route in L1 LSP, the "level-1" parameter can be used as follows:

```
default-information originate level-1
```

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#default-information originate
(config-router)#exit
(config)#exit
```

distance (IPv4)

Use this command in router mode to set the administrative distance for all IPv4 routes or routes from a specific source.

Use the no parameter with this command to remove an administrative distance.

Command Syntax

```
distance <1-255> (System-ID (WORD|)|)
no distance (System-ID|)
```

Parameters

`<1-255>`	Distance range.
`System-ID`	Source ID in XXXX.XXXX.XXXX format.
`WORD`	Access-list name.

Default

By default, all options are turned off.

Command Mode

Router mode

Examples

The following example shows setting the administrative distance for all routes.

```
#configure terminal
(config)#router isis
(config-router)#distance 10
```

The following example shows setting the administrative distance for a specific route source.

```
#configure terminal
(config)#router isis
(config-router)#distance 40 0000.0000.0001
```


© 2021 IP Infusion Inc. Proprietary

distance (IPv6)

Use this command in router mode to set the administrative distance for all IPv6 routes.

Use the `no` parameter with this command to remove an administrative distance.

Command Syntax

```
distance <1-255>
no distance
```

Parameters

`<1-255>`	Distance range.

Default

By default, all options are turned off.

Command Mode

Address-family ipv6 mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows setting the administrative distance for all routes.

```
#configure terminal
(config)#router isis
(config-router)#address-family ipv6
(config-router-af)#distance 14
```

© 2021 IP Infusion Inc. Proprietary

domain-password

Use this command to set the authentication password for the Level-2 domain, and optionally, the authentication password on Level-2 sequence number PDUs.

Configuring this command to enable authentication when receiving and sending link state and sequence number PDUs in Level-2 domain. The domain password must be the same in the Level-2 domain.

Use the `no` parameter with this command to clear the domain password.

Command Syntax

```
domain-password WORD
domain-password WORD authenticate snp (send-only|validate)
no domain-password
```

Parameters

`WORD`	Password string.
`authenticate`	Inserts th password into Level-1 sequence number PDUs.
`snp`	sequence number PDUs.
`send-only`	Only inserts the password into the Level-1 sequence number PDUs, but does not check the password in sequence number PDUs that it receives. Use this keyword during a software upgrade to ease the transition.
`validate`	Inserts the password into the Level-1 sequence number PDUs and checks the password in sequence number PDUs received.

Default

By default, there is no domain password.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#domain-password mypasswd

(config)#router isis bb
(config-router)#domain-password myPass authenticate snp send-only

(config)#router isis bb
(config-router)#no domain-password
```


© 2021 IP Infusion Inc. Proprietary

dynamic-hostname

Use this command to configure the hostname to advertise for an ISIS instance using the dynamic hostname exchange mechanism (RFC 2763) and system-ID-to-hostname translation. This command configures a hostname to use for the Dynamic Hostname Exchange Mechanism and System-ID to hostname translation. This is required to get accurate results when using the show isis database and a few other commands.

Use the `no` parameter to disable the Hostname configured.

Command Syntax

```
dynamic-hostname
hostname dynamic
dynamic-hostname area-tag
no dynamic-hostname
no hostname dynamic
```

Parameters

`area-tag`	Use the routing area tag as the hostname, not the router's global hostname.

Default

By default, the Dynamic Hostname Exchange Mechanism is disabled.

Command Mode

Router mode

Example

```
#configure terminal
(config)#router isis bb
(config-router)#dynamic-hostname area-tag
```

fast-reroute per-prefix

Use this command to enable Loop Free Alternate Fast Reroute (LFA FRR) for all prefixes or only those prefixes in a route map.

Use the no form of this command to disable LFA FRR.

Command Syntax

```
fast-reroute per-prefix (level-1|level-2) proto (ipv4) (all|route-map WORD)
 no fast-reroute per-prefix (level-1|level-2) proto (ipv4)
```

Parameters

`level-1`	Level 1 only.
`level-2`	Level 2 only.
`ipv4`	IPv4 address family only.
`all`	All prefixes.
`route-map`	Prefixes from a route map.
`WORD`	Route map name.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#router isis 100
(config-router)#fast-reroute per-prefix level-2 proto ipv4 all
(config-router)#fast-reroute per-prefix level-1 proto ipv4 route-map rmap1
(config-router)#no fast-reroute per-prefix level-2 proto ipv4
```


© 2021 IP Infusion Inc. Proprietary

fast-reroute terminate-hold-on interval

Use this command to set the Loop Free Alternate Fast Reroute (LFA FRR) termination hold-on timer.

Use the no form of this command to set the termination hold-on timer to its default value (1000 milliseconds).

Command Syntax

```
fast-reroute terminate-hold-on interval <100-100000>
no fast-reroute terminate-hold-on interval
```

Parameters

<100-100000>	LFA FRR termination hold-on timer interval in milliseconds.

Default

1000 milliseconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#router isis 100
(config-router)#fast-reroute terminate-hold-on interval 7000
(config-router)#no fast-reroute terminate-hold-on interval
```

fast-reroute tie-break

Use this command to set the tie-breaking policy for selecting a fast reroute repair path. You assign a priority to each type of repair path. The tie-breaker value is used to select an LFA FRR route when multiple LFA FRR routes are available for the same primary route.

Use the `no` form of this command to set the tie-break preference value for a protection type to its default value.

To set all types of repair paths to their default priorities, do not specify a repair path with the `no` form of this command.

Command Syntax

```
fast-reroute tie-break (level-1|level-2) proto (ipv4) (primary-path|interface-
  disjoint|node-protecting|broadcast-interface-disjoint|secondary-path|downstream-
  path) index <1-255>
no fast-reroute tie-break (level-1|level-2) proto (ipv4) (primary- path|interface-
  disjoint|node-protecting|broadcast-interface-disjoint|secondary-
  path|downstream-path)
```

Parameters

`level-1` Level 1 only.

`level-2` Level 2 only.

`ipv4` IPv4 address family only.

`primary-path` Use a path from the Equal-Cost Multipath Path (ECMP) set. An ECMP found during the primary shortest path first (SPF) repair might not be desirable in networks where traffic exceeds the capacity of any single link.

`interface-disjoint`

Link protecting: prefer a backup path that uses a different interface than the interface used to reach destination via the primary path.

`node-protecting`

Bypass the `primary-path` gateway router which might not protect the router that is the next hop in the primary path. This ensures complete traffic protection even if the primary next-hop router fails.

`broadcast-interface-disjoint`

Do not use the interface if connected to a broadcast network. Repair paths protect links when a repair path and a protected primary path use *different* next-hop interfaces. However, on broadcast interfaces, if the repair path is computed via the same interface as the primary path, but their next-hop gateways are different, the router is protected but the link might not be.

`secondary-path` Prefer a non-ECMP backup path.

`downstream-path`

Prefer a backup path to the destination which satisfies the downstream condition where the path cost to reach the destination from the LFA next hop is less than the path cost to the destination from the self node via primary next hop:

Distance_opt(N, D) < Distance_opt(S, D)

This might result in lost traffic, but prevents looping.

`index` Tie breaking index. A lower value has higher preference.

© 2021 IP Infusion Inc. Proprietary

`<1-255>` Tie breaking index value.

Defaults

`primary-path`	20
`interface-disjoint`	60
`node-protecting`	30
`broadcast-interface-disjoint`	70
`secondary-path`	255
`downstream-path`	90

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#router isis 100
(config-router)#fast-reroute tie-break level-2 proto ipv4 node-protecting
index 127
(config-router)#no fast-reroute tie-break level-1 proto ipv4
broadcastinterface-disjoint
```

ignore-lsp-errors

Use this command to ignore link-state packets (LSPs) with checksum errors. By default, ISIS validates the checksum for LSP and if the checksum has an error, the LSP is dropped. Giving this command says to ignore the LSP checksum error and treat it as if checksum is passed.

Use the `no` parameter to turn off this function.

Command Syntax

```
ignore-lsp-errors
no ignore-lsp-errors
```

Parameters

None

Default

By default, the LSP checksum is checked on receipt.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In this sample, rtr1 does not drop LSP packets with bad checksum.

```
#configure terminal
(config)#router isis bb
(config-router)#ignore-lsp-errors
```


© 2021 IP Infusion Inc. Proprietary

ip router isis

Use this command to enable ISIS IPv4 routing on the interface. This command is mandatory to ISIS configuration.

After giving this command, the router sends ISIS Hello with IP address TLV on this interface and IP reachability information TLV in link-state packets are updated.

Use the `no` parameter with this command to disable ISIS IPv4 routing on the interface. This action does not clear the ISIS database. To clear the database, unconfigure the ISIS routing instance.

Command Syntax

```
ip router isis WORD
no ip router isis WORD
```

Parameters

`WORD`	Name that identifies the IS-IS area. Specify an existing area name or a new area name.

Default

By default, IPv4 routing is disabled on the router.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip router isis bb
```

ipv6 router isis

Use this command to enable ISIS IPv6 routing on the interface. This command is mandatory to IPv6 ISIS configuration. Match the ISIS instance tag to one of existing instance's tags, or a new instance with the tag name should be initiated, otherwise routing will not run on this interface.

Configuring this command, the router sends ISIS Hello with IPv6 address TLV on this interface, and IPv6 reachability information TLV in the LSP will be updated.

Use the no parameter with this command to disable ISIS IPv6 routing on the interface.

Command Syntax

```
ipv6 router isis WORD
no ipv6 router isis WORD
```

Parameters

WORD	ISIS instance name.

Default

By default, IPv6 routing is disabled on the router.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 router isis bb
```


© 2021 IP Infusion Inc. Proprietary

isis authentication key-chain

Use this command to set the key chain to be used for authentication on the interface-related packets.

Authentication mode must be set to `md5` to configure the key chain. If no key chain is configured with the `key-chain` command, no key-chain authentication is performed. Only one authentication key-chain is applied to an ISIS interface at a time. That is, issuing a second `isis authentication key-chain` command overrides the first `isis authentication key-chain` command.

If neither the `level-1` nor `level-2` keyword is configured, the key chain applies to the level(s) on which the authentication mode is configured as `md5`. Authentication can be specified for an entire instance of ISIS, instead of at the interface level, by using the `authentication key-chain` command.

Use the `no` parameter with this command to unset the key chain used for authentication on the interface-related packets.

Command Syntax

```
isis authentication key-chain WORD (level-1|level-2|)
no isis authentication key-chain (level-1|level-2|)
```

Parameters

`WORD`	Chain name - valid authentication keys.
`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

By default, this option is disabled. The key chain applies to the level(s) on which authentication mode is configured as MD5 if no level is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis authentication key-chain myKey level-1
```

isis authentication mode md5

Use this command to set the MD5 authentication mode. If the `isis password` command was used, then subsequently an attempt is made to use the `isis authentication mode` command, the attempt fails. To configure `isis authentication mode` command, first use the `no isis password` command. If the `isis authentication mode` command was used, then subsequently an attempt is made to use the `isis password` command, the attempt fails.

To configure clear text authentication using the `isis password` command, first use the `no isis authentication mode` command. The type of authentication and the level to which it applies can be specified for the entire ISIS instance, rather than per interface, using the `authentication mode` command.

Use the `no` parameter with this command to unset the MD5 authentication mode.

Command Syntax

```
isis authentication mode {md5|text} (level-1|level-2|)
no isis authentication mode {md5|text} (level-1|level-2|)
```

Parameters

`md5`	Keyed message digest
`text`	Text mode
`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

By default, this option is disabled. The authentication mode will be set to MD5 for both levels if no level is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis authentication mode md5 level-1
```


© 2021 IP Infusion Inc. Proprietary

isis authentication send-only

Use this command to set the send-only option to the interface-related packets.

Use this command before configuring the ISIS authentication mode and ISIS authentication key-chain, so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all routers that must communicate are configured with this command, enable the authentication mode and key chain on each router.

Use the `no` parameter with this command to unset the send-only option to the interface-related packets.

Command Syntax

```
isis authentication send-only (level-1-only|level-2-only|level-1-2)
no isis authentication send-only
```

Parameters

`level-1-only`	Set send-only option for level-1 only.
`level-2-only`	Set send-only option for level-2 only.
`level-1-2`	Set send-only option for level-1-2 only.

Default

By default, this option is disabled. The send-only option applies to both levels if no level is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis authentication send-only level-1-only
```

isis bfd

Use this command to enable/disable the BFD check on interface.

The `isis bfd` command allows a user to enable BFD on an interface. The `isis bfd disable` command disables BFD checking on an interface. However, the `no isis bfd` and `no isis bfd disable` commands both remove the enable/disable configuration, but do not disable/enable BFD.

The `bfd all-interfaces` command enables BFD on all interfaces attached to an instance then configuring. This command disables BFD configuration on a particular interface.

Command Syntax

```
isis bfd (disable|)
no isis bfd (disable|)
```

Parameters

`disable`	Specify to disable BFD.

Default

By default, bfd feature enable/disable is not configured.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis bfd disable
```


© 2021 IP Infusion Inc. Proprietary

isis circuit-type

Use this command to set the circuit type for the interface.

If level-1 or level-2-only is specified in this command, ISIS sends only the specified level of PDUs. On the point-to-point interface, there is only one type of Hello packet, so in this case ISIS Hello will be sent regardless of circuit-type. If is-type is configured as level-1 or level-2 only, routing for this instance is performed for only the specified level. In this manner, only the particular level of PDU is sent on the interface.

Use the `no` parameter to reset circuit type to the default.

Command Syntax

```
isis circuit-type (level-1|level-1-2|level-2-only)
no isis circuit-type
```

Parameters

`level-1`	Specify that only Level-1 adjacencies are formed.
`level-1-2`	Specify that Level-1-2 adjacencies are formed.
`level-2-only`	Specify that only Level-2 adjacencies are formed.

Default

By default, the default circuit-type is level-1-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis circuit-type level-2-only
```

© 2021 IP Infusion Inc. Proprietary

isis csnp-interval

Use this command to set CSNP (Complete sequence number PDU) interval in seconds.

Configuring this command changes the interval between two consecutive CSNP transmission. By default, CSNP is sent every 10 seconds only by LAN DIS. This parameter is only valid on broadcast interface, since periodic CSNP is only sent on broadcast interface, while CSNP on Point-to-Point interface is sent only when adjacency is initiated.

Use the `no` parameter with this command to reset CSNP interval to the default value.

Command Syntax

```
isis csnp-interval <1-65535> (level-1|level-2|)
no isis csnp-interval (level-1|level-2|)
```

Parameters

`<1-65535>`	Specify the CSNP interval in seconds.
`level-1`	Specify Level-1 CSNP.
`level-2`	Specify Level-2 CSNP.

Default

By default, ISIS uses 10 seconds for the interval and the interval is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis csnp-interval 20
```


© 2021 IP Infusion Inc. Proprietary

isis fast-reroute per-prefix candidate disable

Use this command to prevent an interface from becoming an Loop Free Alternate Fast Reroute (LFA FRR) for a primary route.

Use the no form of this command to enable an interface to become an LFA FRR for a primary route.

Command Syntax

```
isis fast-reroute per-prefix candidate disable (level-1|level-2)
no isis fast-reroute per-prefix candidate disable (level-1|level-2)
```

Parameters

`level-1`	Level-1 only
`level-2`	Level-2 only

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis fast-reroute per-prefix candidate disable level-2
(config-if)#no isis fast-reroute per-prefix candidate disable level-2
```

isis hello-interval

Use this command to set the Hello interval in seconds. The Hello-interval is set with the hello-multiplier (see `isis hello-multiplier` command).

Configuring this command changes the time interval between two consecutive Hello transmissions. If a device receives its own LSP with a maximum sequence number, then it suspends ISIS for the hold interval. DIS sends Hello transmissions at three times the rate than non-DIS. If ISIS is elected as DIS on this interface, ISIS sends Hello every 3.3 seconds.

If `minimal` keyword is specified, Holding timer in Hello PDU is set to 1 second and Hello interval is calculated by dividing by the hello-multiplier. For example, if the hello-multiplier is configured as 4 and `hello-interval minimal` is the command used, an Hello PDU is sent every 250 milliseconds.

Use the `no` parameter to set the Hello interval to the default.

Command Syntax

```
isis hello-interval <1-65535> (level-1|level-2|)
isis hello-interval minimal (level-1-only|level-2-only|level-1-2)
no isis hello-interval (level-1|level-2|)
no isis hello-interval minimal
```

Parameters

`<1-65535>`	Specify the hello interval in seconds.
`minimal`	Specify the holding-time as 1 second.
`level-1`	Specify Level-1 CSNP.
`level-2`	Specify Level-2 CSNP.
`level-1-only`	Specify only Level-1 CSNP.
`level-2-only`	Specify only Level-2 CSNP.
`level-1-2`	Specify only Level-1-2 CSNP.

Default

By default, ISIS uses 10 seconds for the interval and the interval is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#isis hello-interval 5 level-1

(config-if)#isis hello-interval minimal level-1-only
```

 © 2021 IP Infusion Inc. Proprietary

isis hello-multiplier

Use this command to set multiplier for Hello holding time.

Changes Holding Timer in Hello PDU. Holding timer is calculated by “Hello-Interval” multiplied by this value. If `minimal` keyword is specified with the Hello-Interval, the holding timer is set to 1 second and the hello-interval is calculated by dividing 1 by this value.

Use the `no` parameter with this command to set multiplier to the default.

Command Syntax

```
isis hello-multiplier <2-100> (level-1|level-2|)
no isis hello-multiplier (level-1|level-2|)
```

Parameters

`<2-100>`	Specify a hello multiplier value.
`level-1`	Specify Level-1 hello.
`level-2`	Specify Level-2 hello.

Default

By default, ISIS uses 3 seconds for the multiplier value and the multiplier is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis hello-multiplier 4
```

isis hello padding

Use this command to enable IS-IS hello padding at the interface level.

Intermediate System-to-Intermediate System (IS-IS) hellos are padded to the full maximum transmission unit (MTU) size. The benefit of padding IS-IS hellos to the full MTU is that it allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

Use the `no` parameter with this command to disable IS-IS hello padding.

Command Syntax

```
isis hello padding
```

```
no isis hello padding
```

Parameters

None

Default

By default, ISIS hello padding is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#isis hello padding

(config-if)#no isis hello padding
```


© 2021 IP Infusion Inc. Proprietary

isis lsp-interval

Use this command to set the link-state packet (LSP) transmission interval.

Giving this command changes the minimum interval between two consecutive LSP transmission. When flooding or some other event triggers LSP transmission, the LSP is put in the interface queue and scheduled to send according to this interval. Two consecutive LSP transmissions are scheduled to have at least this interval.

Use the `no` parameter with this command to set LSP transmission interval to the default.

Command Syntax

```
isis lsp-interval <1-4294967295>
no isis lsp-interval
```

Parameters

`<1-4294967295>` LSP transmission interval in milliseconds.

Default

By default, ISIS uses 33 milliseconds for the interval.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#isis lsp-interval 100

(config-if)#no isis lsp-interval
```

isis mesh-group

Use this command to set Mesh Group ID on the current interface.

Use the `no` parameter to unset mesh group on the current interface.

Command Syntax

```
isis mesh-group <1-4294967295>
no isis mesh-group
```

Parameters

`<1-4294967295>` Specify a mesh group number

Default

By default, mesh groups are not enabled on this interface.

Command Mode

Interface mode

Examples

```
(config)#interface eth0
(config-if)#isis mesh-group 20

(config)#interface eth2
(config-if)#no isis mesh-group
```


© 2021 IP Infusion Inc. Proprietary

isis metric

Use this command to set the default metric for the interface. The interface default metric is put into IP reachability information TLVs and in IS reachability information TLVs in link-state packets. The value is used for SPF calculation, and is applied when the metric-style is configured as “narrow”.

Use the `no` parameter with this command to set default metric to the default.

Command Syntax

```
isis metric <1-63> (level-1|level-2|)
no isis metric (level-1|level-2|)
```

Parameters

`<1-63>`	Default metric.
`level-1`	Default metric for level-1 circuit.
`level-2`	Default metric for level-2 circuit.

Default

By default, ISIS uses 10 for the metric value and the value is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis metric 20
```

isis network

Use this command to change a broadcast interface network type to a point-to-point network type.

Use the `no` parameter with this command to revert to the default setting of a broadcast interface network type.

Command Syntax

```
isis network (broadcast|point-to-point)
no isis network
```

Parameters

`broadcast`	Specify ISIS a broadcast multi-access network.
`point-to-point`	Specify ISIS a point-to-point network.

Default

By default, the network is set to a broadcast multi-access network type.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis network point-to-point
```


© 2021 IP Infusion Inc. Proprietary

isis password

Use this command to set the authentication password of Hello PDU on the interface.

If the `isis authentication mode` command was used, then subsequently an attempt is made to use the `isis password` command, the attempt fails. To configure clear text authentication using the `isis password` command, first use the `no isis authentication mode` command.

Use the `no` parameter to clear the password.

Command Syntax

```
isis password WORD (level-1|level-2|)
no isis password (level-1|level-2|)
```

Parameters

`WORD`	Specify a password string.
`level-1`	Specify a password for Level-1 hello PDUs.
`level-2`	Specify a password for Level-2 hello PDUs.

Default

By default, no password is configured; this applies to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis password mypassword level-1
```

isis priority

Use this command to set the priority for LAN DIS election. This command changes the priority value in LAN ISIS Hello PDUs. A lower priority value is less preferred in DIS election, and a higher priority value is more preferred.

Note: This command is not valid for Point-to-Point interface.

Use the `no` parameter to set priority to the default.

Command Syntax

```
isis priority <0-127> (level-1|level-2|)
no isis priority (level-1|level-2|)
```

Parameters

`<0-127>`	Priority value
`level-1`	Specify a password for Level-1 hello PDUs.
`level-2`	Specify a password for Level-2 hello PDUs.

Default

By default, ISIS uses 64 for the priority value, and the priority is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis priority 127
```


© 2021 IP Infusion Inc. Proprietary

isis retransmit-interval

Use this command to set the link-state packet (LSP) retransmission interval.

Use the `no` parameter to set the interval to the default.

Command Syntax

```
isis retransmit-interval <1-65535>
no isis retransmit-interval
```

Parameters

`<1-65535>`	Interval for retransmission of the same LSP in seconds.

Default

By default, ISIS uses an interval of 5 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#isis retransmit-interval 10

(config-if)#no isis retransmit-interval
```

ispf

Use this command to enable incremental SPF for a routing process.

Use the `no` parameter to disable incremental SPF from a routing process.

Command Syntax

```
ispf (level-1|level-2-only|)
no ispf
```

Parameters

`level-1`	Act as level-1 only IS.
`level-2-only`	Act as level-2 only IS.

Default

By default, all levels are turned off.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#ispf level-1

(config)#router isis bb
(config-router)#no ispf
```


© 2021 IP Infusion Inc. Proprietary

isis wait-timer

Use the isis wait-timer seconds command to configure the number of seconds the router will wait for adjacency information

Use the `no` parameter to set the wait-timer to the default.

Command Syntax

```
isis wait-timer <1-65535> (level-1|level-2|)
no isis wait-timer (level-1|level-2|)
```

Parameters

`level-1`	Act as level-1 only IS.
`level-2`	Act as level-2 only IS.

Default

By default, wait-timer will be 20 seconds (2 times the hello timer).

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#isis wait-timer 30

(config)#router isis bb
(config-router)#no isis wait-timer
```

© 2021 IP Infusion Inc. Proprietary

isis wide-metric

Use this command to set wide metric for the interface.

Interface wide-metric is put into Extended IP reachability TLVs. Extended IS reachability TLVs and IPv6 rechability TLVs in LSPs. The value is used for SPF calculation. The value is applied when metric-style is configured as 'wide'.

Use the `no` parameter to set wide metric to the default.

Command Syntax

```
isis wide-metric <1-16777214> (level-1|level-2|)
no isis wide-metric (level-1|level-2|)
```

Parameters

`<1-16777214>`	Specify a wide metric.
`level-1`	Specify the wide metric for Level-1 circuit.
`level-2`	Specify the wide metric for Level-2 circuit.

Default

By default, ISIS uses 10 for the metric value and the metric is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

None.

Examples

```
#configure terminal
(config)#interface eth0
(config-router)#isis wide-metric 100

(config)#interface eth0
(config-router)#no isis wide-metric
```


© 2021 IP Infusion Inc. Proprietary

isis tag

Use this command to sets the tag for link-state packets (LSPs) sent out advertising routes for networks directly connected to an interface.

If you do not specify a parameter, then the tag value is set for level-1-2 boundary.

Use the `no` parameter to unset the tag.

Command Syntax

```
isis tag <1-4294967295> (level-1|level-2|)
no isis tag (level-1|level-2|)
```

Parameters

`<1-4294967295>`	Tag value.
`level-1`	Specify the tag value for the level-1 boundary.
`level-2`	Specify the tag value for the level-2 boundary.

Command Mode

Interface mode

Examples

```
>ena
#con term
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#interface eth0
(config-if)#isis tag 500 level-1
```

isis te-metric

Use this command to set Traffic Engineering (TE) metric for the interface. Interface te-metric is put into Extended IS reachability TLV. The value is used for CSPF calculation. The value is applied when metric-style is configured as wide.

Use the `no` parameter to unset the Traffic Engineering metric.

Command Syntax

```
isis te-metric <1-16777214> (level-1|level-2|)
no isis te-metric (level-1|level-2|)
```

Parameters

`<1-16777214>`	Specify a TE metric.
`level-1`	Specify the TE metric for level-1 circuit.
`level-2`	Specify the TE metric for level-2 circuit.

Default

By default, it will take ISIS wide metric value.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-DC version 5.0

Examples

```
#configure terminal
(config)#interface eth1
(config-router)#isis te-metric 100
(config)#interface eth1
(config-router)#no isis te-metric
```


© 2021 IP Infusion Inc. Proprietary

is-type

Use this command to set the IS to the specified level of routing.

Changing `is-type` brings down, then brings up a particular level of routing. There is a limitation: Only one ISIS instance can run Level-2 routing (either Level-2 only IS, or Level-1-2 IS).

Use the `no` parameter to set the IS to the default.

Command Syntax

```
is-type (level-1|level-1-2|level-2-only)
no is-type
```

Parameters

`level-1`	Act as level-1 only IS.
`level-1-2`	Act as level-1-2 IS.
`level-2-only`	Act as level-2 only IS.

Default

By default, ISIS uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#is-type level-1

(config)#router isis bb
(config-router)#no is-type
```

key chain

Use this command to enter the key chain management mode and to configure a key chain with a key chain name. This command allows you to enter the keychain mode to specify keys on this key chain.

Command Syntax

```
key chain WORD
no key chain WORD
```

Parameters

WORD	Specify the name of the key chain to manage.

Default

By default, keychain mode is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the creation of a key chain named `mychain` and the change to keychain mode:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#
```


© 2021 IP Infusion Inc. Proprietary

key

Use this command to manage, add or delete authentication keys in a key-chain. This command allows you to enter the keychain-key mode to set a password for the key.

Command Syntax

```
key <0-2147483647>
no key <0-2147483647>
```

Parameters

`<0-2147483647>` Specify a key identifier.

Default

By default, ISIS uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Command Mode

Keychain mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures a key number 1 and shows the change to keychain-key command mode.

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#
```

key-string

Use this command to define a password in plain-text to be used by a key.

The password is stored as encrypted, and is displayed in encrypted text when show running-config command is executed.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
key-string WORD
no key-string
```

Parameters

`WORD`	Specify a string of characters to be used as a password by the key. The length of the string should be between 1-80 characters.

Default

By default, password is not configured.

Command Mode

Keychain mode and Keychain-key mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, the password for `key 1` in the key chain named `mychain` is set to `prime`:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#key-string prime

(config-keychain)#key 1
(config-keychain-key)#no key-string
```


© 2021 IP Infusion Inc. Proprietary

key-string encrypted

Use this command to define a password in its encrypted format to be used by a key.

Use the `no` parameter with this command to disable this feature

Command Syntax

```
key-string encrypted WORD
no key-string encrypted
```

Parameters

`WORD`	Specify the encrypted string of characters to be used as a passoword by the key. The length of this string should be between 18-162 characters.

Default

By default, password is not configured.

Command Mode

Keychain mode and Keychain-key mode.

Applicability

This command was introduced in OcNOS version 4.1.

Examples:

In the following example, the encrypted password for key 1 in the key chain named mykeychain is set to 0xd6c50b442de47f70 (equivalent to "mychain" in plain-text):

```
#configure terminal
(config)#key chain mykeychain
(config-keychain)#key 1
(config-keychain-key)#key-string encrypted 0xd6c50b442de47f70
(config-keychain)#key 1
(config-keychain-key)#no key-string
```

© 2021 IP Infusion Inc. Proprietary

lsp-gen-interval

Use this command to set the minimum interval before regenerating the same link-state packet (LSP). The smaller the interval, the faster the convergence. However, this setting might cause more frequent flooding.

Use the `no` parameter with this command to set the interval to the default.

Command Syntax

```
lsp-gen-interval <1-120>
lsp-gen-interval (level-1|level-2) <1-120>
no lsp-gen-interval (level-1|level-2|)
```

Parameters

`<1-120>`	Minimum interval in seconds.
`level-1`	Interval for Level-1 IS.
`level-2`	Interval for Level-2 IS.

Default

By default, ISIS uses 30 seconds for the interval and the interval is applied to both level-1 and level-2.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router isis bb
(config-router)#lsp-gen-interval 5
```


© 2021 IP Infusion Inc. Proprietary

lsp-mtu

Use this command to set maximum transfer unit for link-state packets (LSPs).

Use the `no` parameter with this command to set the interval to the default.

Command Syntax

```
lsp-mtu (level-1|level-2|) <512-1492>
no lsp-mtu (level-1|level-2|)
```

Parameters

`<512-1492>`	MTU size
`level-1`	Size for Level-1 IS.
`level-2`	Size for Level-2 IS.

Default

By default, the MTU is 1492 bytes.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router isis bb
(config-router)#lsp-mtu 555
```

© 2021 IP Infusion Inc. Proprietary

lsp-refresh-interval

Use this command to set the link-state packet (LSP) refresh interval.

IP Infusion Inc. recommends making the `lsp-refresh-interval` smaller than the max-lsp-lifetime value.

Use the `no` parameter to set the interval to the default value.

Command Syntax

```
lsp-refresh-interval <1-65535>
no lsp-refresh-interval
```

Parameters

`<1-65535>`	Refresh interval in seconds.

Default

By default, the interval is 900 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#lsp-refresh-interval 600

(config)#router isis bb
(config-router)#no lsp-refresh-interval
```


© 2021 IP Infusion Inc. Proprietary

max-area-address

Use this command to set the maximum number of ISIS areas that can be configured on this router with the `net` command. By default, ISIS permits a maximum of three areas that can be defined on a router.

Use the `no` parameter with this command to set the maximum number of ISIS areas to its default (3).

Command Syntax

```
max-area-address <3-254>
no max-area-address
```

Parameters

`<3-254>`	The maximum number of areas in the network.

Default

By default, the maximum number of areas is 3.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router isis net2
(config-router)#max-area-address 5
(config-router)#net 71.0001.0000.0000.0001.00
(config-router)#net 72.0001.0000.0000.0001.00
(config-router)#net 73.0001.0000.0000.0001.00
(config-router)#net 74.0001.0000.0000.0001.00
(config-router)#net 75.0001.0000.0000.0001.00
```

© 2021 IP Infusion Inc. Proprietary

max-lsp-lifetime

Use this command to set the maximum link-state packet (LSP) lifetime. You must set `max-lsp-lifetime` greater than the lsp-refresh-interval interval.

Use the `no` parameter to set the lifetime to the default.

Command Syntax

```
max-lsp-lifetime <350-65535>
no max-lsp-lifetime
```

Parameters

`<350-65535>`	Maximum LSP lifetime in seconds.

Default

By default, max-lsp-lifetime is set to 1200 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#max-lsp-lifetime 1500

(config)#router isis bb
(config-router)#no max-lsp-lifetime
```


© 2021 IP Infusion Inc. Proprietary

metric-style

Use this command to configure the ISIS metric style. Use the following table when changing the method of how TLV encodes and SPF calculates a decision:

Metric-style Command	Wide SPF	Wide TLV	Narrow SPF	Narrow TLV
narrow (default)	OFF	OFF	ON	OFF
narrow transition	ON	OFF	ON	ON
wide	ON	ON	OFF	OFF
wide transition	ON	ON	ON	OFF
transition	ON	ON	ON	ON

Where:

- Wide SPF: Uses wide TLVs for SPF calculation.
- Wide TLV: Encodes wide TLVs in the LSP.
- Narrow SPF: Uses narrow TLVs for SPF calculation.
- Narrow TLV: Encodes narrow TLVs in the LSP.

Use the `no` parameter to set the style to the default style, narrow.

Command Syntax

```
metric-style (narrow|wide|transition) (level-1|level-2|)
metric-style (narrow|wide) transition (level-1|level-2|)
no metric-style
```

Parameters

`narrow`	Specify the old style of TLVs with narrow metric.
`wide`	Specify the new style of TLVs to carry wider metric.
`transition`	Specify to send and accept both styles of TLVs during transition.
`level-1`	Specify the level-1 metric style.
`level-2`	Specify the level-2 metric style.
`transition`	Accept both styles of TLVs during transition

Default

By default, ISIS uses narrow metric style for level 1 and 2.

Command Mode

Router mode

Examples

```
(config)#router isis bb
(config-router)#metric-style narrow transition
```


© 2021 IP Infusion Inc. Proprietary

mpls traffic-eng

Use this command to configure MPLS Traffic Engineering feature for ISIS.

Use the `no` parameter to turn off the feature.

Note: Metric-style wide must be enabled before using this CLI.

Command Syntax

```
mpls traffic-eng (level-1|level-2)
no mpls traffic-eng (level-1|level-2)
```

Parameters

`level-1`	Specify the level-1 MPLS Traffic Engineering feature.
`level-2`	Specify the level-2 MPLS Traffic Engineering feature.

Default

If this command is not used, ISIS does not encode traffic engineering TLVs and Sub-TLVs.

Command Mode

Router mode

Examples

```
(config)#router isis bb
(config-router)#metric-style wide
(config-router)#mpls traffic-eng level-1

(config)#router isis bb
(config-router)#no mpls traffic-eng level-1
```

© 2021 IP Infusion Inc. Proprietary

mpls traffic-eng router-id

Use this command to configure the traffic engineering stable IP address for a system.

Use the `no` parameter to turn off the feature.

Command Syntax

```
mpls traffic-eng router-id A.B.C.D
no mpls traffic-eng router-id
```

Parameters

`A.B.C.D`	Specify the ISIS router-ID in an IP address format.

Default

If this command is not used, and traffic engineering is enabled, ISIS will use global router-id..

Command Mode

Router mode

Examples

```
(config)#router isis bb
(config-router)#mpls traffic-eng router-id 10.10.0.23

(config)#router isis bb
(config-router)#no mpls traffic-eng router-id
```


© 2021 IP Infusion Inc. Proprietary

net

Use this command to add a Network Entity Title (NET) for the instance.

On a router running ISIS, a NET can be 8 to 20 bytes in length. The last byte is always the n-selector, and must be zero. The n-selector indicates no transport entity, and means that the packet is for the routing software of the system. The six bytes directly preceding the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2).

The bytes preceding the system ID are the area ID, which can be from 1 - 13 bytes in length. By default, a maximum of three NETs per router are allowed with a different area ID but the system ID should be the same for all NETs. You can increase the number of area IDs per system ID with the `max-area-address` command.

Use the `no` parameter to remove the NET.

Command Syntax

```
net NET
no net NET
```

Parameters

`NET`	Specify a network entity title (NET) in 1 to 13 octets (that is, XX.XXXX. ... .XXXX.XX).

Default

By default, ISIS does not configure a NET and routing is not enabled for the interface.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router isis bb
(config-router)#net 49.0000.0001.0002.0003.00
```

passive-interface

Use this command to suppress routing updates on all interfaces or on a specified interface, which puts the interfaces into passive mode.

To advertise passive prefixes in LSP, an interface must be configured with ip router isis when using "passive-interface" command. If interface is not configured with isis instance "passive-interface IFNAME" command must be used to add that interface as passive. Enabling passive interface on an ISIS enabled interface disables ISIS routing updates on the interface and makes the interface passive.

Use the `no` parameter with this command to remove interfaces from passive mode

Note: The command `passive-interface IFNAME disable` is used to make a particular interface active after the `passive-interface` command (with no parameters) has set all interfaces as passive.

Command Syntax

```
passive-interface
passive-interface IFNAME
passive-interface IFNAME disable


no passive-interface
no passive-interface IFNAME
no passive-interface IFNAME disable
```

Parameters

`IFNAME`	Interface name. If this parameter is omitted, then all interfaces become passive or active.
`disable`	Disable passive interface.

Command Mode

Router mode

Examples

The following suppresses routing updates on a specified interface.

```
#configure terminal
(config)#router isis 100
(config-router)#passive-interface
(config-router)#passive-interface eth0 disable
```


© 2021 IP Infusion Inc. Proprietary

prc-interval-exp

Use this command to configure exponential back-off delay between PRC calculations.

Use the `no` parameter to disable any set exponential back-off delay between PRC calculations.

Command Syntax

```
prc-interval-exp
prc-interval-exp <0-2147483647> <0-2147483647>
no prc-interval-exp
```

Parameters

`<0-2147483647>`	Set the minimum delay between receiving a change to PRC calculation in milliseconds.
`<0-2147483647>`	Set the maximum delay between receiving a change to PRC calculation in milliseconds.

Default

By default, minimum delay is 500 milliseconds and maximum delay is 50 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#router isis
(config-router)#prc-interval-exp 100 10000

(config)#router isis
(config-router)#no prc-interval-exp
```

redistribute

Use this command to redistribute routes from another protocol into the ISIS routing table.

Use the `no` parameter to disable this function.

Command Syntax

```
redistribute (kernel|connected|static|rip|ospf|bgp) {metric <0-16777215>| metric-
  type (internal|external)|level-1|level-2|level-1-2|route-map WORD}
no redistribute (kernel|connected|static|rip|ospf|bgp)  {metric <0-16777215>|
  metric-type (internal|external)|level-1|level-2|level-1-2|route-map WORD}
```

Parameters

`kernel`	Redistribute kernel routes.
`connected`	Redistribute connected routes.
`static`	Redistribute static routes.
`rip`	Redistribute RIP routes.
`ospf`	Redistribute OSPF routes.
`bgp`	Redistribute BGP routes.
`metric`	Specify the metric for redistributed routes.
`<0-16777215>`	Specify the IS-IS default metric.
`metric-type`	Specify the IS-IS exterior metric type for redistributed routes:
`internal`	Set IS-IS internal metric type.
`external`	Set IS-IS external metric type.
`level-1`	Redistribute routes into level 1 only
`level-2`	Redistribute routes into level 2 only (default)
`level-1-2`	Redistribute routes into both levels.
`route-map`	Specify a Route map reference.
`WORD`	Specify name of the route-map.

Default

By default, redistribute command is disabled.

If no level parameter is specified, by default redistributed routes will be added in level-2 LSP. If is-type of an IS-IS instance is level-1, the level parameter must be set to level-1 for redistribute command to take effect and redistribute routes in L1 LSP.

Command Mode

For Ipv4: Router mode

For Ipv6: address-family ipv6 mode

© 2021 IP Infusion Inc. Proprietary

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>ena
#con term
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#router isis A
(config-router)#redistribute bgp metric 12
```

redistribute isis

Use this command to redistribute reachability information from one level to the other level. If an distribute-list name is given with this command for an access list that does not exist, the routes are still redistributed.

Use the `no` parameter with this command to stop redistribution.

Command Syntax

```
redistribute isis level-1 into level-2
redistribute isis level-2 into level-1
redistribute isis level-1 into level-2 distribute-list WORD
redistribute isis level-2 into level-1 distribute-list WORD
no redistribute isis level-1 into level-2
no redistribute isis level-2 into level-1
```

Parameters

`level-1`	Specify an inter-area route from level-1.
`level-2`	Specify an inter-area routes from level-2.
`into`	Specify a level from level-n into level-m.
`level-1`	Specify an inter-area route into level-1.
`level-2`	Specify an inter-area routes into level-2.
`distribute-list`	Indicate the distributed-list parameter.
`WORD`	Specify the actual selected route.

Default

By default, ISIS redistributes selected L1 routes into L2.

Command Mode

For Ipv4: Router mode

For Ipv6: address-family ipv6 mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#redistribute isis level-2 into level-1

(config)#router isis bb
(config-router)#redistribute isis level-2 into level-1 distribute-list new

(config)#router isis bb
(config-router)#no redistribute isis level-2 into level-1
```


© 2021 IP Infusion Inc. Proprietary

redistribute isis WORD

Use this command to redistribute reachability information from one isis instance into another instance. Only one isis instance can be redistributed.

Use the `no` parameter with this command to stop redistribution.

Note: This command is not supported for address family IPv6.

Command Syntax

```
redistribute isis WORD {metric <0-16777215>| metric-type (internal|external)
  |level-1|level-2|level-1-2|route-map WORD}
```

```
no redistribute isis WORD {metric <0-16777215>| metric-type
  (internal|external)|level-1|level-2|level-1-2|route-map WORD}
```

Parameters

`WORD`	Specify an isis instance name or tag
`metric`	Specify the metric for redistributed routes.
`<0-16777215>`	Specify the IS-IS default metric.
`metric-type`	Specify the IS-IS exterior metric type for redistributed routes:
`internal`	Set IS-IS internal metric type.
`external`	Set IS-IS external metric type.
`level-1`	IS-IS Level-1 routes.
`level-2`	IS-IS Level-2 routes.
`level-1-2`	IS-IS Level-1 and Level-2 routes.
`route-map`	Specify a Route map reference.
`WORD`	Specify name of the route-map.

Default

By default, redistribute command is disabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>ena
#con term
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#router isis A
(config-router)#redistribute isis B metric 12
```

router isis

Use this command to initiate an ISIS routing instance. This command starts the ISIS routing instance and enters router configuration mode. Configure at least one NET to start routing. Also, enable a particular interface with the ip router isis command.

Use the `no` parameter with this command to remove an ISIS routing instance.

Command Syntax

```
router isis WORD
no router isis WORD
```

Parameters

`WORD`	Name that specifies an ISO routing instance tag.

Default

By default, ISIS routing instance is not configured.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router isis New
(config-router)#
```


© 2021 IP Infusion Inc. Proprietary

send-lifetime

Use this command to specify the time period during which the authentication key on a key chain can be sent.

Use the `no` parameter with this command to negate this command.

Command Syntax

```
send-lifetime HH:MM:SS MONTH <01-31> <1993-2035> HH:MM:SS MONTH <01-31> <1993-2035>
send-lifetime HH:MM:SS MONTH <01-31> <1993-2035> infinite
send-lifetime HH:MM:SS MONTH <01-31> <1993-2035> duration <1-2147483646>
no send-lifetime
```

Parameters

`HH:MM:SS`	Specify the start time of send-lifetime in hours, minutes and seconds.
`<01-31>`	Specify the day of the month to start. If the day is a single-digit, the leading 0 must be added, example: 01, 02, 03, etc.
`MONTH`	Specify the month of the year to start as the first three letters of the month with first letter in caps, for example, Jan. (case sensitive)
`<1993-2035>`	Specify the year to start.
`HH:MM:SS`	Specify the end time of send-lifetime in hours, minutes and seconds.
`<01-31>`	Specify the day of the month to end. If the day is a single-digit, the leading 0 must be added, example: 01, 02, 03, etc.
`MONTH`	Specify the month of the year to end as the first three letters of the month with first letter in caps, for example, Jan. (case sensitive)
`<1993-2035>`	Specify the year to end.
`duration`	Indicate the duration parameter.
`<1-2147483646>`	Specify the actual end time duration of a key in seconds.
`infinite`	Specify the end time to never expire.

Applicability

No default value is specified

Command Mode

Keychain-key mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the setting of `send-lifetime` for `key 1` on the key chain named `mychain`:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
```

```
(config-keychain-key)#send-lifetime 03:03:01 Jan 03 2004 04:04:02 Dec 06 2006
```


© 2021 IP Infusion Inc. Proprietary

snmp restart isis

Use this command to restart SNMP in Intermediate System to Intermediate System (IS-IS)

Command Syntax

```
snmp restart isis
```

Parameters

None

Default

By default, snmp restart is not configured.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart isis
```

spf-interval-exp

Use this command to set the minimum and maximum hold intervals between Shortest Path First (SPF) calculations.

The `spf-interval-exp` command configures the minimum and maximum interval time between the receipt of a topology change and the calculation of the SPF.

Use the `no` parameter with this command to set the minimum and maximum hold intervals to the default.

Command Syntax

```
spf-interval-exp <0-2147483647> <0-2147483647>
spf-interval-exp (level-1|level-2) <0-2147483647> <0-2147483647>
no spf-interval-exp ((level-1|level-2)|)
```

Parameters

`<0-2147483647>`	Specify the minimum delay between receiving a change to the SPF calculation in milliseconds. The default SPF minimum hold-time interval value is 500 milliseconds.
`<0-2147483647>`	Specify the maximum delay between receiving a change to the SPF calculation in milliseconds. The default SPF maximum hold-time interval value is 50 seconds.
`level-1`	Specify an interval for Level-1 IS.
`level-2`	Specify an interval for Level-2 IS.

Default

By default, ISIS uses 500 milliseconds and 50,000 milliseconds for the minimum and maximum hold intervals, respectively. The values are applied to both level-1 and level-2 if the `level` parameter is omitted.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#spf-interval-exp level-1 600 60000

(config)#router isis bb
(config-router)#no spf-interval-exp level-1
```


© 2021 IP Infusion Inc. Proprietary

summary-address

Use this command to configure Summary Address to summarize IPv4 reachability information.

Use the `no` parameter with this command to unconfigure the summary.

Command Syntax

```
summary-address A.B.C.D/M (level-1 |level-1-2 |level-2) (metric <1-63>|)
no summary-address A.B.C.D/M
```

Parameters

`A.B.C.D/M`	Specify the IPv4 prefix to be announced.
`level-1`	Specify the reachability information only for Level-1.
`level-1-2`	Specify the reachability information for both Level-1 and Level-2.
`level-2`	Specify the reachability information only for Level-2.
`metric`	Specify the metric for the summarized address.
`<1-63>`	Specify the metric. The default is 0.

Default

By default, ISIS does not configure the summary-address. Level must be configured along with summary-address. Metric is optional.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#summary-address 10.10.0.0/16 level-1-2 metric 3

(config)#router isis bb
(config-router)#no summary-address 10.10.0.0/16
```

summary-prefix

Use this command to configure Summary Prefix to summarize IPv6 reachability information.

Use the `no` parameter with this command to unconfigure the summary.

Command Syntax

```
summary-prefix X:X::X:X/M (level-1 |level-1-2 |level-2) (metric <1-63>|)
no summary-prefix X:X::X:X/M
```

Parameters

`X:X::X:X/M`	Specify the IPv6 prefix to be announced.
`level-1`	Specify the reachability information only for Level-1.
`level-1-2`	Specify the reachability information for both Level-1 and Level-2.
`level-2`	Specify the reachability information only for Level-2.
`metric`	Specify the metric for the summarized address.
`<1-63>`	Specify the metric. The default is 0.

Default

By default, ISIS does not configure the summary-prefix. Level must be configured along with summary-prefix. Metric is optional.

Command Mode

Address Family IPv6 mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router isis 1
(config-router)#address-family ipv6
(config-router-af)#summary-prefix 2356::1/64 level-1 metric 30
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 IS-IS Graceful Restart Commands

This chapter describes the IS-IS graceful restart commands:

- capability restart graceful
- isis restart grace-period
- isis restart-hello-interval
- isis restart helper
- isis restart suppress-adjacency
- restart isis graceful
- restart-timer

capability restart graceful

Use this command to enable the graceful restart capability.

Use the `no` parameter with this command to negate this command.

Command Syntax

```
capability restart graceful
no capability restart graceful
```

Parameters

NA

Default

By default, graceful restart capability is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example enables the graceful restart capability on a router.

```
#configure terminal
(config)#router isis bb
(config-router)#capability restart graceful
```


© 2021 IP Infusion Inc. Proprietary

isis restart grace-period

Use this command to configure the T3 timer, the time the restarting router retains the forwarding table.

Use the `no` parameter to use the default value.

Command Syntax

```
isis restart grace-period <1-65535>
no isis restart grace-period
```

Parameters

`<1-65535>`	Grace period in seconds.

Default

By default, ISIS uses 65535 for the period value, and the value is applied to both level-1 and level-2.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example enables and then disables a restart grace period at one second.

```
#configure terminal
(config)#isis restart grace-period 1

(config)#no isis restart grace-period
```

isis restart-hello-interval

Use this command to configure the T1 timer, interval of ISIS Hello packet with restart TLV.

Use the `no` parameter to use the default value.

Command Syntax

```
isis restart-hello-interval <1-65535> (level-1|level-2|)
no isis restart-hello-interval (level-1|level-2|)
```

Parameters

`<1-65535>`	Specify the number of seconds in the interval.
`level-1`	Specify the hello-interval for level-1 IIHs.
`level-2`	Specify the hello-interval for level-1 IIHs.

Default

By default, ISIS uses 3 seconds for the hello value, and the interval is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example enables and then disables a restart hello interval at 123 seconds for a level 1 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#isis restart-hello-interval 123 level-1

(config-if)#no isis restart-hello-interval level-1
```


© 2021 IP Infusion Inc. Proprietary

isis restart helper

Use this command to configure the router's helper mode capability.

Use the `no` parameter to disable the helper mode for this router.

Command Syntax

```
isis restart helper
no isis restart helper
```

Parameters

None

Default

By default, most routers are not a restart helper router.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example enables and then disables ISIS restart helper.

```
#configure terminal
(config)#isis restart helper

(config)#no isis restart helper
```

isis restart suppress-adjacency

Use this command to enable ISIS to request that its adjacency be suppressed after the ISIS daemon process starts or restarts until the Link State Packet Database (LSPDB) synchronizes.

Use the `no` parameter to disable suppress-adjacency.

Command Syntax

```
isis restart suppress-adjacency
no isis restart suppress-adjacency
```

Parameters

None

Default

By default, ISIS does not request that its adjacency be suppressed after the ISIS daemon process starts or restarts.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example enables and then disables ISIS restart suppress adjacency.

```
#configure terminal
(config)#isis restart suppress-adjacency

(config)#no isis restart suppress-adjacency
```


© 2021 IP Infusion Inc. Proprietary

restart isis graceful

Use this command to restart the ISIS router.

Command Syntax

```
restart isis graceful (grace-period <1-65535>|)
```

Parameters

<1-65535>	Grace period in seconds.

Default

By default, the ISIS router is not restarted gracefully. Default grace-period is 65535 seconds.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#restart isis graceful grace-period 60
```

restart-timer

Use this command to restart the ISIS T2 timer. When a node comes up after graceful restart, within this time, the LSPDB sync should be completed.

Use the `no` parameter with this command to negate this command.

Command Syntax

```
restart-timer <5-65535> (level-1|level-2|)
no restart-timer (level-1|level-2|)
```

Parameters

`<5-65535>`	Restart time in seconds
`level-1`	Restart is only for Level-1.
`level-2`	Restart is only for Level-2.

Default

The default value is 60 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example enables and then disables the restart timer at 555 seconds for a level 2 interface.

```
#configure terminal
(config)#router isis bb
(config-router)#restart-timer 555 level-2

(config)#router isis bb
(config-router)#no restart-timer level-2
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 IS-IS Show Commands

This chapter provides describes the IS-IS show commands:

- show clns is-neighbors
- show clns neighbors
- show cspf rsvp forwarding-timer
- show debugging isis
- show ip isis igp-shortcut-lsp
- show ip isis route
- show ip isis route igp-shortcut
- show ip protocols
- show ip route fast-reroute
- show ip isis route fast-reroute
- show ip isis lfa-config
- show isis counter
- show isis database
- show isis interface
- show isis spf-logs
- show isis topology
- show running-config interface isis
- show running-config router isis

show clns is-neighbors

Use this command to display IS neighbor adjacencies.

Command Syntax

```
show clns is-neighbors (detail|)
show clns WORD is-neighbors (detail|)
show clns is-neighbors IFNAME (detail|)
show clns WORD is-neighbors IFNAME (detail|)
```

Parameters

`detail`	Detailed information.
`WORD`	Information for a single IS-IS area.
`IFNAME`	Information for a single interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show clns is-neighbors detail
Tag abc: VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0003 eth1        Up     L1   64        0000.0000.0003.01
L1 Adjacency ID: 1
L2 Adjacency ID: 2
Uptime: 00:12:31
Area Address(es): 52
IP Address(es): 11.11.11.2
Level-1 Protocols Supported: IPv4
Adjacency advertisement: Advertise
#
```

Table 3-173 explains the fields in the output.

Table 3-173: show clns is-neighbors output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
System Id	Uniquely identifies a system within an area.
Interface	Interface from which the system was learned.

© 2021 IP Infusion Inc. Proprietary

Table 3-173: show clns is-neighbors output (Continued)

Field	Description
State	Adjacency state: Init: Router is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent. Up: IS is considered reachable
Type	Type of adjacency: L1: Router adjacency for level 1 routing only L2: Router adjacency for level 2 only L1L2: Router adjacency for level 1 and level 2 routing
Priority	IS-IS priority that the respective neighbor is advertising. The highest priority neighbor is elected the designated IS-IS router for the interface.
Circuit Id	Number that the router uses to uniquely identify its IS-IS interface. When the interface is attached to a broadcast network, the Circuit ID is concatenated with System ID of the designated router for the interface.
Adjacency ID	Adjacency identifier.
Uptime	How long the adjacency has existed.
Area Addresses	Area addresses associated with the intermediate-system adjacencies.
IPv4/IPv6 address(es)	IP addresses of the ES or IS.
Protocols Supported	IPv4 and/or IPv6.
Adjacency advertisement	Restart: Suppress or Advertise.

show clns neighbors

Use this command to display ES and IS neighbor adjacencies.

Command Syntax

```
show clns neighbors (detail|)
show clns WORD neighbors (detail|)
show clns neighbors IFNAME (detail|)
show clns WORD neighbors IFNAME (detail|)
```

Parameters

`detail`	Detailed information for all interfaces.
`WORD`	Information for a single IS-IS area.
`IFNAME`	Information for a single interface.

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show clns neighbors detail

Tag abc: VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0003 eth1        0800.277b.411d  Up     6         L1   IS-IS
L1 Adjacency ID: 1
L2 Adjacency ID: 2
Uptime: 00:15:58
Area Address(es): 52
IP Address(es): 11.11.11.2
Level-1 Protocols Supported: IPv4
Adjacency advertisement: Advertise
#
```

Table 3-174 explains the fields in the output.

Table 3-174: show clns neighbors output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
System Id	Uniquely identifies a system within an area.
Interface	Interface from which the system was learned.

© 2021 IP Infusion Inc. Proprietary

Table 3-174: show clns neighbors output (Continued)

Field	Description
SNPA	SubNetwork Point of Attachment (SNPA): MAC address of the next-hop.
State	Adjacency state: Init: Router is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent. Up: ES or IS is considered reachable
Holdtime	Number of seconds before this adjacency entry times out.
Type	Type of adjacency: L1: Router adjacency for level 1 routing only L2: Router adjacency for level 2 only L1L2: Router adjacency for level 1 and level 2 routing
Protocol	Protocol through which the adjacency was learned.
Adjacency ID	Adjacency identifier.
Uptime	How long the adjacency has existed.
Area Addresses	Area addresses associated with the intermediate-system adjacencies.
IPv4/IPv6 address(es)	IP addresses of the ES or IS.
Topology	IPv4 and/or IPv6.
Protocols Supported	IPv4 and/or IPv6.
Adjacency advertisement	Restart: Suppress or Advertise.

show cspf rsvp forwarding-timer

This command displays the information of Graceful Restart capable RSVP client to ISIS or OSPF, CSPF that are currently shutdown.

Command Syntax

```
show cspf rsvp forwarding-timer
```

Parameters

None

Command Mode

Privileged Exec modes

Applicability

This command was introduced before OcNOS-SP version 5.0.

Example

```
OcNOS#sh cspf rsvp forwarding-timer
CSPF Server Protocol-Name GR-State Time Remaining (sec) Disconnected-time
ISIS RSVP ACTIVE 88 2021/08/18 04:49:23
OcNOS#
```


© 2021 IP Infusion Inc. Proprietary

show debugging isis

Use this command to display the status of the debugging of the ISIS system.

Command Syntax

```
show debugging isis
```

Parameters

None

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging isis
IS-IS debugging status:
IS-IS Interface FSM debugging is on
IS-IS Neighbor FSM debugging is on
IS-IS events debugging is on
IS-IS PDU debugging is on
IS-IS lsp debugging is on
IS-IS spf debugging is on
IS-IS NSM debugging is on
IS-IS Check-sum debugging is on
IS-IS Authentication debugging is on
IS-IS Protocol-error debugging is on
IS-IS Local Updates debugging is on
IS-IS Hello debugging is on
IS-IS BFD debugging is on
IS-IS MPLS debugging is on
IS-IS RIB debugging is on
#
```

© 2021 IP Infusion Inc. Proprietary

show ip isis igp-shortcut-lsp

Use this command to display IS-IS shortcut MPLS label-switched paths (LSPs).

Command Syntax

```
show ip isis (WORD|) igp-shortcut-lsp
```

Parameters

WORD	Information for a single IS-IS area.

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip isis igp-shortcut-lsp
#
```

Table 3-175 explains the fields in the output.

Table 3-175: show ip isis igp-shortcut-lsp output

Field	Description
Tunnel-endpoint	Tunnel endpoint address.
Tunnel-id	Tunnel identifier.
Tunnel-metric	Tunnel metric.
active/inactive	Whether the tunnel is active or inactive.

© 2021 IP Infusion Inc. Proprietary

show ip isis route

Use this command to display IS-IS routing table for IPv4.

Command Syntax

```
show ip isis (WORD|) route
```

Parameters

WORD	Information for a single IS-IS area.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip isis route
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
Tag xyz: VRF : default
          Destination         Metric      Next-Hop            Interface       Tag
L1        10.10.10.0/24       20          11.11.11.1          eth1            0
C         11.11.11.0/24       10          -                   eth1            0
#
```

Header

Each entry in this table has a code preceding it, indicating the source of the routing entry. Table 3-176 shows these codes.

Table 3-176 explains the fields in the output.

Table 3-176: route codes and modifiers

Code	Description
C	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from other routing protocols.
E	External.
L1	IS-IS level-1.
L2	IS-IS level-2.
ia	IS-IS inter area (leaked).

Table 3-176: route codes and modifiers (Continued)

Code	Description
D	Discard route. A device performing summarization installs a discard route in its routing table for the summarized network range to prevent routing loops where portions of the summarized network range do not have a more specific route in the RIB. External and internal discard route entries are installed by default. During route summarization, routing loops can happen if data sent to a nonexisting network appears to be a part of the summary, and the router doing the summarization has a less specific route that points back to the sending router for the network.
e	External metric. Routes can be redistributed into IS-IS with either internal or external metrics (internal is the default). The metric type determines the base metric value of the redistributed routes. The value of an internal metric is lower than 64. The value of an external metric is 64-128.

Route Entry Fields

Table 3-177 shows the route entry fields.

Table 3-177: route entry fields

Field	Description
Code	As explained in Table 3-176.
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
Destination	IP address of the remote network.
Metric	ISIS metric used for SPF calculation (1-63). When a route is imported into the IS-IS network without a specified metric, IS-IS uses 10 for the metric value and the value is applied to both level-1 and level-2.
Next-Hop	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Interface	Interface used to get to the next-hop address for this route.
Tag	Name that identifies the IS-IS area.

© 2021 IP Infusion Inc. Proprietary

show ip isis route igp-shortcut

Use this command to display the IS-IS IGP shortcut routing table.

Command Syntax

```
show ip isis (WORD|) route igp-shortcut
```

Parameters

WORD	Information for an IS-IS area.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip isis new_isis route igp-shortcut
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, D - discard, e - external metric

Tag aa: VRF : default
     Destination         Metric      Tunnel-ID         Tunnel-End-Point
#
```

Header

Each entry in this table has a code preceding it, indicating the source of the routing entry. Table 3-178 shows these codes.

Table 3-178: Route codes and modifiers

Code	Description
C	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from other routing protocols.
E	External.
L1	IS-IS level-1.
L2	IS-IS level-2.
ia	IS-IS inter area (leaked).

Table 3-178: Route codes and modifiers (Continued)

Code	Description
D	Discard route. A device performing summarization installs a discard route in its routing table for the summarized network range to prevent routing loops where portions of the summarized network range do not have a more specific route in the RIB. External and internal discard route entries are installed by default. During route summarization, routing loops can happen if data sent to a nonexisting network appears to be a part of the summary, and the router doing the summarization has a less specific route that points back to the sending router for the network.
e	External metric. Routes can be redistributed into IS-IS with either internal or external metrics (internal is the default). The metric type determines the base metric value of the redistributed routes. The value of an internal metric is lower than 64. The value of an external metric is 64-128.

Route Entry Fields

Table 3-179 shows the route entry fields.

Table 3-179: Route entry fields

Field	Description
Code	As explained in Table 3-176.
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
Destination	IP address.
Metric	Tunnel metric.
Tunnel-ID	Tunnel identifier.
Tunnel-End-Point	Tunnel endpoint address.

© 2021 IP Infusion Inc. Proprietary

show ip protocols

Use this command to display IP process parameters and statistics.

Command Syntax

```
show ip protocols
show ip protocols isis
```

Parameters

None

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip protocols
Routing Protocol is "isis 1 "
Redistributing:
Area Address(es): 52
Distance : (default is 115)
#
```

Table 3-180 explains the output fields.

Table 3-180: show ip protocols output

Field	Description
Routing Protocol	“isis” and the name that identifies the IS-IS area.
Redistributing	Protocols being redistributed (such as RIP, OSPF, or BGP), including metric, metric type (internal or external), and route map.
redistribute isis	Whether redistributing IS-IS level-1 into level-2 and vice versa.
Area Address	Network address of the areas into which the routing process is injecting routes.
Distance: (default is 115)	Administrative distance.

show ip route fast-reroute

Use this command to display Loop Free Alternate Fast Reroute (LFA FRR) routes.

Command Syntax

```
show ip route fast-reroute
```

Parameters

None

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area ,p -
stale info
* - candidate default

IP Route Table for VRF "default"
i L140.40.40.0/24 [115/10] via 10.10.10.142, eth1, 00:00:50
                           [FRR-NH] via 30.30.30.144, eth3

i L150.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:00:50
                           [FRR-NH] via 10.10.10.142, eth1

i L160.60.60.0/24 [115/15] via 10.10.10.142, eth1, 00:00:50
                           [FRR-NH] via 20.20.20.143, eth2
```


© 2021 IP Infusion Inc. Proprietary

show ip isis route fast-reroute

Use this command to display Loop Free Alternate Fast Reroute (LFA FRR) route information and interfaces on which LFA FRR is disabled.

Command Syntax

```
show ip isis (WORD|) route fast-reroute
```

Parameters

`WORD` Routing area tag.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#show ip route fast-reroute
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type
1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area ,p - stale info
* - candidate default

IP Route Table for VRF "default"
i L140.40.40.0/24 [115/10] via 10.10.10.142, eth1, 00:00:50
                          [FRR-NH] via 30.30.30.144, eth3

i L150.50.50.0/24 [115/15] via 20.20.20.143, eth2, 00:00:50
                          [FRR-NH] via 10.10.10.142, eth1

i L160.60.60.0/24 [115/15] via 10.10.10.142, eth1, 00:00:50
                          [FRR-NH] via 20.20.20.143, eth2
```

show ip isis lfa-config

Use this command to display the Loop Free Alternate Fast Reroute (LFA FRR) tie-break preferences for protection types and the termination hold-on timer.

Command Syntax

```
show ip isis (WORD|) lfa-config (level-1|level-2)
```

Parameters

`WORD` Routing area tag.

`level-1` Level 1 only.

`level-2 Level 2 only`

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#show ip isis lfa-config level-1

TIE-Breaker           Preference values
-------------------------------------------------
Primary Path:                 20
Link Protecting:              30
Node Protecting:              60
Broadcast Interface Disjoint: 70
Secondary Path:                0
Downstream Path:               0
```

Termination Hold On Interval : 1000 ms

© 2021 IP Infusion Inc. Proprietary

show isis counter

Use this command to display the MIB variables used to construct routing tables for IP networks for IS-IS as defined in RFC 4444.

Command Syntax

```
show isis counter
```

Parameters

None

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show isis counter
Tag abc: VRF : default
IS-IS Level-1 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 7
isisSysStatPRCRuns: 0

IS-IS Level-2 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 3
isisSysStatPRCRuns: 0
#
```

show isis database

Use this command to display link-state database (LSDB) database information. The LSDB is the core of IS-IS routing. All link-state information advertised by neighbors in the same area is stored in the LSDB.

Command Syntax

```
show isis database
show isis database (detail|verbose)
show isis database (detail|verbose) WORD
show isis database (detail|verbose) WORD (l1|l2|level-1|level-2)
show isis database (detail|verbose) (l1|l2|level-1|level-2)
show isis database (detail|verbose) (l1|l2|level-1|level-2) WORD
show isis database WORD
show isis database WORD (l1|l2|level-1|level-2)
show isis database WORD (l1|l2|level-1|level-2) (detail|verbose)
show isis database WORD (detail|verbose)
show isis database WORD (detail|verbose) (l1|l2|level-1|level-2)
show isis database (l1|l2|level-1|level-2)
show isis database (l1|l2|level-1|level-2) (detail|verbose)
show isis database (l1|l2|level-1|level-2) (detail|verbose) WORD
show isis database (l1|l2|level-1|level-2) WORD
show isis database (l1|l2|level-1|level-2) WORD (detail|verbose)
```

Parameters

`detail`	Detailed information.
`verbose`	Verbose information.
`WORD`	Link-state packet (LSP) identifier in the form of XXXX.XXXX.XXXX.XX-XX.
`l1`	IS-IS level-1.
`l2`	IS-IS level-2.
`level-1`	IS-IS level-1.
`level-2`	IS-IS level-2.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show isis database detail
Area bb:
IS-IS Level-1 Link State Database:
```


© 2021 IP Infusion Inc. Proprietary

```
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
000F.0000.0001.00-00* 0x00000007   0xE15E        1188              1/0/0
  Area Address: 49.000F
  NLPID:        0xCC
  IP Address:   10.10.12.97
  Metric: 10         IP 10.10.12.0 255.255.255.0
  Metric: 10         IS 000F.0000.0001.02
000F.0000.0001.02-00* 0x00000003   0x3C66        1026              1/0/0
  Metric:  0         IS 000F.0000.0001.00
  Metric:  0         IS 000F.0000.0002.00
000F.0000.0002.00-00  0x00000003   0x8C4B        1025              1/0/0
  Area Address: 49.000F
  NLPID:        0xCC
  Hostname:     isisd@redhat
  IP Address:   10.10.12.94
  Metric: 10         IP 10.10.12.0 255.255.255.0
  Metric: 10         IS 000F.0000.0001.02
#
```

Table 3-181 explains the output fields.

Table 3-181: show isis database output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
IS-IS Level-n Link State Database	Each IS-IS level has a section with Link-State Packet (LSP) information.
LSPID	Link-state packet identifier in the form of XXXX.XXXX.XXXX.XX-XX. The first six octets (“XXXX.XXXX.XXXX”) are the system identifier of the router that originated the LSP. The next octet is the pseudonode identifier: • When this octet is nonzero, the LSP describes links from a designated router (pseudonode) that creates and floods an LSP that describes all systems attached to the network. This mechanism is similar to a router link-state advertisement (LSA) in OSPF. • When this octet is zero, the LSP is from a nonpseudonode which describes the state of the originating router. The last octet is the LSP number. If the value is 0x00, the entire LSP was carried in one LSP. If there is more data than can fit in a single LSP, the LSP is divided into multiple LSP fragments and each fragment has a different LSP number. An asterisk (*) means the LSP originated on the system where the command was given.
LSP Seq Num	LSP sequence number.
LSP Checksum	LSP checksum.
LSP Holdtime	Amount of time the LSP remains valid (in seconds). An LSP hold time of zero means the LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP will stay in the LSDB before being completely removed.
ATT	Attached bit. A Level-2 IS indicates its attachment to other areas by setting its attached bit in its Level-1 LSP 0. In other words, this is only set for inter-area routes. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers will use the attach bit to find the closest Level-2 router. They will point a default route to the closest Level-2 router.

Table 3-181: show isis database output

Field	Description
P	Partition repair. A Level-1 area can become partitioned; this bit means the partition can be repaired via use of Level-2 routes.
OL	Overload bit. Determines whether the IS is congested. When the overload-bit is set in an LSP, other routers will not use this router as a transit router during SPF calculation. Only packets for destinations directly connected to the overloaded router will be sent to this router.

This command also displays information about the IS-IS TLVs in Table 3-182 if present in an LSP. For more about the TLV information, search for “IS-IS TLV Codepoints” on the Interne, check ISO/IEC 10589:2002(E), or other standard mentioned in Table 3-182.

Table 3-182: IS-IS TLV Codepoints

IS-IS TLV Codepoint	Description	Standard
1	Area Addresses	ISO 10589
2	IIS Neighbors	ISO 10589
3	ES Neighbors	ISO 10589
10	Authentication	ISO 10589, RFC 6233
22	Extended IS reachability	RFC 5305
128	IP internal reachability	RFC 1195, RFC 5302
129	Protocols supported	RFC 1195
130	IP external reachability	RFC 1195, RFC 5302
132	IP interface address	RFC 1195
134	Traffic engineering router ID	RFC 5305
135	Extended IP reachability	RFC 5305
137	Host name	RFC 5301, RFC 6233
222	Multi IS reachability	RFC 5120
229	Multi topology	RFC 5120
232	IPv6 interface address	RFC 5308
235	Multi IPv4 reachability	RFC 5120
236	IPv6 reachability	RFC 5308
237	Multi IPv6 reachability	RFC 5120

© 2021 IP Infusion Inc. Proprietary

show isis interface

Use this command to display detailed interface information.

Command Syntax

```
show isis interface
show isis interface IFNAME
show isis interface counter
```

Parameters

IFNAME	Interface name.
counter	Interface counters.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>show isis interface
eth2 is up, line protocol is up
Routing Protocol: IS-IS (abc)
Network Type: Broadcast
Circuit Type: level-2
Local circuit ID: 0x01
Extended Local circuit ID: 0x00000004
Local SNPA: 0800.2731.a9a0
IP interface address:
10.10.10.1/24
IPv6 interface address:
fe80::a00:27ff:fe31:a9a0/64
Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
Number of active level-2 adjacencies: 0
Level-2 LSP MTU: 1492
Next IS-IS LAN Level-2 Hello in 9 seconds
eth1 is up, line protocol is up
Routing Protocol: IS-IS (abc)
Network Type: Broadcast
Circuit Type: level-1
Local circuit ID: 0x02
Extended Local circuit ID: 0x00000003
Local SNPA: 0800.2714.e7f8
IP interface address:
11.11.11.1/24
IPv6 interface address:
fe80::a00:27ff:fe14:e7f8/64
Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0003.01
Number of active level-1 adjacencies: 1
Level-1 LSP MTU: 1492
```

```
Next IS-IS LAN Level-1 Hello in 5 seconds

>show isis interface eth1
eth1 is up, line protocol is up
Routing Protocol: IS-IS ((null))
Network Type: Broadcast
Circuit Type: level-1
Local circuit ID: 0x02
Extended Local circuit ID: 0x00000003
Local SNPA: 0800.27e3.0e64
IP interface address:
30.0.0.1/24
IPv6 interface address:
fe80::a00:27ff:fee3:e64/64
LDP-ISIS Sync Configured
Holddown timer = 100 seconds, Remaining time = 90 seconds
Level-1 Metric: 63/16777214, Priority: 64, Circuit ID: 0000.0000.0001.02
Number of active level-1 adjacencies: 1
Level-1 LSP MTU: 1492
Next IS-IS LAN Level-1 Hello in 1 seconds
```

Table 3-183 explains the output fields.

Table 3-183: show isis interface

Field	Description
IFNAME is up, line protocol is up/down	Whether the interface is up or down
Routing Protocol	“IS-IS” and the name that identifies the IS-IS instance.
Network Type	• Broadcast • Point-to-Point • Loopback
Circuit Type	Whether the interface is configured for: • Local routing: level-1 • Area routing: level 2 • Local and area routing: level-1-2
Local circuit ID	Local circuit identifier assigned when interface is created. Each IS-IS interface is assigned a circuit identifier to identify the interface within the link-state database. If the interface is attached to a multiaccess network, the circuit ID is concatenated with the system ID of the designated IS. This is called the pseudonode ID.
Extended Local circuit ID	Interface index.
Local SNPA	SubNetwork Point of Attachment: for broadcast networks, MAC address.
IP interface address	IPv4 addresses assigned to IS-IS interface.
IPv6 interface address	IPv6 addresses assigned to IS-IS interface.
LDP-ISIS Sync Configured	LDP IS-IS synchronization is enabled.

© 2021 IP Infusion Inc. Proprietary

Table 3-183: show isis interface (Continued)

Field	Description
Holddown timer	Delay for notifications of LDP convergence to IS-IS
Remaining time	Remaining LDP convergence hold time in seconds.
Holddown timer not configured	The LDP convergence holddown timer has not been set.
Level-1 Metric	Interface metric value; used for SPF calculation.
Priority	Priority for designated IS election.
Circuit ID	Unique ID assigned to a circuit internally.
Number of active level-1 adjacencies	Number of adjacencies formed with a neighboring router.
Level-1 LSP MTU	Maximum transmission unit: maximum transmission size for a packet on this interface.
Level-2 Metric	Interface metric value; used for SPF calculation.
Priority	Priority for designated IS election.
Circuit ID	Unique ID assigned to a circuit internally.
Number of active level-2 adjacencies	Number of adjacencies formed with a neighboring router.
Level-2 LSP MTU	Maximum transmission unit: maximum transmission size for a packet on this interface.
Next IS-IS LAN Level-1 Hello	For broadcast networks, when the next IS hello will be sent on this interface.
Next IS-IS LAN Level-2 Hello	For broadcast networks, when the next IS hello will be sent on this interface.
Next IS-IS Hello in	For point-to-point networks, when the next IS hello will be sent on this interface.
Bandwidth	Traffic engineering: interface bandwidth.
Maximum reservable bandwidth	Traffic engineering: maximum reservable interface bandwidth.
Available bandwidth at priority	Traffic engineering: available interface bandwidth at priority.
Bidirectional Forwarding Detection is disabled/enabled/ configured	BFD state

show isis spf-logs

Use this command to display the Shortest Path First (SPF) related information. It also display Partial Route Calculation (PRC) related information only when prc-interval-exp is enabled.

Command Syntax

```
show isis (WORD|) spf-logs (level-1|level-2|level-1-2)
```

Parameters

WORD	Routing area tag.
level-1	Level 1 only.
level-2	Level 2 only.
level-1-2	Level 1-2

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 3.0.

Example

```
OcNOS#show isis spf-logs level-1
Tag 1:  VRF : default
Level-1 spf logs:
 Next SPF is not scheduled yet
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 SPF algorithm executed 5 times
 SPF algorithm last executed 00:05:06.106 ago

PRC logs:
Next PRC is not scheduled yet
PRC schedule delay min 16 secs 0 msecs
PRC schedule delay max 65 secs 0 msecs
PRC algorithm executed 2 times
PRC algorithm last executed 00:03:58.256 ago
```


© 2021 IP Infusion Inc. Proprietary

show isis topology

Use this command to display paths to Intermediate Systems.

Command Syntax

```
show isis topology (l1|l2|level-1|level-2|)
show isis WORD topology (l1|l2|level-1|level-2|)
```

Parameters

WORD	Display information for specified instance.
l1	Display the path to all level-1 routers in the area.
l2	Display the path to all level-2 routers in the domain.
level-1	Display the path to all level-1 routers in the area.
level-2	Display the path to all level-2 routers in the domain.

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show isis topology

Tag abc: VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop            Interface   SNPA
000F.0000.0001       --
000F.0000.0002       10         000F.0000.0002      eth2        0006.5B0E.D27D

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop            Interface   SNPA
0000.0000.0001       10         0000.0000.0001      eth2        0000.0CFA.F002
```

Table 3-184 explains the output fields.

Table 3-184: show isis topology output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
IS-IS paths to level-n routers	Each IS-IS level has a section with topology information.
System Id	Uniquely identifies a system within an area.
Metric	ISIS metric used for SPF calculation (1-63).

Table 3-184: show isis topology output

Field	Description
Next-Hop	This route is available through the next hop router located at this IP address.
Interface	Interface from which the system was learned.
SNPA	SubNetwork Point of Attachment (SNPA): MAC address of the device.

© 2021 IP Infusion Inc. Proprietary

show running-config interface isis

Use this command to display the ISIS interface configuration.

Command Syntax

```
show running-config interface IFNAME isis
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth0 isis
!
interface eth0
 isis tag 500 level-1
!
```

show running-config router isis

Use this command to display the ISIS router configuration.

Command Syntax

```
show running-config router isis
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config-router)#show running-config router isis
!
router isis 1
passive-interface eth1
!
```


© 2021 IP Infusion Inc. Proprietary

Neighbor Discovery Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Neighbor Discovery Commands*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Neighbor Discovery Commands

This chapter provides a description, syntax, and examples of the ND commands. It includes the following commands:

- arp-ageing-timeout
- arp-reachable-time
- clear arp
- clear ipv6 neighbors
- debug ip arp
- debug ipv6 nd
- ip arp
- ip arp vrf
- ipv6 nd current-hoplimit
- ipv6 nd link-mtu
- ipv6 nd managed-config-flag
- ipv6 nd other-config-flag
- ipv6 nd other-config-flag
- ipv6 nd prefix
- ipv6 nd ra-interval
- ipv6 nd reachable-time
- ipv6 nd retransmission-time
- ipv6 nd suppress-ra
- ip proxy-arp
- ipv6 neighbor
- nd-ageing-timeout
- nd-reachable-time
- no debug all
- show arp
- show debugging ip arp
- show debugging ipv6 nd
- show ipv6 neighbors

© 2021 IP Infusion Inc. Proprietary

arp-ageing-timeout

Use this command to set the ARP ageing timeout.

Use `no` form of this command to set the ageing to its default value.

Command Syntax

```
arp-ageing-timeout <60-28800>
no arp-ageing-timeout
```

Parameter

`<60-28800>`	Specify the ARP ageing timeout.

Default value

By default, arp-ageing-timeout value is 1500

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe2
(config-if)#arp-ageing-timeout 5000
(config-if)#exit

(config)#interface xe2
(config-if)#no arp-ageing-timeout
```


© 2021 IP Infusion Inc. Proprietary

arp-reachable-time

Use this command to set the ARP reachable time.

Use `no` form of this command to set the reachable time to its default value.

Command Syntax

```
arp-reachable-time <10-3600>
no arp-reachable-time
```

Parameters

`<10-3600>`	Specify the ARP reachable time.

Default value

By default, arp-reachable-time is 60

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe2
(config-if)#arp-reachable-time 120
(config-if)#exit

(config)#interface xe2
(config-if)#no arp-reachable-time
```

clear arp

Use this command to clear dynamic ARP entries.

Command Syntax

```
clear arp (| A.B.C.D) (| vrf (all | VRFNAME | default))
clear arp IFNAME (| vrf (all | VRFNAME | default))
```

Parameters

`A.B.C.D`	Specify the IP address of the ARP entry.
`IFNAME`	Specify the name of the interface.
`all`	All VRFs.
`VRFNAME`	VPN routing/forwarding instance name.
`default`	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear arp
#clear arp xe1
#clear arp 10.10.10.10
#clear arp vrf VRF1
```


© 2021 IP Infusion Inc. Proprietary

clear ipv6 neighbors

Use this command to clear dynamic neighbor entries.

Command Syntax

```
clear ipv6 neighbors (|X:X::X:X) (|vrf (all | VRFNAME | default))
clear ipv6 neighbors IFNAME (|vrf (all | VRFNAME | default))
```

Parameters

`X:X::X:X`	Specify the neighbor's IPv6 address.
`IFNAME`	Specify the name of the interface.
`all`	All VRFs.
`VRFNAME`	VPN routing/forwarding instance name.
`default`	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 neighbors
#clear ipv6 neighbors xe1
#clear ipv6 neighbors 2000::3
#clear ipv6 neighbors vrf VRF1
```

debug ip arp

Use this command to enable debugging for ARP events or packets.

Use the `no` parameter with this command to disable event or packet debugging.

Command Syntax

```
debug ip arp (event | packet)
no debug ip arp (event | packet)
```

Parameters

`event`	ARP event debugging.
`packet`	ARP packet debugging.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip arp event
```


© 2021 IP Infusion Inc. Proprietary

debug ipv6 nd

Use this command to enable debugging for neighbor events or packets.

Use the `no` parameter with this command to disable event or packet debugging.

Command Syntax

```
debug ipv6 nd (event | packet)
no debug ipv6 nd (event | packet)
```

Parameters

`event`	ARP event debugging.
`packet`	ARP packet debugging.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ipv6 nd packet
```

ip arp

Use this command to create a static ARP entry.

Use the `no` parameter to remove the static ARP entry.

Command Syntax

```
ip arp A.B.C.D XXXX.XXXX.XXXX (alias|)
no ip arp A.B.C.D
```

Parameters

`A.B.C.D`	Specify the IP address of the ARP entry.
`XXXX.XXXX.XXXX`	Specify the MAC (hardware) address of the ARP entry.
`alias`	Specify the response to ARP requests for the IP address.

Default value

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip arp 10.10.10.10 0000.0001.4566
(config)#no ip arp 10.10.10.10
```


© 2021 IP Infusion Inc. Proprietary

ip arp vrf

Use this command to create a static ARP entry for the non-default VRF.

Note: This command is supported only for multiple VRF support.

Command Syntax

```
ip arp vrf NAME A.B.C.D XXXX.XXXX.XXXX (alias|)
```

Parameter

NAME	Specify VRF name to which entry need to be added.
A.B.C.D	Specify the IP address of the ARP entry.
XXXX.XXXX.XXXX	Specify the MAC (hardware) address of the ARP entry.
alias	Specify the response to ARP requests for the IP address.

Default value

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip arp vrf VRF1 10.10.10.10 0000.0001.4566
```

ipv6 nd current-hoplimit

Use this command to set an ND (Neighbor Discovery) advertised hop limit for an interface.

Use the `no` option of this command to set the current hop limit to its default value.

Command Syntax

```
ipv6 nd current-hoplimit <0-255>
no ipv6 nd current-hoplimit
```

Parameter

`<0-255>`	Hop limit.

Default

By default, hop limit is 64

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd current-hoplimit 10
(config-if)#no ipv6 nd current-hoplimit
```


© 2021 IP Infusion Inc. Proprietary

ipv6 nd link-mtu

Use this command to set an advertised maximum transmission unit (MTU).

Use the `no` option with the command to reset the MTU to the default statute.

Command Syntax

```
ipv6 nd link-mtu (<1280-65535>)
no ipv6 nd link-mtu
```

Parameters

`<1280-65535>`	Link MTU value.

Default

By default, link MTU value is 1500

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd link-mtu 1600
(config-if)#no ipv6 nd link-mtu
```

ipv6 nd managed-config-flag

Use this command to set the managed address configuration flag in the Router Advertisement to be used for the IPv6 address auto-configuration.

Use the `no` parameter with this command to reset the value to default.

Command Syntax

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

Parameters

None

Default

The managed address configuration flag is not set.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd managed-config-flag
(config-if)#no ipv6 nd managed-config-flag
```


© 2021 IP Infusion Inc. Proprietary

ipv6 nd other-config-flag

Use this command to set the other stateful configuration flag in Router Advertisement to be used for IPv6 address auto-configuration.

Use `no` parameter with this command to reset the value to default.

Command Syntax

```
ipv6 nd other-config-flag
no ipv6 nd other-config-flag
```

Parameters

None

Default

Other stateful configuration flag is not set.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd other-config-flag
(config-if)#no ipv6 nd suppress-ra
```

ipv6 nd prefix

Use this command to set IPv6 prefix information that is advertised for address auto-configuration.

Use `no` parameter with this command to remove an IPv6 prefix.

Command Syntax

```
ipv6 nd prefix X:X::X:X/M <0-4294967295> <0-4294967295> (off-link|) (no-
  autoconfig|)
ipv6 nd prefix X:X::X:X/M
ipv6 nd prefix valid-lifetime <0-4294967295>
ipv6 nd prefix preferred-lifetime <0-4294967295>
ipv6 nd prefix offlink
ipv6 nd prefix no-autoconf
no ipv6 nd prefix X:X::X:X/M (off-link|) (no-autoconfig|)
no ipv6 nd prefix valid-lifetime
no ipv6 nd prefix preferred-lifetime
```

Parameters

`X:X::X:X/M`	IPv6 prefix.
`<0-4294967295>`	Valid lifetime in seconds. Use the preferred-lifetime value < valid-lifetime.
`<0-4294967295>`	Preferred lifetime in seconds. Use the preferred-lifetime value < valid-lifetime.
`off-link`	Do not use prefix for onlink determination.
`no-autoconfig`	Do not use prefix for autoconfiguration.

Default

By default, valid life time is 2592000 seconds and preferred life time is 604800 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Defaults

The default valid lifetime is 2592000 seconds.

The default preferred lifetime is 604800 seconds.

Examples

```
(config)#interface eth3
(config-if)#ipv6 nd prefix 2001:ffff::/64

(config)#interface eth3
(config-if)#ipv6 nd prefix no-autoconf
```


© 2021 IP Infusion Inc. Proprietary

```
(config)#interface eth3
(config-if)#ipv6 nd prefix preferred-lifetime 550000
```

ipv6 nd ra-interval

Use this command to specify the interval between IPv6 Router Advertisements (RA).

Use `no` parameter with this command to set the value to its default.

Note: The RA interval will have a random variation from configured interval to avoid synchronization of advertisement with routers.

Command Syntax

```
ipv6 nd ra-interval <4-1800> (<3-1350>|)
no ipv6 nd ra-interval
```

Parameter

`<4-1800>`	RA interval in seconds.
`<3-1350>`	Minimum RA interval (in seconds).

Default

By default, RA interval is 600 seconds, and Minimum RA interval is 0.33*RA interval.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd ra-interval 60 15
(config-if)#ipv6 nd prefix 3ffe:ffff:ffff::/64

(config-if)#no ipv6 nd ra-interval
```


© 2021 IP Infusion Inc. Proprietary

ipv6 nd ra-lifetime

Use this command to specify the Router Advertisement (RA) lifetime for this device to act as a default gateway for the network.

Use `no` parameter with this command to reset the value to default.

Command Syntax

```
ipv6 nd ra-lifetime <0-9000>
no ipv6 nd ra-lifetime
```

Parameter

`<0-9000>`	RA lifetime duration in seconds.

Default

The default RA lifetime is 1800 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd ra-lifetime 9000
(config-if)#no ipv6 ra-lifetime 9000
```

ipv6 nd reachable-time

Use this command to specify the reachable time in the Router Advertisement to be used for detecting unreachability of the IPv6 neighbor.

Use the `no` parameter with this command to set the value to its default.

Command Syntax

```
ipv6 nd reachable-time <0-3600000>
no ipv6 nd reachable-time
```

Parameter

`<0-3600000>`	Reachable time in milliseconds.

Default

By default, reachable time is zero (0) milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd reachable-time 1800000
(config-if)#no ipv6 nd reachable-time 1800000
```


© 2021 IP Infusion Inc. Proprietary

ipv6 nd retransmission-time

Use this command to set an IPv6 advertised retransmission time for the current interface.

Use the `no` form of the command to set the retransmission time to its default value.

Command Syntax

```
ipv6 nd retransmission-time (0-4294967295)
no ipv6 nd retransmission-time
```

Parameter

`<0-4294967295>` Retransmission time in milliseconds

Default

By default, retransmission time is zero (0) milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd retransmission-time 1200
(config-if)#no ipv6 nd retransmission-time
```

ipv6 nd suppress-ra

Use this command to suppress IPv6 Router Advertisement (RA) transmission for the current interface. Router Advertisement is used for IPv6 stateless auto-configuration.

Use the `no` parameter with this command to enable Router Advertisement transmission.

Command Syntax

```
ipv6 nd suppress-ra (mtu |)
no ipv6 nd suppress-ra (mtu |)
```

Parameters

`mtu`	Do not send maximum transmission unit (MTU) in Router Advertisement messages

Default

By default, ipv6 nd suppress-ra is suppressed

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd suppress-ra
```


© 2021 IP Infusion Inc. Proprietary

ip proxy-arp

Use this command to enable the proxy ARP feature.

Use the `no` parameter to disable the proxy ARP feature.

Command Syntax

```
ip proxy-arp
no ip proxy-arp
```

Parameter

None

Default value

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ip proxy-arp
(config-if)#no ip proxy-arp
```

ipv6 neighbor

Use this command to add a static neighbor entry.

Use the `no` form of this command to remove a static neighbor entry.

Command Syntax

```
ipv6 neighbor X:X::X:X IFNAME XXXX.XXXX.XXXX
no ipv6 neighbor X:X::X:X IFNAME
```

Parameter

`X:X::X:X`	Specify the neighbor's IPv6 address.
`IFNAME`	Specify the name of the interface.
`XXXX.XXXX.XXXX`	Specify the MAC hardware address.

Default value

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 neighbor 2000::3 xe1 0000.0002.3dc1
(config)#no ipv6 neighbor 2000::3 xe1
```


© 2021 IP Infusion Inc. Proprietary

nd-ageing-timeout

Use this command to set the neighbor ageing timeout value.

Use `no` form of this command to set the ageing to its default value.

Command Syntax

```
nd-ageing-timeout <60-28800>
no nd-ageing-timeout
```

Parameters

`<60-2880>`	ND ageing timeout in seconds.
`IFNAME`	Specify the name of the interface.
`XXXX.XXXX.XXXX`	Specify the MAC hardware address.

Default value

By default, nd-ageing-timeout is 1500 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#nd-ageing-timeout 3600
(config-if)#no nd-ageing-timeout
```

© 2021 IP Infusion Inc. Proprietary

nd-reachable-time

Use this command to set neighbor reachable time value.

Use `no` form of this command to set the reachable time to its default value.

Command Syntax

```
nd-reachable-time <10-3600>
no nd-reachable-time
```

Parameter

`<10-3600>`	ND reachable time in seconds.

Default value

By default, nd-reachable-time is 60 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#nd-reachable-time 300
(config-if)#no nd-reachable-time
```


© 2021 IP Infusion Inc. Proprietary

no debug all

Use this command to disable all ARP and the neighbor debugging.

Command Syntax

```
no debug all
undebug all
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#no debug all
```

show arp

Use this command to display ARP entry information.

Command Syntax

```
show arp (| (A.B.C.D | detail | static) (| vrf (all | VRFNAME | default)))
show arp IFNAME (| vrf (all | VRFNAME | default))
show arp summary (|IFNAME) (| vrf (all | VRFNAME | default))
```

Parameters

`detail`	Display detailed information.
`static`	Display static ARP entries.
`A.B.C.D`	Specify the IP address of the ARP entry.
`IFNAME`	Specify the name of the interface.
`all`	All VRFs.
`VRFNAME`	VPN routing/forwarding instance name.
`default`	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show arp

Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 2
Address          Age      MAC Address     Interface  State
10.12.18.1       00:00:18 44e4.d982.274b  eth0       REACHABLE
10.10.10.20      00:02:33 a8b1.d433.4140  xe1        STALE

#show arp summary vrf default

IP ARP Table - Adjacency Summary

  Resolved   : 2
  Incomplete : 0
  Unknown    : 0
  Total      : 2
```


© 2021 IP Infusion Inc. Proprietary

Table 1-185 explains the show command output fields.

Table 1-185: show arp output details

Entry	Description
Address	ARP entry's IP address in the device.
Age	The number of minutes before the ARP entry was refreshed. If this value reaches the ARP aging period, the entry is removed from the table. Static entries do not age out.
MAC Address	Physical address of the host.
Interface	Logical address to connect the device over network.
State	INCOMPLETE – first ARP request sent, send ARP request. REACHABLE – normal expiration reset use counter. STALE – still usable; needs verification reset use counter; change state to delay. DELAY – schedule ARP request; needs verification reset use counter. PROBE – sending ARP request reset use counter. FAILED – no response received send ARP request. NOARP – normal expiration; never verified reset use counter. PERMANENT – never expires; never verified reset use counter.

Network devices are considered adjacent if they can reach each other with a single hop. The summary command shows the count of the state of devices that are adjacencies.

Table 1-186 explains the show command output fields.

Table 1-186: show arp summary output details

Field	Description
Resolved	Count of working/known adjacencies.
Incomplete	Count of yet to be established adjacencies.
unknown	Count of adjacencies not currently in ARP table.
Total	Total count of all adjacencies.

show debugging ip arp

Use this command to display debugging information for ARP.

Command Syntax

```
show debugging ip arp
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging ip arp
ND IP Debugging status:
  ND ip arp event debugging is off
  ND ip arp packet debugging is off
```


© 2021 IP Infusion Inc. Proprietary

show debugging ipv6 nd

Use this command to display debugging information for the neighbor.

Command Syntax

```
show debugging ipv6 nd
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging ipv6 nd
ND IPV6 Debugging status:
  ND ipv6 event debugging is off
  ND ipv6 packet debugging is off
```

show ipv6 neighbors

Use this command to display the neighbor information.

Command Syntax

```
show ipv6 neighbors (| (X:X::X:X | detail | static) (| vrf (all | VRFNAME |
  default)))
show ipv6 neighbors IFNAME (| vrf (all | VRFNAME | default))
show ipv6 neighbors summary (| IFNAME) (| vrf (all | VRFNAME | default))
```

Parameters

`detail`	Show detail information of neighbor.
`static`	Static entry.
`X:X::X:X`	Specify the neighbor's IPv6 address.
`IFNAME`	Specify the name of the interface.
`all`	All VRFs.
`VRFNAME`	VPN routing/forwarding instance name.
`default`	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 neighbors

R - Reachable, I - Incomplete, S - Stale, F - Failed, P - Probe,
D - Delay, PR - Permanent

Flags: (D) - Static neighbors attached to down interface

IPv6 Neighbor Table for context default
Total number of entries:2
Address         Age       MAC Address     Source  Interface      State
fe80::210:18ff:fe7f:f758
                00:43:04  0010.187f.f758  icmpv6  eth0             S
2000::5         00:55:25  0000.0001.0242  icmpv6  xe1              S

#show ipv6 neighbors summary

IPv6 Neighbors Table - Adjacency Summary

  Resolved   : 2
  Incomplete : 0
  Unknown    : 0
  Total      : 2
```


© 2021 IP Infusion Inc. Proprietary

Table 1-187 shows the status codes displayed at the start of a route entry.

Table 1-187: status code output details

Status Code	Field	Description
R	Reachable	Normal expiration reset use counter.
I	Incomplete	First ARP request sent, send ARP request.
S	Stale	Still usable; needs verification reset use counter; change state to delay.
F	Failed	ARP requests response not received.
P	Probe	ARP request reset use counter.
D	Delay	Schedule ARP request; needs verification reset use counter.
PR	Permanent	Never expires; never verified reset use counter.

Table 1-188 explains the show command output fields.

Table 1-188: show ipv6 neighbors output details

Field	Description
Address	ARP entry's IP address in the device.
Age	The number of minutes before the ARP entry was refreshed. If this value reaches the ARP aging period, the entry is removed from the table. Static entries do not age out.
MAC Address	Physical address of the host.
Source	ARP request source in the interface.
Interface	Logical address to connect the device over network.
State	ARP request state that is being handled by the IPv6 neighbor session.

Table 1-189 explains the show command output fields.

Table 1-189: show arp summary output details

Field	Description
Resolved	Count of working/known adjacencies.
Incomplete	Count of yet to be established adjacencies.
unknown	Count of adjacencies not currently in ARP table.
Total	Total count of all adjacencies.

© 2021 IP Infusion Inc. Proprietary

SECTION 7 Multicast

Multicast Configuration Guide

Contents

This document contains these chapters and appendices:

- Chapter 1, *IGMP Configuration*
- Chapter 2, *IGMP Proxy Configuration*
- Chapter 3, *PIM Sparse Mode Configuration*
- Chapter 4, *PIM Dense Mode Configuration*
- Chapter 5, *IGMP Snooping Configuration*
- Chapter 6, *MSDP Configuration*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 IGMP Configuration

This chapter describes how to configure Internet Group Management Protocol (IGMP).

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to any immediately-neighboring multicast routers.

Using the information obtained through IGMP, the router maintains a list of multicast group on a per-interface basis. The routers that receive these IGMP packets send multicast data that they receive for requested groups out the network segment of the known receivers.

By default, when PIM is enabled on an interface, IGMP version 3 is enabled. IGMP can be enabled on an interface explicitly.

IGMP Versions

OcNOS supports IGMPv2 and IGMPv3, as well as IGMPv1 report reception. By default, OcNOS enables IGMPv3 when PIM is enabled on an interface.

IGMPv3 includes the following key changes from IGMPv2:

- Support for Source-Specific Multicast (SSM), which builds shortest path trees from each receiver to the source, through the following feature:
  - Host messages that can specify both the group and the source.
  - The multicast state that is maintained for groups and sources, not just for groups as in IGMPv2.
- Hosts no longer perform report suppression, which means that hosts always send IGMP membership reports when an IGMP query message is received.

IGMP Operation

IGMP works on the premise of three major packets exchange between IGMP enabled routers and hosts, interested in joining a particular group.

IGMP Query Operation

Once IGMP is enabled or pim is enabled (which enables igmpv3), on any interface it starts sending Query message, which is called general query to the all-hosts multicast group at 224.0.0.1 periodically to discover whether any hosts want to receive multicast data.

OcNOS elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes the designated querier. If that router later receives a host query message from a router with a lower IP address, it drops its role as the designated querier and sets its querier timer again.

In the figure below Router-1 eth2 sends query every query-interval. Since Router1-eth2 IP address is less than Router-2 eth2, Router-1 eth2 becomes querier on the LAN.

IGMP Membership Report Operation

When a host receives a query from the local router it sends a Host Membership Report for all the multicast groups for which it wants to receive multicast traffic. This is called solicited membership report.

When a host joins a new group, the host immediately sends a Membership Report to inform a local router that it wants to receive multicast traffic for the group it has just joined without waiting to receive a Query. This is called unsolicited membership report.

In the figure below Host-1 and Host-2 sends membership reports to Router-1 eth2 for all the multicast groups for which they want to receive multicast traffic. Upon reception of membership report Router-1 maintains an IGMP group table containing multicast group-address, interface name on which it receives the report.

IGMP Leave Operation

When a multicast host leaves a group, a host that runs IGMPv2 or later sends an IGMP leave message. To check if this host is the last host to leave the group, the router sends an IGMP query (Called as Group-specific-query) message and starts a timer that you can configure called the last member query response interval. If no reports are received before the timer expires, the software removes the group state. The router continues to send multicast traffic for a group until its state is removed.

In the figure below Host-1 and Host-2 sends leave message to Router-1 eth2 for all the multicast groups for which they don’t want to receive multicast traffic. In response to leave message Router-1 eth2 sends an group-specific-query message before removing the multicast group address from the IGMP table.

Topology

The procedures in this section use the topology in Figure 1-10.

© 2021 IP Infusion Inc. Proprietary

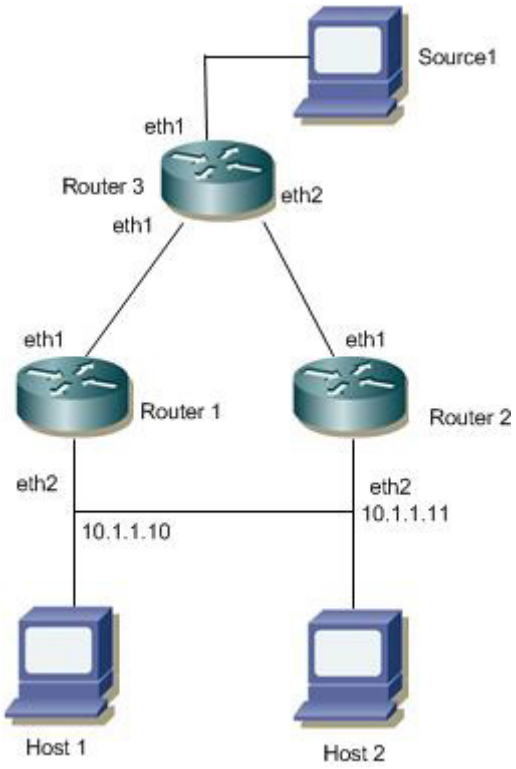


Figure 1-10: IGMP Topology

IGMP Configuration

The following example shows IGMP configuration on Router1.

Configuring IGMP Version

The configuration that follows shows how IGMP version can be configured.

`#configure terminal`	Enter configure mode.
`(config)#ip multicast-routing`	Enable IP multicast routing
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 10.1.1.10/24`	Assign IP address to an interface
`(config-if)#ip igmp version 2`	Enable IGMP version as v2.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Enter the commands listed in this section to confirm the previous configurations.

```
#show  running-config
!
no service password-encryption
```

```
!
hostname rtr1
!
ip multicast-routing
!
!
interface eth2
ip address 10.1.1.10/24
no shutdown
ip igmp version 2
```

Configuring IGMP Parameters

The configuration that follows shows how IGMP parameters can be configured.

`#configure terminal`	Enter configure mode.
`(config)#ip multicast-routing`	Enable IP multicast routing
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip igmp access-group 1`	Configures a access-list policy to control the multicast groups that hosts on the subnet serviced by an interface can join.
`(config-if)#ip igmp immediate-leave group-list 1`	Enables the device to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group.
`(config-if)#ip igmp  join-group 224.1.1.1`	Statically binds a multicast group to the outgoing interface
`(config-if)# ip igmp  last-member-query-count 7`	Sets the query count used when the software starts up.
`(config-if)# ip igmp  last-member-query-interval 25500`	Sets the query interval used when the software starts up.
`(config-if)#ip igmp limit 100`	Configure Max Allowed State on this interface
`(config-if)#ip igmp querier-timeout 300`	Sets the querier timeout that the router uses when deciding to take over as the querier.
`(config-if)#ip igmp  query-interval 200`	Sets the frequency at which the router sends IGMP host query messages.
`(config-if)#ip igmp  query-max-response-time 150`	Sets the response time advertised in IGMP queries.
`(config-if)#ip igmp  ra-option`	Enable ra-option.
`(config-if)#ip igmp  robustness-variable 4`	Sets the robustness variable.
`(config-if)#ip igmp startup-query-count 4`	Sets the query count used when the router starts up.
`(config-if)# ip igmp startup-query-interval 50`	Sets the query interval used when the router starts up.
`(config-if)# ip igmp static-group 225.1.1.1`	Statically binds a multicast group to the outgoing interface.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Enter the commands listed in this section to confirm the previous configurations.

© 2021 IP Infusion Inc. Proprietary

```
Rtr1#show  running-config
!
no service password-encryption
!
hostname rtr1
!
!
ip multicast-routing
!
!
interface eth2
 ip address 10.1.1.10/24
 no shutdown
 ip igmp access-group 1
 ip igmp immediate-leave group-list 1
 ip igmp last-member-query-count 7
 ip igmp limit 100
 ip igmp join-group 224.1.1.1
 ip igmp static-group 225.1.1.1
 ip igmp last-member-query-interval 25500
 ip igmp querier-timeout 300
 ip igmp query-interval 200
 ip igmp query-max-response-time 150
 ip igmp startup-query-interval 50
 ip igmp startup-query-count 4
 ip igmp robustness-variable 4
 ip igmp ra-option
 ip igmp version 2
 !!

Rtr1#show  ip igmp   interface  eth2
Interface eth2 (Index 4)
 IGMP Enabled, Active, Querier, Configured for version 2
Internet address is 10.1.1.10
IGMP interface limit is 100
IGMP interface has 2 group-record states
IGMP Interface statistics:
v1-reports: 0
v2-reports: 0, v2-leaves: 0
v3-reports: 0
IGMP query interval is 200 seconds
IGMP Startup query interval is 50 seconds
IGMP Startup query count is 4
IGMP querier timeout is 300 seconds
IGMP max query response time is 150 seconds
Group Membership interval is 950 seconds
IGMP Last member query count is 7
Last member query response interval is 25500 milliseconds
```

Here is the sample configuration on Router-1 with all the IGMP related commands configured.

```
Rtr1#show  running-config
!
no service password-encryption
!
hostname rtr1
!
!
```

```
ip domain-lookup
!
ip multicast-routing
!
ip pim register-rp-reachability
ip pim crp-cisco-prefix
!
interface lo
 ip address 127.0.0.1/8
 ip address 1.1.1.57/32 secondary
 ipv6 address ::1/128
 no shutdown
!
interface eth0
 ip address 10.12.48.179/24
 no shutdown
!
interface eth1
 ip address 192.168.1.27/24
 no shutdown
 ip igmp version 2
 !
interface eth2
 ip address 10.1.1.10/24
 no shutdown
 ip igmp access-group 1
 ip igmp immediate-leave group-list 1
 ip igmp last-member-query-count 7
 ip igmp limit 100
 ip igmp join-group 224.1.1.1
 ip igmp static-group 225.1.1.1
 ip igmp last-member-query-interval 25500
 ip igmp querier-timeout 300
 ip igmp query-interval 200
 ip igmp query-max-response-time 150
 ip igmp startup-query-interval 50
 ip igmp startup-query-count 4
 ip igmp robustness-variable 4
 ip igmp ra-option
 ip igmp version 2

!
line con 0
 login
line vty 0 16
 exec-timeout 0 0
 login
line vty 17 39
 login
!
End
```


© 2021 IP Infusion Inc. Proprietary

IGMP Group Table after IGMPV2 Membership Report is received

IGMP group table is populated at router by virtue of either static join is configured on interface or dynamic report is being received on the interface.

The `show ip igmp group` command displays the IGMP group table. In this table, the following fields are defined.

Table 1-190: IGMP group table after IGMPV2 membership report

Group address	Displays the Multicast Group for which report is received.
Interface	Interface name on which Membership report is received.
Uptime	Duration since the report is received.
Expiry	Time frame in which the multicast group is going to expire.
Last Reporter	Host address from where the report is generated.

```
Rtr1#show  ip igmp groups
IGMP Connected Group Membership
Group Address    Interface      Uptime     Expires      Last Reporter
224.0.1.3            eth2       00:10:06   00:03:43     10.1.1.52
224.1.1.1            eth2       01:54:53   static         0.0.0.0
225.1.1.1            eth2       00:17:22   static         0.0.0.0

Rtr1#show ip igmp groups detail
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.0.1.3
Flags:          R
Uptime:         00:10:06
Group mode:     Exclude (Expires: 00:03:43)
State: Active
Last reporter:  10.1.1.52
Source list is empty

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.1.1.1
Flags:          L
Uptime:         01:54:59
Group mode:     Exclude (Static)
State: Active
Last reporter:  0.0.0.0
Source list is empty

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          225.1.1.1
```

```
Flags:          SG
Uptime:         00:17:28
Group mode:     Exclude (Static)
State: Active
Last reporter:  0.0.0.0
Source list is empty
```

IGMP Group Table after IGMPV3 Membership report is received

IGMP group table is populated at router by virtue of either static join is configured on interface or dynamic report is being received on the interface. Here IGMPV3 should be configured on the interface (by default IGMPv3 will be enabled if pim is configured on the interface).

The `show ip igmp group` command displays the IGMP group table. In this table, the following fields are defined.

Table 1-191: IGMP group table after IGMPV3 membership

Group address	Displays the Multicast Group for which report is received.
Interface	Interface name on which Membership report is received.
Uptime	Duration since the report is received.
Expiry	Time frame in which the multicast group is going to expire.
Last Reporter	Host address from where the report is generated.

```
rtr6#show  ip igmp  groups
IGMP Connected Group Membership
Group Address    Interface            Uptime   Expires  Last Reporter
224.0.1.3        eth2                 00:08:50 00:02:10 192.168.10.52
rtr6#show  ip igmp  groups detail
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.0.1.3
Flags:          R
Uptime:         00:08:50
Group mode:     Exclude (Expires: 00:04:57)
Last reporter:  192.168.10.52
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)

Exclude Source List :
  Source Address  Uptime    v3 Exp    Fwd  Flags
  1.2.3.4         00:08:50  stopped   No   R

For IGMPV3 report source list specifies which source to be included or exclude
based on the membership report sent by the hosts.

In the above show command, Source address 1.2.3.4 is excluded to send
Multicast data  for group 224.0.1.3
```


© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 IGMP Proxy Configuration

In some simple tree topologies, it is not necessary to configure complex multicast routing protocols, such as PIM, on the boundary devices. It is sufficient to learn and proxy the group membership information and simply forward multicast packets based upon that information. Using IGMP forwarding (RFC 4605) to replicate multicast traffic on devices such as the edge boxes can greatly simplify the design and implementation of those devices. By not supporting more complicated multicast routing protocol such as Protocol Independent Multicast (PIM), it reduces not only the cost of the devices but also the operational overhead. Another advantage is that it makes the proxy devices independent of the multicast routing protocol used by the core network routers.

IGMP proxy can be used in such topologies instead of PIM. With IGMP proxy configured, the device serves as a proxy for the downstream hosts to send IGMP messages, maintain group memberships, and implement multicast forwarding based on the memberships. In this case, each boundary device configured with IGMP proxying is a host but no longer a PIM neighbor to the upstream device.

A device with IGMP proxy configured maintains a group membership database, which stores the group memberships on all the downstream interfaces. Each entry comprises the multicast address, filter mode, and source list. Such an entry is a collection of members in the same multicast group on each downstream interface.

A proxy device performs host functions on the upstream interface based on the database. It responds to queries according to the information in the database or sends join/leave messages when the database changes. On the other hand, the proxy device performs router functions on the downstream interfaces by participating in the querier election, sending queries, and maintaining memberships based on the reports.

Terminology

Following is a brief description of terms and concepts used to describe the IGMP Proxy:

Upstream interface

Also referred to as the proxy interface. A proxy interface is an interface on which IGMP proxy service is configured. It is in the direction toward the root of the multicast forwarding tree. An upstream interface acts as a host running IGMP; therefore, it is also called host interface.

Downstream interface

An interface that is running IGMP and in the direction contrary to the root of the multicast forwarding tree. A downstream interface acts as a router running IGMP; therefore, it is also called router interface.

Member State

State of the associated group address and interface.

- Idle - Interface has not yet responded to a group membership query or general query for this group.
- Delay - Interface has responded to the latest group membership query or general query for this group.

IGMP-Proxy Configuration Steps

This section provides the configuration steps for configuring IGMP Proxy and example for a relevant scenario.

- Enable IP multicast on each router (see Enabling IP Multicast Routing)
- Enable IGMP Proxy service on the upstream interface.
- Enable IGMP mrouter configuration on the downstream interface.
- Enable IGMP proxy unsolicited report interval on the proxy interface. The proxy group membership reports are forwarded to the upstream router in this unsolicited report interval time. This is an optional parameter in which the default value of 1 sec is considered for forwarding proxy groups to upstream router.

Note: Configure IP addresses on all the interfaces used in the topology.

Unicast routing protocol should be configured in the PIM domain.

Topology

In this network topology, Router 1 acts as a proxying router to the upstream router Router 2 in which PIM domain is present. Also the source address is 172.31.1.52 and the group address is set to 224.0.1.3.

Note: Any PIM mode (PIM-SM,PIM-DM,PIM-SMDM) should be enabled on all the interfaces in the PIM domain.

Here in this example default value for unsolicited report interval is considered.

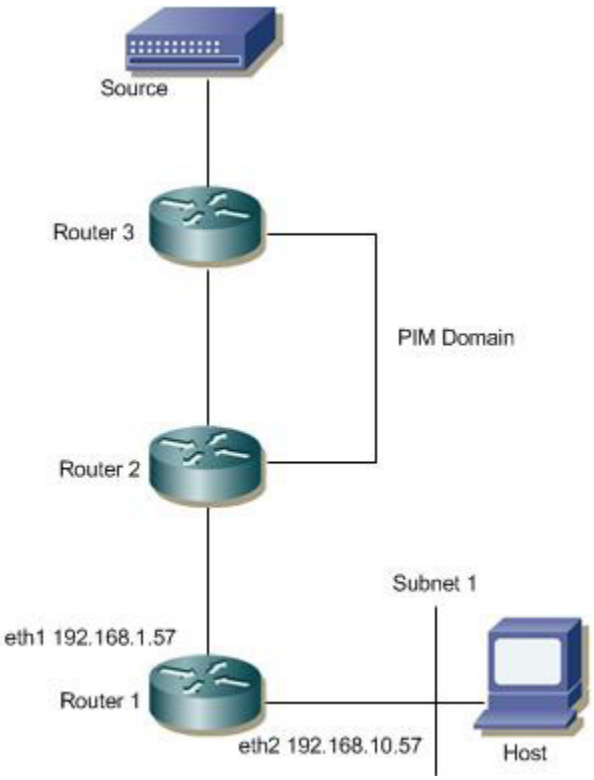


Figure 2-11: IGMP Proxy Topology

In this example, Routers 2 and 3 are running PIM and Router1 is the IGMP Proxying router.

- Host ends an IGMP membership report to Subnet 1.
- Downstream interface on Router1 received IGMP reports from host and updates the proxy interface.

© 2021 IP Infusion Inc. Proprietary

- IGMP Proxying router (Router1) maintains the group membership information and forwards the received report to the upstream router (Router2).
- Source then sends a data packet for group.
- When the data packet reaches Router1, it forwards via the interface, eth2, because it has an IGMP join requested for Multicast traffic.

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

`#configure terminal`	Enter configure mode.
`(config)# ip multicast-routing`	Enable IP multicast routing.
`(config)#exit`	Exit Configure mode.

Enabling Proxy upstream interface

Enable IGMP proxy service on the interface in which the interface is in the direction toward the root of the multicast forwarding tree. In this example eth1 is the upstream interface which acts as an IGMP host.

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 192.168.1.57/24`	Assign IP address to an interface
`(config-if)#ip igmp proxy-service`	Enable IGMP proxy service on the upstream interface.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit Configure mode.

Enabling Proxy downstream interface

Enable IGMP mrouter proxy on the interface in which the interface is in the direction contrary to the root of the multicast forwarding tree. In this example eth2 is the downstream interface which is connected to receiver.

`#configure terminal`	Enter configure mode.
`(config)#interface eth2`	Enter interface mode
`(config-if)#ip address 192.168.10.57/24`	Assign IP address to an interface
`(config-if)#ip igmp mroute-proxy eth1`	Enable IGMP mroute proxy on the downstream interface and specify the upstream proxy interface name.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Here is the same configuration for IGMP Proxying router.

```
hostname Router1
!
interface lo
!!
ip multicast-routing
!
interface eth0
!
interface eth1
 ip address 192.168.1.57/24
 no shutdown
 ip igmp proxy-service
!
interface eth2
 ip address 192.168.10.57/24
 no shutdown
 ip igmp mroute-proxy eth1
!
```

IGMP proxy interface

The following output displays the IGMP Proxy interface information.

```
Router1#show ip igmp interface

Interface eth1 (Index 3)
 IGMP Enabled, Active, Version 3 (default), proxy-service
 IGMP host version 3
 Internet address is 192.168.1.57
 Unsolicited Report Interval is 1000 milliseconds


Interface eth2 (Index 4)
 IGMP Enabled, Active, Querier, Version 3 (default)
 IGMP mroute-proxy interface is eth1
 Internet address is 192.168.10.57
 IGMP interface has 1 group-record states
IGMP Interface statistics:
v1-reports: 0
v2-reports: 1, v2-leaves: 0
v3-reports: 0
IGMP query interval is 125 seconds
 IGMP Startup query interval is 31 seconds
 IGMP Startup query count is 2
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Group Membership interval is 260 seconds
 IGMP Last member query count is 2
 Last member query response interval is 1000 milliseconds
```


© 2021 IP Infusion Inc. Proprietary

IGMP proxy

The following output displays the IGMP proxy information.

```
Router1#show ip igmp proxy

Interface eth2 (Index 4)
Administrative status: enabled
Operational status: up
Upstream interface is eth1
Number of multicast groups: 1
```

IGMP proxy groups

The following output displays the IGMP proxy group membership information.

```
Router1#show ip igmp proxy groups

IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
224.0.1.3        eth1                 Active    Delay
```

IP Multicast Routing Table

```
The show ip mroute command displays the IP multicast routing table.
Router1#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(172.31.1.52, 224.0.1.3), uptime 00:00:05
Owner IGMP-Proxy-Service, Flags: F
  Incoming interface: eth1
  Outgoing interface list:
    eth2 (1)
```

Enabling Unsolicited report interval

Enable IGMP proxy unsolicited report interval on the upstream interface. The proxy group membership reports are forwarded to the upstream router in this unsolicited report interval time.

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#ip igmp proxy unsolicited-report-interval 20000`	Enable IGMP proxy unsolicited report interval value on the upstream interface.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Here is the same configuration for IGMP Proxying router.

```
hostname Router1
!
interface eth0
!
interface eth1
ip address 192.168.1.57/24
ip igmp proxy-service
ip igmp proxy unsolicited-report-interval 20000
!
interface eth2
ip address 192.168.10.57/24
ip igmp mrouter-proxy eth1
!
interface lo
!
!
ip multicast-routing
!
```

IGMP proxy Unsolicited report interval

The following output displays the IGMP proxy unsolicited report interval information.

```
Router1#show ip igmp interface eth1

Interface eth1 (Index 3)
 IGMP Enabled, Active, Version 3 (default), proxy-service
 IGMP host version 3
 Internet address is 192.168.1.57
 Unsolicited Report Interval is 20000 milliseconds
```

IGMP proxy group with unsolicited report interval

The following output displays the IGMP proxy group membership information when the proxy unsolicited report interval is configured to specific value.

```
Router1#show ip igmp proxy groups

IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
224.0.1.3        eth1                 Active    Idle
```

IP Multicast Routing Table

The `show ip mroute` command displays the IP multicast routing table.

```
Router1#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
```


© 2021 IP Infusion Inc. Proprietary

```
(172.31.1.52, 224.0.1.3), uptime 00:00:05
Owner IGMP-Proxy-Service, Flags: F
  Incoming interface: eth1
  Outgoing interface list:
    eth2 (1)
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 PIM Sparse Mode Configuration

The Protocol Independent Multicasting-Sparse Mode (PIM-SM) is a multicast routing protocol designed to operate efficiently across Wide Area Networks (WANs) with sparsely distributed groups. It helps geographically dispersed network nodes to conserve bandwidth and reduce traffic by simultaneously delivering a single stream of information to multiple locations. PIM-SM uses the IP multicast model of receiver-initiated membership, supporting both shared and shortest-path trees, and uses soft-state mechanisms to adapt to changing network conditions. It relies on a topology-gathering protocol to populate a multicast routing table with routes.

Terminology

Following is a brief description of terms and concepts used to describe the PIM-SM protocol:

Rendezvous Point

A Rendezvous Point (RP) router is configured as the root of a non-source-specific distribution tree for a multicast group. Join messages from receivers for a group are sent towards the RP. Data from senders is sent to the RP so that receivers can discover who the senders are, and receive traffic destined for the group.

Multicast Routing Information Base

The Multicast Routing Information Base (MRIB) is a multicast topology table derived from the unicast routing table. In PIM-SM, the MRIB decides where to send Join/Prune messages. It also provides routing metrics for destination addresses. These metrics are used when sending and processing Assert messages.

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only if `IF1` is the interface the router uses to reach `SourceA`. To determine if the interface is correct, it consults its unicast routing tables. The packet that arrives through interface `IF1` is forwarded because the routing table lists this interface as the shortest path. The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link, once in each direction.

Tree Information Base

The Tree Information Base (TIB) is a collection of states at a PIM router storing the state of all multicast distribution trees at that router. The TIB is created by receiving Join/Prune messages, Assert messages, and IGMP information from local hosts.

Upstream

Upstream indicates that traffic is going towards the root of the tree. The root of the tree might be either the Source or the RP.

Downstream

Downstream indicates that traffic is going away from the root of the tree. The root of tree might be either the Source or the RP.

Source-Based Trees

In Source-Based Trees, the forwarding paths are based on the shortest unicast path to the source. If the unicast routing metric used is `hop counts`, the branches of the multicast Source-Based Trees are minimum hop. If the metric used is `delay`, the branches are minimum delay. A corresponding multicast tree directly connects the source to all receivers for every multicast source. All traffic to the members of an associated group passes along the tree made for their source. Source-Based Trees have two entries with a list of outgoing interfaces -- the source address and the multicast group.

Shared Trees

Shared trees, or RP trees (RPT), rely on a central router called the Rendezvous Point (RP) that receives all traffic from the sources, and forwards that traffic to the receivers. There is a single tree for each multicast group, regardless of the number of sources. Only the routers on the tree know about the group, and information is sent only to interested receivers. With an RP, receivers have a place to join, even if no source exists. The shared tree is unidirectional, and information flows only from the RP to the receivers. If a host other than the RP has to send data on the tree, the data must first be tunneled to the RP, then multicast to the members. This means that even if a receiver is also a source, it can only use the tree to receive packets from the RP, and not to send packets to the RP (unless the source is located between the RP and the receivers).

Note: Not all hosts are receivers.

Bootstrap Router

When a new multicast sender starts sending data packets, or a new receiver starts sending Join messages towards the RP for that multicast group, the sender needs to know the next-hop router towards the RP. The bootstrap router (BSR) provides group-to-RP mapping information to all the PIM routers in a domain, allowing them to map to the correct RP address.

Data Flow from Source to Receivers in PIM-SM Network Domain

1. Sending out Hello Messages

   PIM routers periodically send Hello messages to discover neighboring PIM routers. Hello messages are multicast using the address, 224.0.0.13 (`ALL-PIM-ROUTERS` group). Routers do not send any acknowledgement that a Hello message was received. A `holdtime` value determines the length of time for which the information is valid. In PIM-SM, a downstream receiver must join a group before traffic is forwarded on the interface.

2. Electing a Designated Router

   In a multi-access network with multiple routers connected, one of the routers is selected to act as a designated router (DR) for a given period. The DR is responsible for sending Join/Prune messages to the RP for local members.

3. Determining the Rendezvous Point

   PIM-SM uses a BSR to originate bootstrap messages, and to disseminate RP information. The messages are multicast to the group on each link. If the BSR is not apparent, the routers flood the domain with advertisements.

© 2021 IP Infusion Inc. Proprietary

The router with the highest priority (if priorities are same, the higher IP address applies) is selected to be the RP. Routers receive and store bootstrap messages originated by the BSR. When a DR gets a membership indication from IGMP for (or a data packet from) a directly connected host, for a group for which it has no entry, the designated router (DR) maps the group address to one of the candidate RPs that can service that group. The DR then sends a Join/Prune message towards that RP. In a small domain, the RP can also be configured statically.

4. Joining the Shared Tree

   To join a multicast group, a host sends an IGMP message to its upstream router, after which the router can accept multicast traffic for that group. The router sends a Join message to its upstream PIM neighbor in the direction of the RP. When a router receives a Join message from a downstream router, it checks to see if a state exists for the group in its multicast routing table. If a state already exists, the Join message has reached the shared tree, and the interface from which the message was received is entered in the Outgoing Interface list. If no state exists, an entry is created, the interface is entered in the Outgoing Interface list, and the Join message is again sent towards the RP.

5. Registering with the RP

   A DR can begin receiving traffic from a source without having a Source or a Group state for that source. In this case, the DR has no information on how to get multicast traffic to the RP through a tree. When the source DR receives the initial multicast packet, it encapsulates it in a Register message, and unicasts it to the RP for that group. The RP de-encapsulates each Register message, and forwards the extracted data packet to downstream members on the RPT. Once the path is established from the source to the RP, the DR begins sending traffic to the RP as standard IP multicast packets, as well as encapsulated within Register messages. The RP temporarily receives packets twice. When the RP detects the normal multicast packets, it sends a Register-Stop message to the source DR, meaning it should stop sending register packets.

6. Sending Register-Stop Messages

   When the RP begins receiving traffic from the source, both as Register messages and as unencapsulated IP packets, it sends a Register-Stop message to the DR. This notifies the DR that the traffic is now being received as standard IP multicast packets on the SPT. When the DR receives this message, it stops encapsulating traffic in Register messages.

7. Pruning the Interface

   Routers attached to receivers send Prune messages to the RP to disassociate the source from the RP. When an RP receives a Prune message, it no longer forwards traffic from the source indicated in the Prune message. If all members of a multicast group are pruned, the IGMP state of the DR is deleted, and the interface is removed from the Source and Group lists of the group.

8. Forwarding Multicast Packets

   PIM-SM routers forward multicast traffic onto all interfaces that lead to receivers that have explicitly joined a multicast group. Messages are sent to a group address in the local subnetwork, and have a Time to Live (TTL) of one (1). The router performs an RPF check, and forwards the packet. If a downstream router has sent a join to this router or is a member of this group, then traffic that arrives on the correct interface is sent to all outgoing interfaces that lead to downstream receivers.

PIM-SM Configuration

PIM-SM is a soft-state protocol. The required steps to configure PIM-SM are the following:

- Enable IP multicast on each PIM router (see Enabling IP Multicast Routing)
- Enable PIM-SM on the desired interfaces (see Enable PIM-SM on an Interface)
- Configure the RP statically (see Configuring Rendezvous Point Statically or dynamically (see Configure Rendezvous Point Dynamically Using Bootstrap Router Method) depending on which method you use)

All multicast group states are dynamically maintained as the result of IGMP `Report/Leave` and PIM `Join/Prune` messages.

This section provides the steps to configure the PIM-SM feature. Configuration steps and examples are used for two relevant scenarios.

Topology

The following figure displays the network topology used in these examples.

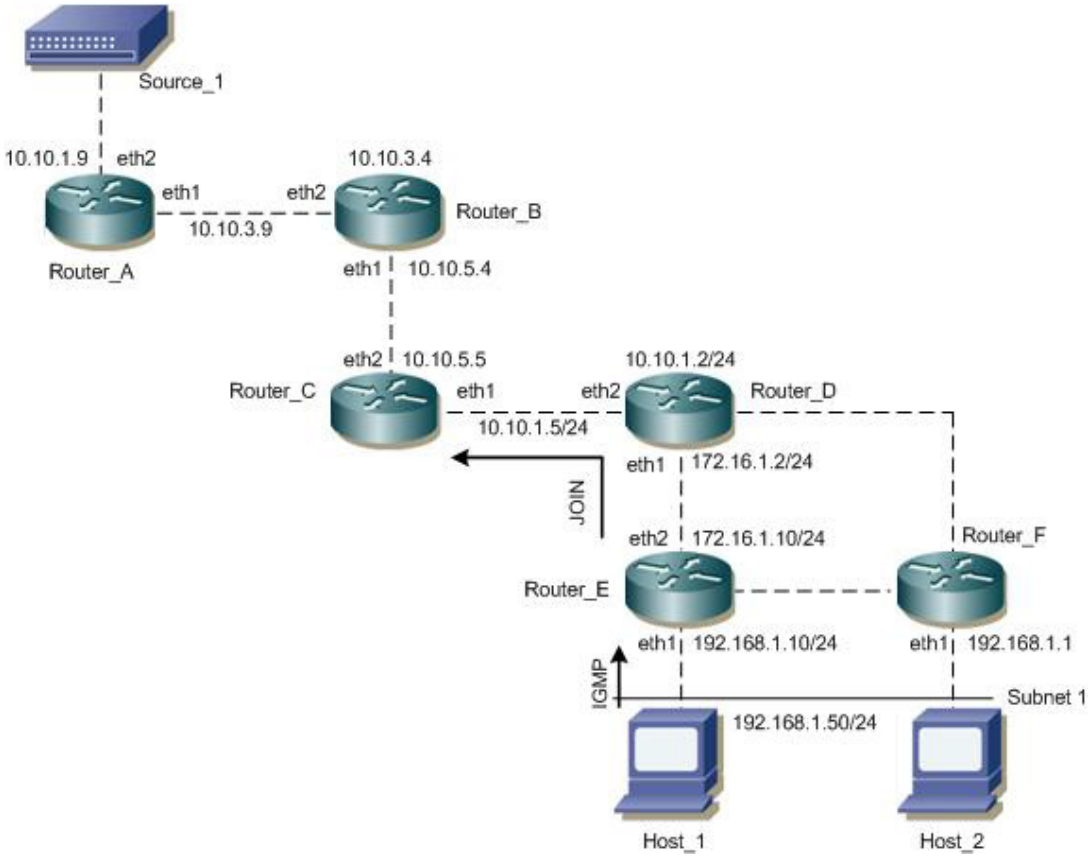


Figure 3-12: PIM-SM Topology

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

© 2021 IP Infusion Inc. Proprietary

Enable IP Multicast Routing

`#configure terminal`	Enter configure mode.
`(config)#ip multicast-routing`	Enable IP multicast routing.
`(config)#exit`	Exit Configure mode.

Enable PIM-SM on an Interface

Enable PIM-SM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM. In the following sample configuration, both eth1 and eth2 are enabled for PIM-SM on the router.

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to be configured and Enter interface mode.
`(config-if)#ip address 10.10.12.11/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim sparse-mode`	Enable PIM sparse mode on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to be configured and Enter interface mode.
`(config-if)#ip address 10.10.13.11/24`	Configure the IP address for `eth2`.
`(config-if)#ip pim sparse-mode`	Enable PIM sparse mode on the interface.
`(config-if)#exit`	Exit interface mode.

Configuring Rendezvous Point Statically

Every PIM multicast group needs to be associated with the IP address of a Rendezvous Point (RP), which is a router that resides in a multicast network domain. The address of the RP is used as the root of a group-specific distribution tree. All nodes in the domain that want to receive traffic sent to the group are aware of the address of the RP. For all senders to reach all receivers within a group, all routers in the domain must be able to map to the RP address configured for the group. There can be several RPs configured in a network deploying PIM-SM, each serving a different group.

You can statically configure a RP by specifying the RP address with in every router in the PIM domain. The use of statically configured RPs is ideal for small network environments or ones that do not require many RPs and/or require changing the assignment of the RPs often. Changing the assignment of an RP requires the re-configuration of the RP address in all of the routers in the PIM domain.

In static RP configurations, RP failover is not available.

When configuring the RP statically, do the following:

- On every router, include the `ip pim rp-address A.B.C.D` statement even if a router does not have any source or group member attached to it
- Assign only one RP address for a multicast group in the PIM domain

Using the topology depicted in Figure 3-12, `Router_C` is the RP, and all routers are statically configured with RP information. Host_1 and Host_2 join group 224.0.1.3 for all the sources. They send the IGMP membership report to Subnet 1. Two routers are attached to Subnet 1, `Router_E` and `Router_F`; both have default DR priority on `eth1`.

Since `Router_E` has a higher IP address on interface `eth1`, it becomes the Designated Router, and is responsible for sending Join messages to the RP (`Router_C`).

Configure Static RP

`#configure terminal`	Enter configure mode.
`(config)#ip pim rp-address 10.10.1.5`	Statically configure an RP address for multicast groups.
`(config)#exit`	Exit Configure mode.

Here is the sample configuration for `Router_D`:

```
hostname Router_D
!
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing

ip pim rp-address 10.10.1.5
!
```

Validation

Enter the commands listed in this section to confirm the previous configurations.

RP Details

At Router_D, the `show ip pim rp mapping` command shows that `10.10.1.5` is the RP for all multicast groups `224.0.0.0/4`, and is statically configured. All other routers will have a similar output:

```
R-D#show ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0


Group(s): 224.0.0.0/4, Static
    RP: 10.10.1.5
         Uptime: 00:19:31
R-D#
```

Override RP cnt: 0At Router_D, use the `show ip pim rp-hash` command to display the selected RP for a specified group (224.0.1.3):

```
Router_D#show ip pim rp-hash 224.0.1.3
RP: 10.10.1.5
```

 © 2021 IP Infusion Inc. Proprietary

Interface Details

The `show ip pim interface` command displays the interface details for `Router_E`, and shows that `Router_E` is the Designated Router on `Subnet 1`.

```
Router_E#show ip pim interface
Address          Interface VIFindex Ver/   Nbr      DR    DR
                                    Mode   Count   Prior
192.168.1.10      eth1      0       v2/S   1         1     192.168.1.10
172.16.1.10       eth2      2       v2/S   1         1     172.16.1.10
```

IP Multicast Routing Table

Note: The multicast routing table displays for an RP router are different from other routers.

The `show ip pim mroute` command displays the IP multicast routing table. In this table, the following fields are defined:

```
R-E#show ip pim mroute
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
 Local     i.............................
 Joined    .............................
 Asserted  .............................
FCR:

R-E#
```

At `Router_E`, `eth2` is the incoming interface of the (*, G) entry, and `eth1` is on the outgoing interface list of the (*, G) entry. This means that there is a group member through `eth1`, and the RP is reachable through `eth2`.

The 0 position on this 32-bit index is for `eth1` (as illustrated in the interface display above). The `j` on the 0 index indicates that the `Join` has come from `eth1`.

Since `Router_C` is the RP, and the root of this multicast tree, the `show ip pim mroute` command on `Router_C` shows `RPF nbr` as 0.0.0.0 and `RPF idx` as none.

```
R-C#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 224.0.1.3)
```

```
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..............................
 Joined    j..............................
 Asserted  ..............................
FCR:

R-C#
```

Configure Rendezvous Point Dynamically Using Bootstrap Router Method

A static RP configuration works for a small, stable PIM network domain; however, it is not practical for a large and/or complex one. In such a network, if the RP fails or you have to change the assignment of the RP, you are required to reconfigure the static configurations on all PIM routers. Also, if you have several multicast groups mapped to several RPs, there are many repetitive configurations you are required to perform, which can be time consuming and laborious. Thus when it comes configuring RP in large and/or complex networking environments, configuring it dynamically is the best and most scalable method to use. Bootstrap router (BSR) configuration is one method of configuring the RP dynamically.

The BSR mechanism in a PIM domain uses the concept of a RP as a way for receivers to discover the sources that send to a particular multicast group. The BSR mechanism gives a way for a multicast router to learn the set of group-to-RP mappings required in order to function. The BSR's function is to broadcast the RP set to all routers in the domain.

Some of the PIM routers within a PIM domain are configured as Candidate-RPs (C-RPs). A subset of the C-RPs is eventually used as the actual RPs for the domain. An RP configured with a lower value in the priority field has a higher priority.

Some of the PIM routers in the domain are configured to be Candidate-BSRs (C-BSR). One C-BSR is selected to be the BSR for the domain, and all PIM routers in the domain learn the result of this election through Bootstrap messages (BSM). The C-BSR with highest value in the priority field is elected to be the BSR. The C-RPs then report their candidacies to the elected BSR, which chooses a subset of the C-RPs, and distributes corresponding group-to-RP mappings to all the routers in the domain using Bootstrap messages.

This section provides 2 examples to illustrate the BSR configuration for configuring RP dynamically.

Example 1

For this example, refer to Figure 1 for the topology.

To dynamically configure the RP, `Router_C` on `eth1` and `Router_D` on `eth1` are configured as a Candidate RP using the `ip pim rp-candidate` command. `Router_D` on `eth1` is also configured as the Candidate BSR. Since no other router has been configured as the candidate BSR, `Router_D` becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

The highest priority router (configured with lowest priority value) is chosen as the RP. If two or more routers have the same priority, a hash function in the BSR mechanism is used to choose the RP to ensure that all routers in the PIM-domain have the same RP for the same group.

To change the default priority of any candidate RP, use the `ip pim rp-candidate IFNAME PRIORITY` command. At `Router_D`, the `show ip pim rp mapping` command shows that `Router_C` is chosen as the RP for a specified group.

 © 2021 IP Infusion Inc. Proprietary

Configure RP Dynamically for Router C

`#configure terminal`	Enter configure mode.
`(config)#ip pim rp-candidate eth1 priority 2`	Give this router the candidate RP status using the IP address of the specified interface.

Configure RP Dynamically for Router D

`#configure terminal`	Enter configure mode.
`(config)#ip pim bsr-candidate eth1`	Give this router the candidate BSR status using the name of the interface.
`(config)#ip pim rp-candidate eth1 priority 2`	Give this router the candidate RP status using the IP address of the specified interface.

The following output displays the complete configuration at `Router_C` and `Router_D`:

```
Router_D#show running-config
!
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
ip multicast-routing
ip pim bsr-candidate eth1
ip pim rp-candidate eth1 priority 2
!

Router_C#show running-config
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing
ip pim rp-candidate eth1
```

Validation

This section provides the steps to verify the RP configuration.

PIM Group-to-RP Mappings

The `show ip pim rp mapping` command displays the group-to-RP mapping details and displays information about RP candidates. There are two RP candidates for the group range, 224.0.0.0/4. RP Candidate 10.10.1.5 has a default priority of 192, whereas, RP Candidate 172.16.1.2 has been configured to have a priority of 2. Since RP candidate 172.16.1.2 has a higher priority, it is selected as RP for the multicast group, 224.0.0.0/4.

```
R-D#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
  RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap, priority 2
         Uptime: 00:02:24, expires: 00:02:11
  RP: 10.10.1.5
    Info source: 10.10.1.5, via bootstrap, priority 2
         Uptime: 00:02:26, expires: 00:02:06
Override RP cnt: 0


Group(s): 224.0.0.0/4, Static
    RP: 10.10.1.5
         Uptime: 00:55:25
R-D#
```

RP Details

To display information about the RP router for a particular group, use the following command. This output displays that 172.16.1.2 has been chosen as the RP for the multicast group 224.0.1.3.

```
Router_D#show ip pim rp-hash 224.0.1.3
Group(s): 224.0.0.0/4
    RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap
```

After RP information reaches all PIM routers in the domain, various state machines maintain all routing states, as a result of Join/Prune from group membership. To display information on interface details and the multicast routing table, refer to the *Configuring Rendezvous Point Statically* section.

Example 2

To dynamically configure the RP, `Router_2` on `eth1` is configured as a Candidate RP using the `ip pim rp-candidate` command. Since no other router is configured as C-RP, `Router_2` becomes the RP. `Router_1` on `eth1` and `Router_2` on `eth1` are configured as the Candidate BSRs. Since `Router_1` has a higher priority value than `Router_2`, `Router_1` becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

Topology

For this example, refer to Figure 3-13 for the topology.

© 2021 IP Infusion Inc. Proprietary

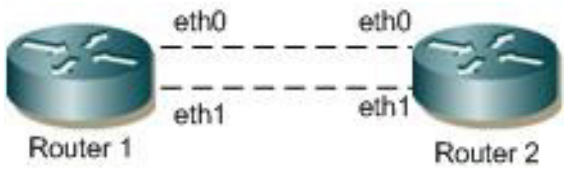


Figure 3-13: Boostrap Router Topology

Configuration

Router 1

`#configure terminal`	Enter configure mode.
`(config)#ip pim bsr-candidate eth1`	Configure `eth1` of Router 1 as C-BSR. The default priority is 64, so it is not necessary to designate a priority.
`(config)#exit`	Exit Configure mode.

Router 2

`#configure terminal`	Enter configure mode.
`(config)#ip pim bsr-candidate eth1 10 25`	Configure `eth1` of Router 2 as C-BSR with a hash mask length of 10, and a priority of 25.
`(config)#ip pim rp-candidate eth1 priority 0`	Configure interface `eth1` as C-RP with a priority of 0.
`(config)#exit`	Exit Configure mode.

Router 2 Unicast BSM

When the `ip pim unicast-bsm` command is configured on an interface that is a DR for a network, then that interface unicasts the stored copy of BSM to the new or rebooting router.

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ip pim dr-priority 10`	Configure `eth1` as DR
`(config-if)#ip pim unicast-bsm`	Enable sending and receiving of Unicast BSM for backward compatibility.
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the C-BSR state on Router 1.

```
#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 20.0.1.21
  Uptime:      00:01:39, BSR Priority: 64, Hash mask length: 10
  Next bootstrap message in 00:00:53
  Role: Candidate BSR
```

```
  State: Elected BSR
```

2. Verify the C-BSR state on Router 2.

   The initial state of C-BSR is P-BSR before transitioning to C-BSR. The two states are illustrated in the sample outputs from the `show ip pim bsr-router` command below.

```
#show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 20.0.1.21
  Uptime:      00:02:39, BSR Priority: 64, Hash mask length: 10
  Expires:     00:00:03
  Role: Candidate BSR
  State: Pending BSR

#show ip pim bsr-router
PIMv2 Bootstrap information
 BSR address: 20.0.1.21
 Uptime:      00:40:20, BSR Priority: 64, Hash mask length: 10
 Expires:     00:02:07
 Role: Candidate BSR
 State: Candidate BSR
Candidate RP: 20.0.1.11(eth2)
    Advertisement interval 60 seconds
    Next C-RP advertisement in 00:00:02
    Backoff cnt 1

#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
  RP: 20.0.1.11
    Info source: 20.0.1.21, via bootstrap, priority 0
         Uptime: 00:02:17, expires: 00:02:26
Override RP cnt: 0
```

3. Verify RP-set information on E-BSR.

```
R1#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
  RP: 20.0.1.11
    Info source: 20.0.1.11, via bootstrap, priority 0
         Uptime: 00:00:22, expires: 00:02:12
Override RP cnt: 0
```

4. Verify RP-set information on C-BSR.

```
ARP1#show ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0

Anycast-RP  1.1.1.152 members :
  4.4.4.5   7.7.7.1   23.23.23.1
```


© 2021 IP Infusion Inc. Proprietary

```
Group(s): 224.0.0.0/4, Static
    RP: 1.1.1.152
         Uptime: 00:00:37
ARP1#
```

Anycast-RP Configuration

The Anycast-RP feature provides load balancing among active RPs and redundancy in a PIM-SM network domain. In a PM-SM configuration, only a single active RP for each multicast group within a domain is permitted. However, in an Anycast-RP configuration, this restriction is removed with the support of multiple active RPs for each group in a domain.

OcNOS supports Anycast-RP using the PIM implementation. In PIM Anycast-RP, Multicast Source Discovery Protocol (MSDP) is not employed to share information about active sources. Instead the Register mechanism in PIM is extended to provide this same function.

The following describes Anycast-RP in PIM-SM:

- A Unicast IP address is used as the RP address. The address is statically configured, and associated with all PIM routers throughout the domain.
- A set of routers in the domain is chosen to act as RPs for this RP address. These routers are called the Anycast-RP set.
- Each router in the Anycast-RP set is configured with a loopback address. The loopback address is configured on all RPs for the loopback interface, then configured as the RP address (static RP), and injected into OSPF using redistribute connected. The PIM-SM implementation uses only the first non-loopback address configured on the loopback interface. Therefore, it is important to be sure that the Anycast-RP address is configured with the first non-loopback address.
- Each router in the Anycast-RP set also needs a separate IP address, which is used for communication between the RPs.
- The RP address, or a prefix that includes the RP address, is injected into the unicast routing system inside the domain.
- Each router in the Anycast-RP set is configured with the addresses of all other routers in the Anycast-RP set. This must be consistently configured in all RPs in the set.h

Topology

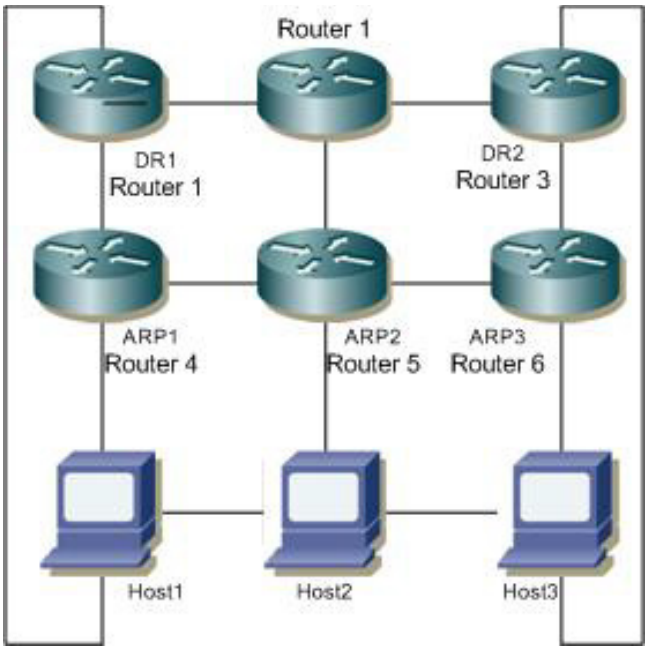


Figure 3-14: Anycast RP Topology

Host1 and Host3 act as hosts and sources for sending join and multicast data packets; Host2 acts as a host.

ARP1, ARP2 and ARP3

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter the loopback interface.
`(config-if)#ip address 1.1.1.152/32 secondary`	Configure the IP address for loopback
`(config-if)#exit`	Exit the Configure mode.
`(config)#ip pim rp-address 1.1.1.152`	Configure the static RP with the address of the loopback.
`(config)#ip pim anycast-rp 1.1.1.152 4.4.4.5`	Configure the member RP address. In this example, `4.4.4.5` is the member RP in ARP2. It is the address used for communication between all RPs.
`(config)#ip pim anycast-rp 1.1.1.152 7.7.7.1`	Configure the member RP address. In this example, `7.7.7.1` is the member RP in ARP3. It is the address used for communication between all RPs.
`(config)#ip pim anycast-rp 1.1.1.152 23.23.23.1`	Configure the member RP address. In this example, `23.23.23.1` is the member RP in ARP1. It is the address used for communication between all RPs.
`(config)#exit`	Exit the Configure mode.

Disable Anycast-RP

`#configure terminal`	Enter configure mode.
`(config)#no ip pim anycast-rp 1.1.1.152`	Disable Anycast-RP.

© 2021 IP Infusion Inc. Proprietary

(config)#no ip pim rp-address 1.1.1.152	Disable static RP.
(config)#exit	Exit Configure mode.

Validation

1. Verify RP-mapping in ARP1.

```
#show ip pim rp mapping
      PIM Group-to-RP Mappings
      Override RP cnt: 0
      Anycast-RP 1.1.1.152 members:23.23.23.1
      Group(s): 224.0.0.0/4, Static
      RP: 1.1.1.152
        Uptime: 00:00:13s
```

2. Verify RP-mapping in ARP1 after disabling anycast-RP and RP-address.

```
ARP1#show ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0

Anycast-RP  1.1.1.152 members :
  4.4.4.5   7.7.7.1   23.23.23.1

Group(s): 224.0.0.0/4, Static
    RP: 1.1.1.152
         Uptime: 00:00:37
ARP1#
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 PIM Dense Mode Configuration

Protocol Independent Multicast - Dense Mode (PIM-DM) is a data-driven multicast routing protocol that builds source-based multicast distribution trees that operate on the flood-and-prune principle. PIM-DM requires unicast-reachability information, but it does not depend on a specific unicast routing protocol.

Terminology

Following is a brief description of terms and concepts used to describe the PIM-DM protocol:

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only when `IF1` is the interface the router would use in order to reach `SourceA`. It determines whether the interface is correct by consulting its unicast routing tables. The packet that arrives through interface `IF1` is forwarded because the routing table lists this interface as the shortest path to the network. The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link once in each direction.

Forwarding Multicast Packets

PIM-DM routers forward multicast traffic to all interfaces that lead to receivers that have explicitly joined a multicast group. Messages are sent to a group address in the local subnetwork. The router performs an RPF check, and forwards the packet. Traffic that arrives on the correct interface is sent to all outgoing interfaces that lead to downstream receivers, if the downstream router is a member of this group.

Upstream

Upstream traffic is traffic that is going towards the source.

Downstream

Downstream traffic is anything other than the upstream interface for that group.

Nexthop

PIM-DM does periodic lookups for prefixes to check router reachability. The nexthop lookup mechanism avoids periodic lookup. During start-up, PIM-DM notifies NSM (Network Services Manager) about the prefixes that pertain to them. NSM notifies the protocols if a better nexthop is available, or if a nexthop becomes unavailable. In this way, PIM-DM does not expend resources to do periodic lookups, because NSM is proactive in their maintenance.

Configuration

Configuring PIM-DM requires the following steps:

- Enable IP multicast on each PIM router (see Enabling IP Multicast Routing)

- Enable PIM-DM on the desired interfaces (see Enabling PIM-DM)

This section provides the configuration steps for configuring PIM-DM and examples for a relevant scenario.

Topology

In this network topology, the Source_1 address is 10.10.1.52 and the group address is set to 224.0.1.3.

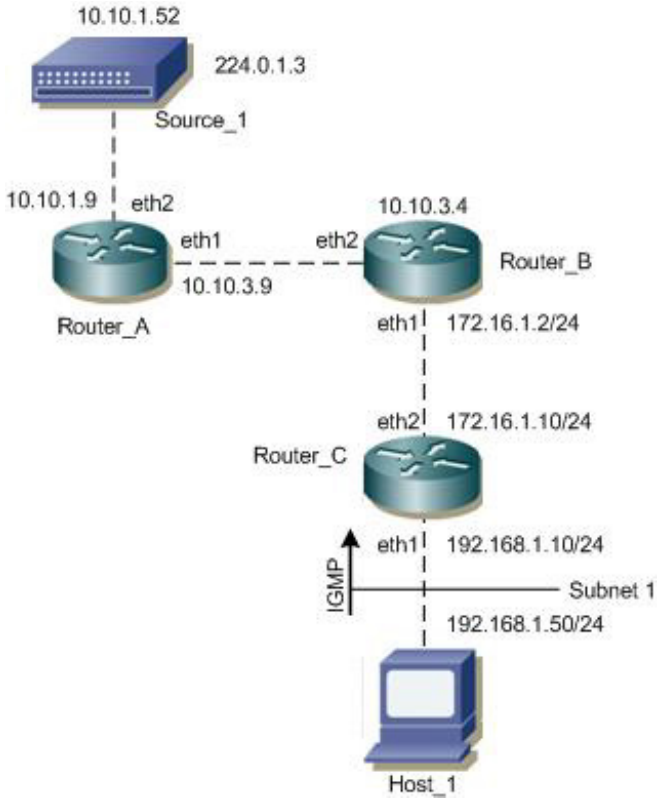


Figure 4-15: PIM-DM Configuration Topology

In this example, all routers are running PIM-DM.

1. Host_1 sends an IGMP membership report to Subnet 1.
2. After Router_C receives this report, it associates its receiving interface, `eth1`, with the group reported in the IGMP message, for example, group1.
3. Source_1 then sends a data packet for group1.
4. Every router creates an (S,G) entry in the multicast routing table.
5. When the data packet reaches `Router_C`, it forwards via the interface, `eth1`, because there is a local member on this interface for this group. `Router_C` has a downstream receiver, so it does not send a prune message to its upstream neighbor router, `Router_B`.

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

© 2021 IP Infusion Inc. Proprietary

`#configure terminal`	Enter configure mode.
`(config)#ip multicast-routing`	Enable IP multicast routing.
`(config)#exit`	Exit Configure mode.

Enabling PIM-DM

Enable PIM-DM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM.

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 10.10.15.12/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim dense-mode`	Enable PIM dense mode on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 10.10.14.12/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim dense-mode`	Enable PIM dense mode on the interface.
`(config-if)#exit`	Exit interface mode.

The following is a sample configuration for `Router_C`:

```
hostname Router_C
!
interface eth0
!
interface eth1
 ip pim dense-mode
!
interface eth2
 ip pim dense-mode
!
interface lo
!
!
ip multicast-routing
!
```

Validation

The `show ip pim interface` command displays the interface details for `Router_C`.

```
Router_C#show ip pim interface
Address          Interface VIFindex Ver/   Nbr     DR
                                    Mode   Count   prior
192.168.1.10      eth1      0       v2/D   0        1
172.16.1.10       eth2      2       v2/D   1        1
```

The `show ip mroute` command displays the IP multicast routing table.

```
Router_C#show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:00:15
Owner PIM-DM, Flags: F
 Incoming interface: eth2
 Outgoing interface list:
    eth1 (1)
```

The `show ip pim mroute` displays the IP PIM-DM multicast routing table.

```
Router_C#show ip pim mroute
PIM-DM Multicast Routing Table
(10.10.1.52, 224.0.1.3)
 RPF Neighbor: 172.16.1.2, Nexthop: 172.16.1.2, eth2
 Upstream IF: eth2
    Upstream State: Forwarding
    Assert State: NoInfo
 Downstream IF List:
    eth1, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 IGMP Snooping Configuration

This chapter describes how to configure Internet Group Management Protocol (IGMP) Snooping.

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Without IGMP, Layer-2 switches handle IP multicast traffic in the same manner as broadcast traffic and forwards frames received on one interface to all other interfaces. This creates excessive traffic on the network, and affects network performance. IGMP Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic. Only one membership report is relayed from a group, instead of a report from each host in the group. To achieve this, IGMP Snooping is enabled on the switches.

Topology

This example describes the configuration on switch S1. The eth1 interface is configured as a multicast router port.

Because IGMP Snooping is used in bridged LAN environments, router R1 does not require running IGMP Snooping, and can run any multicast protocol (such as PIM-SM). Thus, the configuration on R1 is not included in this example.

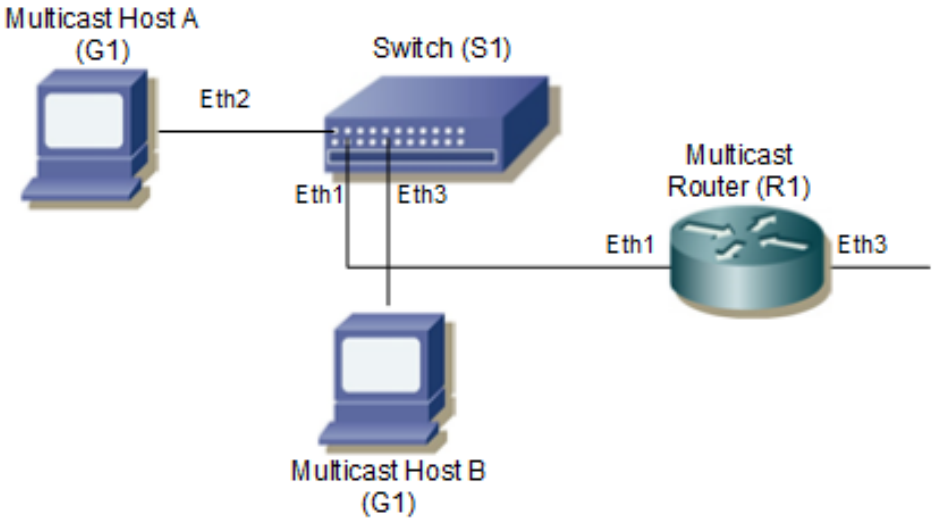


Figure 5-16: IGMP Snooping Topology

As a result of this configuration:

- The switch itself replies with membership report messages in response to queries received on interface eth1. However, if you do not enable report suppression on the switch, when it receives an IGMP Query message on eth1, it forwards it to both Host A and Host B. As a result, both hosts reply with a Membership report (as Layer-2 IGMP is running on the hosts).
- Because Host A and Host B are members of the same multicast group, the router is not notified when A leaves the group, because the group still has another member. When Host B leaves the group, the switch will send a Leave message to the Router with the destination address as 224.0.0.2 (All Router Destination Address).

Configuration

To enable IGMP Snooping on an interface:

1. Add a bridge to the spanning-tree table

2. Specify the interface to be configured
3. Associate the interface with bridge group
4. IGMP snooping will be enabled by default
5. Configure ports that are connected to routers as multicast router ports
6. By default, IGMP report suppression is enabled on the switch

S1

`#configure terminal`	Enter the `Configure` mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Add bridge `1` to the spanning-tree table.
`(config)#vlan database`	enter VLAN mode
`(config-vlan)# vlan 2 bridge 1`	Create VLAN and add it to bridge 1
`(config)#exit`	Exit VLAN mode
`(config)#interface eth3`	Specify the interface `eth3` to be configured, and Enter interface mode.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate the interface `eth1` with bridge-group `1`.
`(config-if)#switchport mode trunk`	Configure the port as an trunk port.
`(config-if)#switchport trunk allowed vlan all`	Add VLAN to trunk
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Specify interface `eth1` to be configured.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate interface `eth1` with bridge-group `1`.
`(config-if)#switchport mode trunk`	Configure the port as an trunk port.
`(config-if)#switchport trunk allowed vlan all`	Add VLAN to trunk
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Specify interface `eth2` to be configured.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate interface `eth2` with bridge-group `1`.
`(config-if)#switchport mode trunk`	Configure the port as an trunk port.
`(config-if)#switchport trunk allowed vlan all`	Add VLAN to trunk
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface vlan1.2`	Specify interface `vlan1.1` to be configured.
`(config)#ip address 1.2.3.4/24`	Specify IP address

© 2021 IP Infusion Inc. Proprietary

(config-if)# igmp snooping mrouter interface eth1	Configure this port as a multicast router port
(config-if)#exit	Exit interface mode

Validation

```
#show running-config interface eth3
!
interface eth3
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan add 2

#show running-config interface eth1
!
interface eth1
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan add 2

#show running-config interface eth2
!
interface eth2
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan add 2

#show igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan Group/Source Address Interface Flags Uptime Expires Last Reporter Version
2 224.1.1.1 eth3 R 00:00:03 00:04:17 0.0.0.0 V3
2 224.1.1.1 eth2 R 00:00:03 00:04:17 0.0.0.0 V3

#show igmp snooping interface vlan1.2
IGMP Snooping information for vlan1.2
IGMP Snooping enabled
Snooping Querier none
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression enabled
IGMPv3 Report suppression enabled
Router port detection using IGMP Queries
Number of router-ports: 1
Number of Groups: 1
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0
Number of v3-reports: 2
Active Ports:
Eth3
Eth1
```

```
    Eth2
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 6 MSDP Configuration

Multicast Source Discovery Protocol (MSDP) is used to exchange multicast source information between BGP-enabled PIM-SM domains. Using MSDP, routers in a PIM-SM domain can rely on their own RP to reach a source in a different PIM-SM domain.

Overview

MSDP routers in a PIM-SM domain have a MSDP peering relationship with MSDP peers in another domain using a TCP connection. MSDP peering is the first step towards exchanging inter-domain multicast source information using MSDP SA (Source-Active) messages.

When an RP in a PIM-SM domain first learns of a new sender (via PIM register messages), it constructs an SA message and sends it to its MSDP peers.

All RPs which intend to originate or receive SA messages must establish MSDP peering with other RPs, either directly or via an intermediate MSDP peer.

An SA message contains these fields:

- Source address of the data source
- Group address the data source sends to
- IP address of the RP

Each SA message received from a MSDP peer goes through an RPF check. The peer-RPF check compares the RP address carried in the SA message with the MSDP peer from which the message was received:

- If the MSDP peer receives an SA from a non-RPF peer towards the originating RP, it drops the message.
- Otherwise, it forwards the message to all its MSDP peers (except the one from which it received the SA message).

When an RP receives a new SA message from a peer in another domain, it checks if there are any receivers interested in the traffic. An RP checks for a (*, G) entry with a non-empty outgoing list. If the outgoing list is non-empty, the RP sends a (S,G) join towards the source.

Caching SA state

If a member joins a group soon after a SA message is received by the local RP, that member needs to wait until the next SA message to learn about the source. MSDP SA caching is done at MSDP peers to reduce join latency for new receivers. The SA cache is populated as soon an MSDP peer receives a SA message from its peer.

MSDP Mesh Group

MSDP Mesh groups are used inside a PIM-SM domain to ease RPF checking and SA forwarding within the domain. Any SA messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group. This reduces SA message flooding and simplifies peer-RPF flooding.

© 2021 IP Infusion Inc. Proprietary

MSDP Default Peer

An MSDP default peer is used when MSDP peers are not BGP peers. SA messages coming from a default peer do not go through an RPF check and are always accepted.

Configure PIM-SM

For the MSDP topology in Figure 6-17, you must enable PIM-SM on all the routers in both PIM domains and make RTR-1 a rendezvous point (RP) in Domain-1 and RTR-2 an RP in Domain-2. For the steps to configure PIM-SM and RPs, see Chapter 3, *PIM Sparse Mode Configuration*.

Configure MSDP

In the topology in Figure 6-17, an MSDP session is established between RTR-1 and RTR-2 in both domains. The following sample configuration on RTR-1 shows how to enable MSDP peering between RTR-1 and RTR-2.

Topology

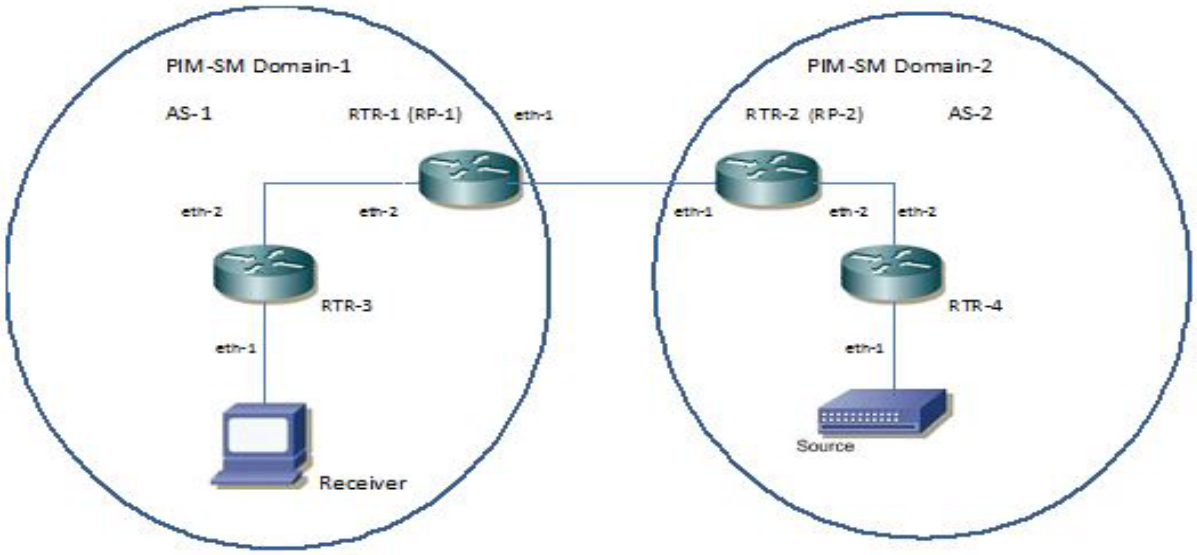


Figure 6-17: MSDP topology

IP addresses:

- RTR-1 eth1: 11.1.1.11
- RTR-1 eth2: 10.1.1.11
- RTR-2 eth1: 11.1.1.12
- RTR-2 eth2: 12.1.1.12
- RTR-4 eth1: 12.1.1.14
- RTR-4 eth2: 20.1.1.14

© 2021 IP Infusion Inc. Proprietary

RTR-3 eth1: 13.1.1.13

RTR-3 eth2: 10.1.1.13

Source: 20.1.1.10

Multicast group: 224.1.1.1

RTR-1

`#configure terminal`	Enter configure mode.

`(config)#ip msdp peer 11.1.1.12`
--or--
`(config)#ip msdp peer 11.1.1.12 connect source eth1`
	Configure a MSDP peer.
	
	Use the connect-source option to specify the primary IP address of the interface to use as the source IP address of the MSDP TCP connection.

`(config)#ip msdp password myPass peer 11.1.1.12`	Configure an MSDP password for the peer. You must specify the same command at RTR-2. The password must match at both the routers.
`(config)#ip msdp default-peer 11.1.1.12`	Configure MSDP default peer.
`(config)#ip msdp mesh-group mesh1 11.1.1.12`	Configure MSDP mesh group.
`(config)#ip msdp originator-id eth2`	Configure MSDP originator identifier.
`(config)#exit`	Exit configure mode.

Validation

RTR-1

```
#show running-config
!
!Last configuration change at 06:54:59 EDT Tue May 28 2019 by ocnos
!
no service password-encryption
!
hostname RTR1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
feature telnet
ssh login-attempts 0
ssh server port 39681568
no feature ssh
snmp-server enable snmp
snmp-server view all .1 included
feature ntp
ntp enable
username ocnos role network-admin password encrypted $1$wOL9u7T.$YENa7qmmtL3zWMXKBWSKw/
feature rsyslog
```

```
ip msdp peer 11.1.1.12
ip msdp default-peer 11.1.1.12
ip msdp mesh-group mesh1 11.1.1.12
ip msdp password myPass peer 11.1.1.12
ip msdp originator-id eth2
!
ip multicast-routing
!
ip pim bsr-candidate eth2
ip pim rp-candidate eth2
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 mtu 65536
!
interface eth0
 ip address 192.168.52.3/24
!
interface eth1
 ip address 11.1.1.11/24
 ip pim bsr-border
 ip pim sparse-mode
!
interface eth2
 ip address 10.1.1.11/24
 ip pim sparse-mode
!
interface eth3
 shutdown
!
router ospf 100
 network 10.1.1.0/24 area 0.0.0.0
 cspf disable-better-protection
!
router bgp 1
 neighbor 11.1.1.12 remote-as 2
!
line con 0
 login
line vty 0 39
 login
!
end
```

This command shows the MSDP peer information at RTR-1:

```
#show ip msdp peer
MSDP Peer 11.1.1.12
Connection status
 State: Up (Established)
```

 © 2021 IP Infusion Inc. Proprietary

```
 Keepalive sent: 1
 Keepalive received: 1
 Number of connect retries: 0
```

In the MSDP topology in Figure 6-17, when a source sends multicast traffic for group 224.1.1.1, RTR-4 (the DR) sends a register packet towards RTR-2 which is the RP in the domain. RTR-2 receives the register packet and sends an MSDP SA message to its MSDP peer (RTR-1). RTR-1 receives the SA message and creates an entry in the SA cache containing the source, group, and RP information.

This command at RTR-1 shows the SA information with source address, group address, and RP address:

```
#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(20.1.1.11, 224.1.1.1), RP 12.1.1.12, 00:00:14/00:03:16
#
```

RTR-3 receives an IGMP join for group 224.1.1.1 and joins the shared tree path toward the RP (RTR-1).

When RTR-1 receives an SA message from RTR-2, because it has a receiver, it sends an (S,G) join towards the source. Now traffic from the source is received at RTR-1 via the shortest path tree formed between RTR-1 and the source. RTR-1 distributes traffic downstream towards the receiver.

This command shows the PIM state at RTR-1 upon receiving an SA message and joining towards the source:

```
#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0

(*, 224.1.1.1)
RP: 10.1.1.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..............................
 Joined    ..j...........................
 Asserted  ..............................
FCR:

(20.1.1.10, 224.1.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 0
Upstream State: JOINED
 Local     ..............................
 Joined    ..............................
 Asserted  ..............................
 Outgoing  ..o...........................

(20.1.1.10, 224.1.1.1, rpt)
```

```
RP: 10.1.1.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: NOT PRUNED
--More--  Local     ..............................
 Pruned    ..............................
 Outgoing  ..o...........................


#sh ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(20.1.1.11, 224.1.1.1), RP 12.1.1.12, 00:00:14/00:03:16
#
```

RTR-2

```
#show running-config
!
!Last configuration change at 13:58:59 EDT Mon May 27 2019 by ocnos
!
no service password-encryption
!
hostname RTR2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
feature telnet
no feature ssh
snmp-server enable snmp
snmp-server view all .1 included
feature ntp
ntp enable
username ocnos role network-admin password encrypted $1$wOL9u7T.$YENa7qmmtL3zWMXKBWSKw/
feature rsyslog
ip msdp peer 11.1.1.11
ip msdp default-peer 11.1.1.11
ip msdp mesh-group mesh1 11.1.1.11
ip msdp password myPass peer 11.1.1.11
ip msdp originator-id eth2
!
ip multicast-routing
!
ip pim bsr-candidate eth2
ip pim rp-candidate eth2
!
interface lo
 ip address 127.0.0.1/8
```

 © 2021 IP Infusion Inc. Proprietary

```
--More--  ipv6 address ::1/128
 mtu 65536
!
interface eth0
 ip address 192.168.52.2/24
!
interface eth1
 ip address 11.1.1.12/24
 ip pim bsr-border
 ip pim sparse-mode
!
interface eth2
 ip address 12.1.1.12/24
 ip pim sparse-mode
!
interface eth3
 shutdown
!
router ospf 200
 network 12.1.1.0/24 area 0.0.0.0
 cspf disable-better-protection
!
router bgp 2
 neighbor 11.1.1.11 remote-as 1
!
line con 0
 login
line vty 0 39
 login
!
end
```

This command shows the MSDP peer information at RTR-2.

```
#show ip msdp peer
MSDP Peer 11.1.1.11
  Connection status
   State: Up (Established)
   Keepalive sent: 15
   Keepalive received: 17
#
```

RTR-3

```
#show running-config
!
!Last configuration change at 14:07:38 EDT Mon May 27 2019 by ocnos
!
no service password-encryption
```

```
!
hostname RTR3
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
feature telnet
ssh login-attempts 0
ssh server port 40574496
no feature ssh
snmp-server enable snmp
snmp-server view all .1 included
feature ntp
ntp enable
username ocnos role network-admin password encrypted $1$wOL9u7T.$YENa7qmmtL3zWMXKBWSKw/
feature rsyslog
!
ip multicast-routing
!
ip pim rp-address 10.1.1.11
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 mtu 65536
!
interface eth0
--More--  ip address 192.168.52.6/24
!
interface eth1
 ip address 13.1.1.13/24
 ip pim sparse-mode
!
interface eth2
 ip address 10.1.1.13/24
 ip pim sparse-mode
!
interface eth3
 shutdown
!
interface eth4
 shutdown
!
router ospf 100
 network 10.1.1.0/24 area 0.0.0.0
 cspf disable-better-protection
!
line con 0
```


© 2021 IP Infusion Inc. Proprietary

```
 login
line vty 0 39
 login
!
end


#sh ip igmp bgr
IGMP Connected Group Membership
Group Address    Interface            Uptime     Expires   State    Last Reporter
224.1.1.1        eth1                 16:58:51   00:03:39  Active   13.1.1.11
#
```

RTR-4

```
#show running-config
!
!Last configuration change at 13:57:34 EDT Mon May 27 2019 by ocnos
!
no service password-encryption
!
hostname RTR4
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
feature telnet
ssh login-attempts 0
ssh server port 20761744
no feature ssh
snmp-server enable snmp
snmp-server view all .1 included
feature ntp
ntp enable
username ocnos role network-admin password encrypted $1$ypBh3Wo/$4Fq/DbkFF/UWeA7YnTYMm1
feature rsyslog
!
ip multicast-routing
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 mtu 65536
!
interface eth0
 ip address 192.168.52.5/24
!
--More-- interface eth1
```

```
 ip address 20.1.1.14/24
 ip pim sparse-mode
!
interface eth2
 ip address 12.1.1.14/24
 ip pim sparse-mode
!
interface eth3
 shutdown
!
router ospf 200
 network 12.1.1.0/24 area 0.0.0.0
 cspf disable-better-protection
!
line con 0
 login
line vty 0 39
 login
!
end
```


© 2021 IP Infusion Inc. Proprietary

Multicast Routing Information Base Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Multicast Commands*
- Chapter 2, *L3 IGMP Multicast Commands*
- Chapter 3, *MLD Multicast Commands*
- Chapter 3, *L2 IGMP Snooping Multicast Commands*
- Chapter 5, *L2 MLD Snooping Commands*
- Chapter 4, *PIMv4 Commands*
- Chapter 7, *PIMv6 Commands*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Multicast Commands

OcNOS multicast protocol modules work with the Multicast Routing Information Base (MRIB).

- clear ip mroute
- debug ip mrib
- ip mroute
- ip multicast route-limit
- ip multicast ttl-threshold
- ip multicast-routing
- ipv6 mroute
- show debugging ip mrib
- show ip mroute
- show ip mvif
- show running-config interface multicast
- show running-config interface multicast

© 2021 IP Infusion Inc. Proprietary

clear ip mroute

Use this command to delete entries from the IP multicast routing table. This command clears the multicast route entries in the multicast route table and removes the entries from the multicast forwarder. MRIB sends a clear message to the multicast protocols. Each multicast protocol has its own clear multicast route command. The protocol-specific clear command clears multicast routes from the protocol and clears the routes from the MRIB.

Command Syntax

```
clear ip mroute *
clear ip mroute A.B.C.D
clear ip mroute A.B.C.D A.B.C.D
clear ip mroute statistics *
clear ip mroute statistics A.B.C.D
clear ip mroute statistics A.B.C.D A.B.C.D
clear ip mroute A.B.C.D pim sparse-mode
clear ip mroute A.B.C.D A.B.C.D pim (dense mode| sparse-mode)
clear ip mroute (vrf NAME|) *
clear ip mroute (vrf NAME|) A.B.C.D
clear ip mroute (vrf NAME|) A.B.C.D A.B.C.D
clear ip mroute (vrf NAME|) statistics *
clear ip mroute (vrf NAME|) statistics A.B.C.D
clear ip mroute (vrf NAME|) statistics A.B.C.D A.B.C.D
clear ip mroute (vrf Name|) A.B.C.D pim sparse-mode
clear ip mroute (vrf Name|) A.B.C.D A.B.C.D pim (dense-mode | sparse-mode)
```

Parameters

`*`	All multicast routes.
`A.B.C.D`	Group IP address.
`A.B.C.D`	Source IP address.
`vrf`	VRF name.
`statistics`	Multicast route statistics.
`dense-mode`	Dense Mode (PIM-DM).
`sparse-mode`	sparse Mode (PIM-SM)

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip mroute vrf VRF_A 225.1.1.1 3.3.3.3
```


© 2021 IP Infusion Inc. Proprietary

debug ip mrib

Use this command to set debug options for IPv4 multicast.

Use the `no` parameter with this command to disable debugging IPv4 multicast.

Command Syntax

```
debug ip mrib (all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-msg|mtrace|mtrace-detail)
debug ip mrib (vrf NAME|)(all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-msg|mtrace|mtrace-detail)
no debug ip mrib (all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-msg|mtrace|mtrace-detail)
no debug ip mrib (vrf NAME|) ((all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-msg|mtrace|mtrace-detail)
```

Parameters

`all`	Enable all IPv4 multicast debugging.
`event`	Enable debugging of multicast events.
`fib-msg`	Enable debugging of multicast FIB messages
`mrib-msg`	Enable debugging of multicast MRIB messages
`mrt`	Enable debugging of multicast route
`mtrace`	Enable debugging of multicast traceroute
`mtrace-detail`	Enable detailed debugging of multicast traceroute messages
`nsm-msg`	Enable debugging of multicast NSM messages
`register-msg`	Enable debugging of multicast PIM Register messages
`stats`	Enable debugging of multicast statistics.
`vif`	Enable debugging of multicast interface
`vrf`	Specify the VRF name

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip mrib all
```

ip mroute

Use this command to create a multicast static route.

Multicast static routes are unicast routes which allow multicast and unicast topologies to be incongruous. These routes are used by multicast routing protocols to perform Reverse Path Forwarding (RPF) checks.

Use the `no` form of this command to clear a multicast static route.

Command Syntax

```
ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|) A.B.C.D
ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|) A.B.C.D <1-255>
no ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|)
```

Parameters

`NAME`	Virtual Routing and Forwarding name
`A.B.C.D/M`	Multicast source IP address and mask of the source
`static`	Static routes.
`rip`	Routing Information Protocol.
`ospf`	Open Shortest Patch First protocol.
`bgp`	Border Gateway Protocol.
`isis`	Intermediate System to Intermediate System protocol.
`A.B.C.D`	IP address to use as the RPF address. A host IP address can be a directly connected system or a remote system. For remote systems, a recursive lookup is done from the unicast routing table to find a directly connected system. Recursive lookup is done up to one level.
`<1-255>`	Administrative distance for the multicast static route. This value determines whether a unicast route or multicast static route is used for the RPF lookup. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence.

Default

The default administrative distance for the multicast static route is 0.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip mroute 10.10.10.50/24 10.10.10.20 1

#configure terminal
(config)#ip mroute vrf VRF_A 10.10.10.50/1 10.10.10.20 1
```


© 2021 IP Infusion Inc. Proprietary

ip multicast route-limit

Use this command to limit the number of multicast routes that can be added to a multicast routing table. It generates an error message when the limit is exceeded. If the threshold parameter is set, a threshold warning message is generated when this threshold is exceeded and the message continues to occur until the number of mroutes reaches the limit set by the limit argument.

Note: The mroute warning threshold must not exceed the mroute limit.

Use the `no` parameter with this command to disable this configuration.

Command Syntax

```
ip multicast route-limit <1-2147483647>
ip multicast route-limit <1-2147483647> <1-2147483647>
ip multicast (vrf NAME|) route-limit <1-2147483647>
ip multicast (vrf NAME|) route-limit <1-2147483647> <1-2147483647>
no ip multicast route-limit
no ip multicast (vrf NAME|) route-limit
```

Parameters

`vrf`	VRF name
`<1-2147483647>`	Number of routes
`<1-2147483647>`	Threshold at which to generate a warning message

Default

The default limit and threshold value is 2147483647.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip multicast route-limit 34 24
```

ip multicast ttl-threshold

Use this command to configure the time-to-live (TTL) threshold of packets being forwarded out of an interface. Only multicast packets with a TTL value greater than the threshold are forwarded out of the interface.

Use the no parameter with this command to return to the default TTL threshold.

Command Syntax

```
ip multicast ttl-threshold <1-255>
no ip multicast ttl-threshold
```

Parameters

<1-255>	The time-to-live threshold.

Default

The default TTL value is 1.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip multicast ttl-threshold 34
```


© 2021 IP Infusion Inc. Proprietary

ip multicast-routing

Use this command to turn on/off multicast routing on the router; when turned off, the multicast protocol daemon remains present, but does not perform multicast functions. When multicast routing is enabled, the MRIB re-creates tunnels, and starts processing any VIF addition/deletion requests, MRT addition/deletion requests, and any multicast forwarding events.

Use the `no` parameter with this command to disable this function. When the `no` parameter is used, the MRIB releases all VIFs and tunnels, cleans up MRTs, stops IGMPv2 operation and stops relaying multicast forwarder events to multicast protocols.

Command Syntax

```
ip multicast-routing
ip multicast-routing (vrf NAME|)
no ip multicast-routing
no ip multicast-routing (vrf NAME|)
```

Parameter

`vrf`	Specify the VRF name.

Default

By default, multicast routing is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip multicast-routing
```

ipv6 mroute

Use this command to create a multicast static route.

Multicast static routes are unicast routes that allow multicast and unicast topologies to be incongruous. These routes are used by multicast routing protocols to perform Reverse Path Forwarding (RPF) checks.

Use the `no` form of this command to clear a multicast static route.

Command Syntax

```
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X <1-255>
no ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|)
```

Parameters

`NAME`	Virtual Routing and Forwarding name
`X:X::X:X/M`	Specify multicast source IP address and mask
`static`	Static routes.
`rip`	Routing Information Protocol.
`bgp`	Border Gateway Protocol.
`ospf`	Open Shortest Path First.
`isis`	Intermediate System to Intermediate System.
`X:X::X:X`	RPF address for the multicast route. A host IP address can be a directly connected system or a remote system. For remote systems, a recursive lookup is done from the unicast routing table to find a directly connected system. Recursive lookup is done up one level.
`<1-255>`	Administrative distance for the multicast static route. This value determines whether a unicast route or multicast static route is used for the RPF lookup. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence.

Default

The default administrative distance for the multicast static route is 0.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#ipv6 mroute 10:10::10:10/64 10:10::10:12 1
```


© 2021 IP Infusion Inc. Proprietary

show debugging ip mrib

Use this command to display IPv4 multicast debugging information.

Command Syntax

```
show debugging ip mrib
show debugging ip mrib (vrf NAME|)
```

Parameters

`vrf`	Display routes from a VPN Routing/Forwarding instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is a sample output of the `show debugging ip mrib` command.

```
#show debugging ip mrib
Debugging status:
  MRIBv4 event debugging is on
  MRIBv4 VIF debugging is on
  MRIBv4 route debugging is on
  MRIBv4 route statistics debugging is on
  MRIBv4 FIB message debugging is on
  MRIBv4 PIM Register message debugging is on
  MRIBv4 NSM IPC message debugging is on
  MRIBv4 MRIB IPC message debugging is on
  MRIBv4 traceroute debugging is on
  MRIBv4 traceroute detailed debugging is on
#
```

show ip mroute

Use this command to display the IP multicast routing (mroute) table. The routing table is based on the pairing of Source Addresses with their respective Destination Multicast Group Address (S, G).

Command Syntax

```
show ip mroute (dense|sparse|) (count|summary|)
show ip mroute A.B.C.D (dense|sparse|)(count|summary|)
show ip mroute A.B.C.D A.B.C.D (dense|sparse|) (count|summary|)
show ip mroute (vrf NAME|) (dense|sparse|) (count|summary|)
show ip mroute (vrf NAME|) A.B.C.D (dense|sparse|) (count|summary|)
show ip mroute (vrf NAME|) A.B.C.D A.B.C.D (dense|sparse|) (count|summary|)
```

Parameters

`A.B.C.D`	Source or Group IP address.
`count`	Route and packet count data.
`summary`	Provide abbreviated display.
`dense`	Show dense multicast routes.
`sparse`	Show sparse multicast routes.
`vrf`	Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command displaying the IP multicast routing table, with and without specifying the group and source IP address:

```
rtr6#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(172.31.1.52, 224.0.0.13), uptime 00:09:39
Owner PIM, Flags: F
  Incoming interface: eth1
  Outgoing interface list:
    eth2 (1)
```

The following is a sample output of this command displaying the packet count from the IP multicast routing table:

© 2021 IP Infusion Inc. Proprietary

```
#show ip mroute count

IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:10

Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent

(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
  Fwd msg: 0/0, Client msg: 0/0/0/0,  Reg: 0/0/0
```

The following is a sample output for this command displaying the IP multicast routing table in an abbreviated form:

```
#show ip mroute summary

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.0.13), 00:01:32/00:03:20, PIM-SM, Flags: TF
```

Table 1-192: mroute pointers

Pointers	Description
I	Immediate statistics
T	Timed statistics
F	Forwarder installed
B	Bidirectional
Timers	• Uptime – route uptime. • Statistics Expiry –The time the routing table waits before updating statistics.
Interface State	Interface Time to Live (TTL)

Table 1-193: Show ip mroute output

Entry	Description
(a.d.c.d, 224.x.x.x)	Source Address paired with its Destination Multicast Group Address
uptime	As stated.

Table 1-193: Show ip mroute output

Entry	Description
Owner	The owner is derived from the multicast group notable address (IANA). In the example above, the owner is specified as PIM because it is using the IANA address: 224.0.0.13. Other owners can be OSPF (224.0.0.5), IS-IS (224.0.0.19–21), and so on.
Flags	The flags associated with this mroute table entry.
Incoming interface	The name of the in coming interface (eth1, xe5/2, etc.).
Outgoing interface list	A numbered list of the outgoing interfaces

Table 1-194: Show ip mroute statistics received and sent

Entry	Description
NOCACHE	Number of No Cache messages received.
WRONGVIF	The Virtual Host Interface (VIF) enables the router to send and receive IP multicast packets on several different interfaces at once. This is the count of wrong VIFs received.
WHOLEPKT	When a source is multicasting a large volume data and the PIM router does not know about the particular Rendezvous Point (RP(G)), the PIM process will constantly receive WHOLEPKT notification from the kernel – this shows the count of such notifications.

© 2021 IP Infusion Inc. Proprietary

show ip mvif

Use this command to display the MRIB VIF table entries.

The Virtual Host Interface (VIF) used in Pragmatic General Multicast (PGM) or “Reliable Multicast.” The VIF enables the router to send and receive IP multicast packets on several different interfaces at once, as dictated by the multicast routing tables on the router.

Command Syntax

```
show ip mvif
show ip mvif IFNAME
show ip mvif (vrf NAME|)
show ip mvif (vrf NAME|) IFNAME
```

Parameters

IFNAME	Specify the interface name.
vrf	Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following are sample outputs of this command displaying the contents for the MRIB VIF table, both with and without the interface parameter specified:

```
#show ip mvif
Interface    Vif   Owner    TTL  Local            Remote           Uptime
             Idx   Module        Address          Address
wm0          0     PIM-SM   1    192.168.1.53     0.0.0.0          00:04:26
Register     1             1    192.168.1.53     0.0.0.0          00:04:26
wm1          2     PIM-SM   1    192.168.10.53    0.0.0.0          00:04:25
#show ip mvif wm0
Interface   Vif   Owner    TTL  Local            Remote           Uptime
            Idx   Module        Address          Address
wm0         0     PIM-SM   1    192.168.1.53     0.0.0.0          00:05:17
```

Table 1-195: Show ip mvif output

Entries	Description
Interface	The name of the interface.
Vif Idx	The VIF Index – the numbering of the entries in the MRIB table.
Owner	What multicast protocol is being used for an entry. For example, PIM-SM (PIM Sparce Mode).

Table 1-195: Show ip mvif output (Continued)

Entries	Description
TTL	Time to Live for the entry.
Local Address	AS stated.
Remote Address	As stated.
Uptime	How long the multicast interface has been operating.

© 2021 IP Infusion Inc. Proprietary

show running-config interface multicast

Use this command to show the running system status and configuration for a multicast interface.

Command Syntax

```
show running-config interface IFNAME ip multicast
```

Parameters

IFNAME	Interface name.

Command Mode

Privileged exec mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 ip multicast
!
interface eth1
!
```

snmp restart mribd

Use this command to restart SNMP in Multicast Routing Information Base (MRIB)

Command Syntax

```
snmp restart mribd
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart mribd
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 L3 IGMP Multicast Commands

This chapter describes the commands for Internet Group Management Protocol (IGMP) including the IGMP proxy service.

For IGMP multicast snooping commands, see Chapter 3, *L2 IGMP Snooping Multicast Commands*.

- clear ip igmp
- debug ip igmp
- ip igmp
- ip igmp access-group
- ip igmp immediate-leave
- ip igmp join-group
- ip igmp last-member-query-count
- ip igmp last-member-query-interval
- ip igmp limit
- ip igmp mroute-proxy
- ip igmp offlink
- ip igmp proxy-service
- ip igmp proxy unsolicited-report-interval
- ip igmp querier-timeout
- ip igmp query-interval
- ip igmp query-max-response-time
- ip igmp ra-option
- ip igmp robustness-variable
- ip igmp ssm-map enable
- ip igmp ssm-map static
- ip igmp static-group
- ip igmp startup-query-count
- ip igmp startup-query-interval
- ip igmp version
- show debugging ip igmp
- show ip igmp groups
- show ip igmp interface
- show ip igmp proxy
- show ip igmp ssm-map
- show running-config interface igmp

© 2021 IP Infusion Inc. Proprietary

clear ip igmp

Use this command to clear all IGMP local-memberships on all interfaces. This command applies to interfaces configured for IGMP Layer-3 multicast protocols, or IGMP Proxy.

Command Syntax

```
clear ip igmp
clear ip igmp group *
clear ip igmp group A.B.C.D
clear ip igmp group A.B.C.D IFNAME
clear ip igmp interface IFNAME
clear ip igmp (vrf NAME|)
clear ip igmp (vrf NAME|) group *
clear ip igmp (vrf NAME|) group A.B.C.D
clear ip igmp (vrf NAME|) group A.B.C.D IFNAME
clear ip igmp (vrf NAME|) interface IFNAME
```

Parameters

`*`	Clears all groups on all interfaces.
`A.B.C.D`	Specify the group address's local-membership to be cleared from all interfaces.
`interface`	Specify an interface. All groups learned from this interface are deleted.
`IFNAME`	Specify name of the interface.
`vrf`	Specify the VRF name.
`group`	Deletes IGMP group cache entries.
`interface`	Specify name of the interface; all groups learned from this interface are deleted.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip igmp
#clear ip igmp group *
#clear ip igmp group 224.1.1.1
#clear ip igmp interface eth1
#clear ip igmp vrf VRF_A
#clear ip igmp vrf new group *
#clear ip igmp vrf new interface eth1
```


© 2021 IP Infusion Inc. Proprietary

debug ip igmp

Use this command to enable debugging of all IGMP, or a specific component of IGMP. This command applies to interfaces configured for IGMP Layer-3 multicast protocols.

Use the `no` parameter with this command to disable all IGMP debugging, or select a specific IGMP component.

Command Syntax

```
debug ip igmp all
debug ip igmp decode
debug ip igmp encode
debug ip igmp events
debug ip igmp fsm
debug ip igmp tib
debug ip igmp (vrf NAME|) all
debug ip igmp (vrf NAME|) decode
debug ip igmp (vrf NAME|) encode
debug ip igmp (vrf NAME|) events
debug ip igmp (vrf NAME|) fsm
debug ip igmp (vrf NAME|) tib
no debug ip igmp all
no debug ip igmp decode
no debug ip igmp encode
no debug ip igmp events
no debug ip igmp fsm
no debug ip igmp tib
no debug ip igmp (vrf NAME|) all
no debug ip igmp (vrf NAME|) decode
no debug ip igmp (vrf NAME|) encode
no debug ip igmp (vrf NAME|) events
no debug ip igmp (vrf NAME|) fsm
no debug ip igmp (vrf NAME|) tib
```

Parameters

`all`	Debug all IGMP.
`decode`	Debug IGMP decoding.
`encode`	Debug IGMP encoding.
`events`	Debug IGMP events.
`fsm`	Debug IGMP Finite State Machine (FSM).
`tib`	Debug IGMP Tree Information Base (TIB).

`vrf`	Debug VPN Routing/Forwarding instance.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ip igmp all
```


© 2021 IP Infusion Inc. Proprietary

ip igmp

Use this command to enable the IGMP operation on an interface. This command enables IGMP operation in stand-alone mode, and can be used to learn local-membership information prior to enabling a multicast routing protocol on the interface. This command will has no effect on interfaces configured for IGMP proxy.

Use the `no` parameter with this command to return all IGMP related configuration to the default (including IGMP proxy service).

Command Syntax

```
ip igmp
no ip igmp
```

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp
```

ip igmp access-group

Use this command to control the multicast local-membership groups learned on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols, IGMP proxy.

Use the `no` parameter with this command to disable this access control.

Command Syntax

```
ip igmp access-group WORD
no ip igmp access-group WORD
```

Parameters

`WORD`	Standard IP access-list name.

Default

No access list configured

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, hosts serviced by Ethernet interface 0 can only join the group 225.2.2.2:

```
#configure terminal
(config)#access-list 1 permit 225.2.2.2 0.0.0.0
(config)#interface eth1
(config-if)#ip igmp access-group xyz
(config-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

ip igmp immediate-leave

In IGMP version 2, use this command to minimize the leave latency of IGMP memberships. This command is used when only one receiver host is connected to each interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols, IGMP Proxy.

To disable this feature, use the `no` parameter with this command.

Command Syntax

```
ip igmp immediate-leave group-list WORD
no ip igmp immediate-leave
```

Parameters

`group-list`	Standard access-list name or number that defines multicast groups in which the immediate leave feature is enabled.
`WORD`	Standard IP access-list name.

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to enable the immediate-leave feature on an interface for a specific range of multicast groups. In this example, the router assumes that the group access-list consists of groups that have only one host membership at a time per interface:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp immediate-leave group-list xyz
(config-if)#exit
(config)#access-list 34 permit 225.192.20.0 0.0.0.255
```

ip igmp join-group

Use this command to configure a join multicast group.

Use the `no` parameter with this command to delete group membership entry.

Command Syntax

```
ip igmp join-group A.B.C.D {(source (A.B.C.D)|)}
no ip igmp join-group A.B.C.D {(source (A.B.C.D)|)}
```

Parameters

`A.B.C.D`	Standard IP multicast group address to be configured as a group member.
`source`	Static source to be joined.
`A.B.C.D`	Standard IP source address to be configured as a source from where multicast packets originate.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp join-group 225.1.1.1 source 1.1.1.2

(config-if)#no ip igmp join-group 225.1.1.1 source 1.1.1.2
```


© 2021 IP Infusion Inc. Proprietary

ip igmp last-member-query-count

Use this command to set the last-member query-count value. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to return to the default value on an interface.

Command Syntax

```
ip igmp last-member-query-count <2-7>
no ip igmp last-member-query-count
```

Parameter

`<2-7>`	Specify the last member query count value.

Default

The default last member query count value is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp last-member-query-count 3
```

ip igmp last-member-query-interval

Use this command to configure the frequency at which the router sends IGMP group-specific host query messages. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to set this frequency to the default value.

Command Syntax

```
ip igmp last-member-query-interval <1000-25500>
no ip igmp last-member-query-interval
```

Parameter

`<1000-25500>`	Frequency (in milliseconds) at which IGMP group-specific host query messages are sent.

Default

1000 milliseconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example changes the IGMP group-specific host query message interval to 2 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp last-member-query-interval 2000
```


© 2021 IP Infusion Inc. Proprietary

ip igmp limit

Use this command to set the maximum number of group membership states, at either the router level or at the interface level. Once the specified number of group memberships is reached, all further local-memberships are ignored. Optionally, an exception access-list can be configured to specify the group-address(es) to be excluded from being subject to the limit.

This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy. The limit applies, individually, to each of its constituent interfaces.

Use the `no` parameter with this command to unset the limit and any specified exception access-list.

Command Syntax

```
ip igmp limit (<1-2097152> (except WORD |)
ip igmp (vrf NAME) limit(<1-2097152> (except WORD |)
no ip igmp limit
no ip igmp (vrf NAME|) limit
```

Parameters

`vrf`	Specify the VRF name.
`<1-2097152>`	Maximum number of group membership states.
`except`	Number or name that defines multicast groups that are exempted from being subject to configured limit.
`WORD`	Standard IP access-list name.

Command Mode

Configure mode and Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures an IGMP limit of 100 group-membership states across all interfaces on which IGMP is enabled, and excludes group 224.1.1.1 from this limitation:

```
#configure terminal
(config)#access-list 1 permit 224.1.1.1 0.0.0.0
(config)#ip igmp limit 100 except xyz
```

The following example configures an IGMP limit of 100 group-membership states on eth1:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp limit 100
```

ip igmp mroute-proxy

Use this command to specify the IGMP Proxy service (upstream host-side) interface with which to be associated. IGMP router-side protocol operation is enabled only when the specified upstream proxy-service interface is functional.

Note: This command should not be used when configuring interfaces enabled for IGMP in association with a multicast routing protocol, otherwise the behavior will be undefined.

Use the `no` parameter with this command to remove the association with the proxy-service interface.

Command Syntax

```
ip igmp mroute-proxy IFNAME
no ip igmp mroute-proxy
```

Parameter

`IFNAME`	Specify an interface name.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures the eth1 interface as the upstream proxy-service interface for the downstream router-side interface, eth1.

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp mroute-proxy eth1
```


© 2021 IP Infusion Inc. Proprietary

ip igmp offlink

Use this command to configure off-link for IGMP.

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
ip igmp offlink
no ip igmp offlink
```

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp offlink

(config-if)#no ip igmp offlink
```

ip igmp proxy-service

Use this command to designate an interface to be the IGMP proxy-service (upstream host-side) interface, thus enabling IGMP host-side protocol operation on this interface. All associated downstream router-side interfaces will have their memberships consolidated on this interface, according to IGMP host-side functionality.

Note: This command should not be used when configuring interfaces enabled for IGMP in association with a multicast-routing protocol, otherwise the behavior will be undefined.

Use the `no` parameter with this command to remove the designation of the interface as an upstream proxy-service interface.

Command Syntax

```
ip igmp proxy-service
no ip igmp proxy-service
```

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example designates the eth1 interface as the upstream proxy-service interface.

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp proxy-service
```


© 2021 IP Infusion Inc. Proprietary

ip igmp proxy unsolicited-report-interval

Use this command to set an unsolicited report interval for an interface designated as an IGMP proxy (upstream host-side).

Use the `no` parameter with this command to remove the unsolicited report interval from the interface.

Command Syntax

```
ip igmp proxy unsolicited-report-interval <1000-25500>
no ip igmp proxy unsolicited-report-interval
```

Parameter

`<1000-25500>`	Specify an unsolicited report interval value in milliseconds.

Default

1000 milliseconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp proxy unsolicited-report-interval 1234

(config-if)#no ip igmp proxy unsolicited-report-interval
```

ip igmp querier-timeout

Use this command to set the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To restore the default value, use the `no` parameter with this command.

Command Syntax

```
ip igmp querier-timeout <60-300>
no ip igmp querier-timeout
```

Parameter

`<60-300>`	Number of seconds that the router waits after the previous querier has stopped querying before it takes over as the querier.

Default

255 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures the router to wait 120 seconds from the time it received the last query before it takes over as the querier for the interface:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp querier-timeout 120
```


© 2021 IP Infusion Inc. Proprietary

ip igmp query-interval

Use this command to set the frequency of sending IGMP host query messages. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To return to the default frequency, use the `no` parameter with this command.

Note: Querier timeout changes by changing query interval.

Command Syntax

```
ip igmp query-interval <1-18000>
no ip igmp query-interval
```

Parameter

`<1-18000>`	Frequency (in seconds) at which IGMP host query messages are sent.

Default

Default query interval is 125 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example changes the frequency of sending IGMP host-query messages to 2 minutes:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp query-interval 120
```

ip igmp query-max-response-time

Use this command to set the maximum response time advertised in IGMP queries. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to restore the default value.

Command Syntax

```
ip igmp query-max-response-time <1-240>
no ip igmp query-max-response-time
```

Parameter

`<1-240>`	Maximum response time (in seconds) advertised in IGMP queries.

Default

10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures a maximum response time of 8 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp query-max-response-time 8
```


© 2021 IP Infusion Inc. Proprietary

ip igmp ra-option

Use this command to configure strict RA (Router Advertisement) validation for IGMP.

Use the `no` parameter with this command to restore the default value.

Command Syntax

```
ip igmp ra-option
no ip igmp ra-option
```

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example configures a maximum response time of 8 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp ra-option

(config-if)#no ip igmp ra-option
```

ip igmp robustness-variable

Use this command to set the robustness variable value on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To return to the default value on an interface, use the `no` parameter with this command.

Command Syntax

```
ip igmp robustness-variable <2-7>
no ip igmp robustness-variable
```

Parameter

`<2-7>`	Specify the robustness variable value.

Default

Default robustness variable value is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp robustness-variable 3
```


© 2021 IP Infusion Inc. Proprietary

ip igmp ssm-map enable

Use this command to enable SSM mapping on the router. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to disable SSM mapping.

Command Syntax

```
ip igmp ssm-map enable
ip igmp (vrf NAME|) ssm-map enable
no ip igmp ssm-map enable
no ip igmp (vrf NAME|) ssm-map enable
```

Parameter

`vrf`	Specify the VRF name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to configure SSM mapping on the router.

```
#configure terminal
(config)#ip igmp ssm-map enable
```

ip igmp ssm-map static

Use this command to specify the static mode of defining SSM mapping. SSM mapping statically assigns sources to IGMPv1 and IGMPv2 groups to translate such (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to remove the SSM map association.

Command Syntax

```
ip igmp ssm-map static WORD A.B.C.D
ip igmp (vrf NAME|) ssm-map static WORD A.B.C.D
no ip igmp (vrf NAME|) ssm-map static WORD A.B.C.D
no ip igmp ssm-map static WORD A.B.C.D
```

Parameters

`vrf`	Specify the VRF name.
`WORD`	Standard IP access-list name.
`A.B.C.D`	Source address to use for static map group.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to configure an SSM static mapping for group-address 224.1.1.1

Note: `access-list` can only be a `permit` type `access-list`

```
#configure terminal
(config)# ip igmp ssm-map static xyz 1.2.3.4
(config)# access-list 1 permit 224.1.1.1 0.0.0.255
```


© 2021 IP Infusion Inc. Proprietary

ip igmp static-group

Use this command to statically configure group membership entries on an interface. To statically add only a group membership, do not specify any parameters. This command applies to IGMP operation on a specific interface to statically add group and/or source records; on a VLAN interface to statically add group and/or source records.

Use the `no` parameter with this command to delete static group membership entries.

Command Syntax

```
ip igmp static-group A.B.C.D (source (A.B.C.D|ssm-map)|)
no ip igmp static-group A.B.C.D (source (A.B.C.D|ssm-map)|)
```

Parameters

`A.B.C.D`	Standard IP Multicast group address to be configured as a static group member.
`source`	Static source to be joined.
`A.B.C.D`	Standard IP source address to be configured as a static source from where multicast packets originate.
`ssm-map`	Mode of defining SSM mapping. SSM mapping statically assigns sources to IGMPv1 and IGMPv2 groups to translate these (*, G) groups' memberships to (S, G) memberships for use with PIM-SSM.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following examples show how to statically add group and/or source records for IGMP:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.3

#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.4 source 1.2.3.4

#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.5 source ssm-map
```

ip igmp startup-query-count

Use this command to set a startup query count for IGMP.

Use the `no` parameter with this command to return to the default version.

Command Syntax

```
ip igmp startup-query-count <2-10>
no ip igmp startup-query-count
```

Parameters

`<2-10>`	Specify a startup query count value.

Default

The default value 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp startup-query-count 2

(config-if)#no ip igmp startup-query-count
```


© 2021 IP Infusion Inc. Proprietary

ip igmp startup-query-interval

Use this command to set a query interval value for IGMP.

Use the `no` parameter with this command to return to the default version.

Command Syntax

```
ip igmp startup-query-interval <1-18000>
no ip igmp startup-query-interval
```

Parameters

`<1-18000>`	Specify a startup query interval value in seconds.

Default

The default value 31 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp startup-query-interval 1

(config-if)#no ip igmp startup-query-interval
```

ip igmp version

Use this command to set the current IGMP protocol version on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to return to the default version.

Command Syntax

```
ip igmp version <1-3>
no ip igmp version
```

Parameters

`<1-3>`	Specify IGMP protocol version number.

Default

The default IGMP protocol version number is 3.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp version 2
```


© 2021 IP Infusion Inc. Proprietary

show debugging ip igmp

Use this command to display the status of the debugging of the IGMP system, or a specific VRF in the IGMP system.

Command Syntax

```
show debugging ip igmp
show debugging ip igmp (vrf NAME|)
```

Parameters

`vrf`	Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging ip igmp
 IGMP Debugging status:
 IGMP Decoder debugging is on
 IGMP Encoder debugging is on
 IGMP Events debugging is on
 IGMP FSM debugging is on
 IGMP Tree-Info-Base (TIB) debugging is on
```

show ip igmp groups

Use this command to display the multicast groups with receivers connected to the router and learned through IGMP.

Command Syntax

```
show ip igmp groups (detail|)
show ip igmp groups A.B.C.D (detail|)
show ip igmp groups IFNAME (detail|)
show ip igmp groups IFNAME A.B.C.D (detail|)
show ip igmp (vrf NAME|) groups (detail|)
show ip igmp (vrf NAME|) groups A.B.C.D (detail|)
show ip igmp (vrf NAME|) groups IFNAME (detail|)
show ip igmp (vrf NAME|) groups IFNAME A.B.C.D (detail|)
```

Parameters

`vrf`	Specify the VRF name.
`A.B.C.D`	Address of multicast group.
`IFNAME`	Name of the interface.
`detail`	IGMPv3 source information.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following command displays local-membership information for all interfaces:

```
rtr1#show ip igmp groups detail
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
SG - Static Group, SS - Static Source)
Interface:      eth1
Group:          224.1.1.1
Flags:          L
Uptime:         00:00:04
Group mode:     Exclude (Expires: 00:04:15, Static)
Last reporter:   3.3.3.3
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)
Include Source List :
 Source Address Uptime    v3 Exp    Fwd Flags
 2.2.2.2         00:00:04 stopped   Yes L
```

Table 2-196 shows the flags codes displayed at the start of a group entry.

© 2021 IP Infusion Inc. Proprietary

Table 2-196: Flags

Flag	Meaning
M	Source Specific Multicast
R	Remote multicast
L	Local multicast
SG	Static Group
SS	Static Source

Table 2-197 explains the output fields.

Table 2-197: show ip igmp groups output

Entry	Description
Interface	The interface on which multicast is operating.
Group	The Multicast group, identified by a multicast IP address.
Flags	Flag on this interface – in this case, the flag indicates that the multicast is Local. See Table 2-196.
Uptime	The amount of time that the multicast connection has been up.
Group mode	The group mode is determined by interactions between IGMP router database entries, which is beyond the scope of this document. For a detailed description of these interactions, see RFC 3376.
Last reporter	The IPv4 address of the last host to send multicast information.
Group source list	A list of flags that indicate the state of the multicast connections. See Table 2-196.
Include Source List	A table containing parameters about the multicast session: • Source Address – The IP address of the Source(s) connected to the multicast hosts. • Uptime – The multicast session's uptime. • v3 Exp – Tells whether IGMPv3 Explicit Tracking is running or not. • Fwd – Whether IGMP information is being forwarded by this device. • Flags – See Table 2-196.

show ip igmp interface

Use this command to display the state of IGMP, IGMP Proxy service for a specified interface, or all interfaces.

Command Syntax

```
show ip igmp interface (IFNAME|)
show ip igmp (vrf NAME|) interface (IFNAME|)
```

Parameters

`vrf`	Specify the VRF name.
`interface`	Specify the interface parameter.
`IFNAME`	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command displays the IGMP interface status on all interfaces enabled for IGMP.

```
#show ip igmp interface
Interface vlan1.1 (Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default)
IGMP querying router is 0.0.0.0
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds|
#
```

Table 2-198 explains the output fields.

Table 2-198: show ip igmp interface

Entry	Description
Interface	Interface type and number
IGMP Active	IGMP status – whether Active or Inactive; whether this interface is a querier; IGMP version (v1, v2, or v3).
IGMP querying router	IP address of the designated router for this LAN segment.
IGMP query interval	Interval at which the Cisco IOS software sends Protocol Independent Multicast (PIM) router query messages.
IGMP querier timeout	An interval of time that the software uses when deciding to take over as the querier.

© 2021 IP Infusion Inc. Proprietary

Table 2-198: show ip igmp interface (Continued)

Entry	Description
IGMP max query response time	An interval of time that is advertised as the maximum response time that is advertised in IGMP queries.
Last member query response interval	This interval is the maximum amount of time between query messages that the querier will wait before sending messages that indicate that the multicast session has ended.
Group Membership interval	A group membership interval timer is maintained for each dynamic multicast group added to a downstream interface in the table. The timer is refreshed when a membership report for a multicast group is received. If the timer expires, the multicast group is removed from the table.

show ip igmp proxy

Use this command to display the state of IGMP Proxy services for a specified interface or for all interfaces.

Command Syntax

```
show ip igmp proxy groups (detail|)
show ip igmp proxy groups A.B.C.D (detail|)
show ip igmp proxy groups IFNAME (detail|)
show ip igmp proxy groups IFNAME A.B.C.D (detail|)
show ip igmp (vrf NAME|) proxy groups (detail|)
show ip igmp (vrf NAME|) proxy groups A.B.C.D (detail|)
show ip igmp (vrf NAME|) proxy groups IFNAME (detail|)
show ip igmp (vrf NAME|) proxy groups IFNAME A.B.C.D (detail|)
```

Parameters

`vrf`	Specify the VRF name.
`groups`	IGMP proxy group membership information.
`A.B.C.D`	Address of multicast group.
`IFNAME`	The name of the VLAN interface.
`detail`	IGMPv3 source information

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip igmp proxy

Interface eth2 (Index 4)
Administrative status: enabled
Operational status: up
Upstream interface is eth1
Number of multicast groups: 1

#show ip igmp proxy groups

IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
224.0.1.3        eth1                 Active    Delay
```


© 2021 IP Infusion Inc. Proprietary

Table 2-199 explains the output fields.

Table 2-199: show ip igmp proxy output

Entry	Description
Interface	Interface and Index of the interface.
Administrative status	Depends on the interface states – Enabled only if both host and downstream interfaces are up. Otherwise, Disabled if only one interface is up.
Operational status	Depends on Administrative status – either Up or Down depending on Administrative status of corresponding interfaces.
Upstream interface	As stated.
Number of multicast groups	The number of multicast groups supported by this proxy.

Table 2-200 explains the output fields.

Table 2-200: show ip igmp proxy groups output

Entry	Description
Group Address	Multicast address associated with each group.
Interface	Interface name, such as eth1, xe3/1, etc..
State	The state of the proxy group – can be either Active or Inactive.
Member state	The state of the proxy group member – can be either Idle or Delay, Idle is the default state.

show ip igmp ssm-map

Use this command to display IGMP SSM-map data.

Command Syntax

```
show ip igmp ssm-map
show ip igmp ssm-map A.B.C.D
show ip igmp (vrf NAME|) ssm-map
show ip igmp (vrf NAME|) ssm-map A.B.C.D
```

Parameters

`vrf`	Specify the VRF name.
`A.B.C.D`	Address of multicast group.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh ip igmp ssm-map
SSM Mapping : Enabled
Database    : Static mappings configured
```


© 2021 IP Infusion Inc. Proprietary

show running-config interface igmp

Use this command to show the running system status and configuration for IGMP.

Command Syntax

```
show running-config interface IFNAME ip igmp
```

Parameters

IFNAME	Interface name.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 ip igmp
!
interface eth1
!
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 L2 IGMP Snooping Multicast Commands

This chapter describes commands for Internet Group Management Protocol (IGMP) multicast snooping.

- igmp snooping
- igmp snooping fast-leave
- igmp snooping mrouter
- igmp snooping querier
- igmp snooping report-suppression
- igmp snooping static-group
- show igmp snooping interface
- show igmp snooping groups
- show igmp snooping mrouter
- show igmp snooping statistics

© 2021 IP Infusion Inc. Proprietary

igmp snooping

Use this command to enable IGMP Snooping. When this command is given in the Configure mode, IGMP snooping is enabled at switch level on all the vlans in switch. When this command is given at the VLAN interface level, IGMP Snooping is enabled for that VLAN.

Note: IGMP Snooping can be only enabled/disabled on VLAN interfaces.

Use the `no` parameter with this command to globally disable IGMP Snooping, or for the specified interface.

Command Syntax

```
igmp snooping
no igmp snooping
```

Parameter

None

Default

IGMP Snooping is enabled.

Command Mode

Interface mode for VLAN interface

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#igmp snooping
(config)#interface vlan1.1
(config-if)#igmp snooping
```


© 2021 IP Infusion Inc. Proprietary

igmp snooping fast-leave

Use this command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing; the IGMP group-membership is removed as soon as an IGMP leave group message is received without sending out a group-specific query.

Use the `no` parameter with this command to disable fast-leave processing.

Command Syntax

```
igmp snooping fast-leave
no igmp snooping fast-leave
```

Parameters

None

Default

IGMP Snooping fast-leave processing is disabled.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to enable fast-leave processing on a VLAN.

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping fast-leave
```

igmp snooping mrouter

Use this command to statically configure the specified VLAN constituent interface as a multicast router interface for IGMP Snooping in that VLAN.

Use the `no` parameter with this command to remove the static configuration of the interface as a multicast router interface.

Command Syntax

```
igmp snooping mrouter interface IFNAME
no igmp snooping mrouter interface IFNAME
```

Parameter

`IFNAME`	Specify the name of the interface.

Default

IGMP Snooping mrouter processing is disabled.

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows interface fe8 statically configured to be a multicast router interface.

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping mrouter interface fe8
```


© 2021 IP Infusion Inc. Proprietary

igmp snooping querier

Use this command to enable IGMP snooping querier functionality on a VLAN when IGMP is not enabled on the particular VLAN. When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces on that VLAN.

The IGMP Snooping querier uses the 0.0.0.0 source IP address, because it only masquerades as a proxy IGMP querier for faster network convergence. It does not start, or automatically cease, the IGMP Querier operation if it detects query message(s) from a multicast router. It restarts as the IGMP Snooping querier if no queries are seen within the other querier interval.

Use the `no` parameter with this command to disable IGMP querier configuration.

Command Syntax

```
igmp snooping querier
no igmp snooping querier
```

Default

By default, Querier is disabled

Parameters

None

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping querier
```

igmp snooping report-suppression

Use this command to enable report suppression for IGMP version 1, 2 and 3 reports. By default report suppression is enabled.

Use the `no` parameter with this command to disable report suppression.

Command Syntax

```
igmp snooping report-suppression
no igmp snooping report-suppression
```

Default

By default, report suppression is enabled.

Parameters

None

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping report-suppression
```


© 2021 IP Infusion Inc. Proprietary

igmp snooping static-group

Use this command to statically configure group membership entries on an interface

Use the `no` parameter with this command to disable report suppression.

Command Syntax

```
igmp snooping static-group A.B.C.D interface IFNAME
no igmp snooping static-group A.B.C.D interface IFNAME
igmp snooping static-group A.B.C.D source A.B.C.D interface IFNAME
no igmp snooping static-group A.B.C.D source A.B.C.D interface IFNAME
```

Parameters

`IFNAME`	Specify the name of the interface.
`A.B.C.D`	Specify the IP address In case of static-group, Multicast Address to be Joined. In case of source, Source Address to be Joined.

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#conf t
(config)#interface vlan1.1
(config-if)#igmp snooping static-group 230.0.0.1 interface xe2
(config-if)#igmp snooping static-group 230.0.0.1 source 10.10.10.10 interface
xe1
(config-if)#exit
(config)#exit
```

show igmp snooping interface

Use this command to know querier, fast-leave, report-suppression is enabled/disabled on that particular interface.

Command Syntax

```
show igmp snooping interface IFNAME
```

Parameters

IFNAME	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command displays the multicast router interfaces in VLAN 1.1.

```
#sh igmp snooping interface
Global IGMP Snooping information
IGMP Snooping Enabled
IGMPv1/v2 Report suppression Enabled
IGMPv3 Report suppression Enabled

IGMP Snooping information for vlan1.1
IGMP Snooping enabled
Snooping Querier none
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression enabled
IGMPv3 Report suppression enabled
Router port detection using IGMP Queries
Number of router-ports: 0
Number of Groups: 0
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0
Number of v3-reports: 0
Active Ports:
  xe5/1

IGMP Snooping information for vlan1.2
IGMP Snooping enabled
Snooping Querier enabled, address 0.0.0.0, Version 3
Querier interval: 125 seconds
Querier Last member query interval: 1000 milliseconds
```

 © 2021 IP Infusion Inc. Proprietary

```
IGMP Snooping maximum query response time is 10 seconds
IGMP Snooping Startup query interval is 31 seconds
Querier robustness: 2
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression enabled
IGMPv3 Report suppression enabled
Router port detection using IGMP Queries
Number of router-ports: 0
Number of Groups: 0
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0
Number of v3-reports: 0
Active Ports:
  xe5/1
```

show igmp snooping groups

Use this command to display the multicast groups learned through snooping or statically configured.

Command Syntax

```
show igmp snooping groups
show igmp snooping groups details
show igmp snooping groups A.B.C.D
show igmp snooping groups A.B.C.D detail
show igmp snooping groups IFNAME
show igmp snooping groups IFNAME A.B.C.D
show igmp snooping groups IFNAME A.B.C.D detail
show igmp snooping groups IFNAME detail
```

Parameters

`A.B.C.D`	Specify multicast group address.
`IFNAME`	Specify the name of the interface.
`detail`	IGMPv3 source information.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
200    230.0.0.1             xe1          S     00:02:07   static   0.0.0.0
V3
#show igmp snooping groups detail
IGMP Snooping Group Membership Details
Flags: (R - Remote, S - Static)

Interface:      xe1
Group:          230.0.0.1
Flags:          S
Uptime:         00:02:08
Group mode:     Exclude (Static)
Last reporter:  0.0.0.0
Source list is empty

#show igmp snooping groups 230.0.0.1
```


© 2021 IP Infusion Inc. Proprietary

```
      IGMP Snooping Group Membership
      Group source list: (R - Remote, S - Static)
      Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
      200    230.0.0.1             xe1          S     00:02:35   static   0.0.0.0
V3
      #show igmp snooping groups 230.0.0.1 detail
      IGMP Snooping Group Membership Details
      Flags: (R - Remote, S - Static)

      Interface:      xe1
      Group:          230.0.0.1
      Flags:          S
      Uptime:         00:02:37
      Group mode:     Exclude (Static)
      Last reporter:  0.0.0.0
      Source list is empty

      #show igmp snooping groups vlan1.200
      IGMP Snooping Group Membership
      Group source list: (R - Remote, S - Static)
      Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
      200    230.0.0.1             xe1          S     00:02:47   static   0.0.0.0
V3
      #show igmp snooping groups vlan1.200 detail
      IGMP Snooping Group Membership Details
      Flags: (R - Remote, S - Static)

      Interface:      xe1
      Group:          230.0.0.1
      Flags:          S
      Uptime:         00:02:50
      Group mode:     Exclude (Static)
      Last reporter:  0.0.0.0
      Source list is empty
```

Table 3-201: Show igmp snooping groups

Entries	Description
Interface	The interface (port) on the multicast router that is marked as taking place in the multicast.
Group	The multicast group identified by an IPv4 address.
Flags	S - Member is statically configured, R - Member is learned from the network.
Uptime	How long the member has been a part of the group.
Group mode	As stated.

Table 3-201: Show igmp snooping groups (Continued)

Entries	Description
Last reporter	In IGMPv3, a host can send a membership report that includes a list of source addresses. When the host sends a membership report in INCLUDE mode, the host is interested in group multicast traffic only from those sources in the source address list. If host sends a membership report in EXCLUDE mode, the host is interested in group multicast traffic from any source except the sources in the source address list. A host can also send an EXCLUDE report in which the source-list parameter is empty, which is known as an EXCLUDE NULL report. An EXCLUDE NULL report indicates that the host wants to join the multicast group and receive packets from all sources.
Vlan	VLAN number ID.
Group/Source Address	Multicast group and source addresses.
Interface	The interface (port) on the multicast router that is marked as taking place in the multicast.
Flags	S - Member is statically configured, R - Member is learned from the network.
Uptime	How long the member has been a part of the group.
Expires	Either by a timeout (IGMPv1) or by checking whether the member is still a part of the multicast (IGMPv2 or v3). Can also be statically configured.
Last Reporter	Indicates that the host wants to join a particular multicast group.
Version	IGMP version (v1, v2, or v3).

© 2021 IP Infusion Inc. Proprietary

show igmp snooping mrouter

Use this command to display the multicast router interfaces, both configured and learned, in a VLAN.

Command Syntax

```
show igmp snooping mrouter IFNAME
```

Parameters

IFNAME	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command displays the multicast router interfaces in VLAN 1.1.

```
#show igmp snooping mrouter vlan1.1
VLAN    Interface             IP-address    Expires
1         xe1(static)
```

show igmp snooping statistics

Use this command to display IGMP Snooping statistics data.

Command Syntax

```
show igmp snooping statistics interface IFNAME
```

Parameters

IFNAME	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show igmp snooping statistics interface vlan1.1
IGMP Snooping statistics for vlan1.1
Group Count            :  1
IGMPv1 reports received  :  0
IGMPv2 reports received   :  0
IGMPv2 leaves received   :  0
IGMPv3 reports received   :  0
IGMPv1 query warnings  :  0
IGMPv2 query warnings  :  0
IGMPv3 query warnings  :  0
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 PIMv4 Commands

The chapter includes the commands that support the Protocol-Independent Multicast (PIM).

- clear ip mroute
- clear ip pim sparse-mode
- debug ip pim
- debug ip pim packet
- debug pim all
- debug ip pim timer assert
- debug ip pim timer bsr
- debug ip pim timer hello
- debug ip pim timer joinprune
- debug ip pim timer register
- ip pim
- ip pim accept-register
- ip pim anycast-rp
- ip pim bsr-border
- ip pim bsr-candidate
- ip pim cisco-register-checksum
- ip pim dr-priority
- ip pim exclude-genid
- ip pim hello-holdtime
- ip pim hello-interval
- ip pim ignore-rp-set-priority
- ip pim jp-timer
- ip pim neighbor-filter
- ip pim passive
- ip pim propagation-delay
- ip pim register-rate-limit
- ip pim register-rp-reachability
- ip pim register-source
- ip pim register-suppression
- ip pim router-id
- ip pim rp-address
- ip pim rp-candidate
- ip pim rp-register-kat
- ip pim spt-threshold
- ip pim ssm

© 2021 IP Infusion Inc. Proprietary

- ip pim state-refresh origination-interval
- ip pim unicast-bsm
- show debugging ip pim
- show debugging pim
- show ip pim bsr-router
- show ip pim interface
- show ip pim local-members
- show ip pim mroute
- show ip pim neighbor
- show ip pim nexthop
- show ip pim rp-hash
- show ip pim rp mapping
- snmp restart pim
- undebug all ip pim

© 2021 IP Infusion Inc. Proprietary

clear ip mroute

Use this command to delete all multicast route table entries and all multicast routes at the PIM protocol level.

Command Syntax

```
clear ip mroute *
clear ip mroute * pim (dense-mode|sparse-mode)
clear ip mroute A.B.C.D
clear ip mroute A.B.C.D A.B.C.D
clear ip mroute A.B.C.D A.B.C.D pim (dense-mode|sparse-mode)
clear ip mroute A.B.C.D pim sparse-mode
clear ip mroute statistics *
clear ip mroute statistics A.B.C.D
clear ip mroute statistics A.B.C.D A.B.C.D
clear ip mroute (vrf NAME|) *
clear ip mroute (vrf NAME|) * pim (dense-mode|sparse-mode)
clear ip mroute (vrf NAME|) A.B.C.D
clear ip mroute (vrf NAME|) A.B.C.D A.B.C.D
clear ip mroute (vrf NAME|) A.B.C.D A.B.C.D pim (dense-mode|sparse-mode)
clear ip mroute (vrf NAME|) A.B.C.D pim sparse-mode
clear ip mroute (vrf NAME|) statistics *
clear ip mroute (vrf NAME|) statistics A.B.C.D
clear ip mroute (vrf NAME|) statistics A.B.C.D A.B.C.D
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`*`	Delete all multicast routes
`pim`	Protocol Independent Multicast (PIM)
`A.B.C.D`	Clears group IP address
`A.B.C.D`	Clears source IP address
`dense-mode`	Clears multicast rout table for PIM dense-mode
`sparse-mode`	Clears multicast route table for PIM sparse mode
`statistics`	Clears multicast route statistics

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip mroute * pim sparse-mode
#clear ip mroute 224.2.2.2 4.4.4.4 pim sparse-mode
```

 © 2021 IP Infusion Inc. Proprietary

clear ip pim sparse-mode

Use this command to clear all rendezvous point (RP) sets learned through the PIMv2 Bootstrap Router (BSR).

Command Syntax

```
clear ip pim sparse-mode bsr rp-set *
clear ip pim (vrf NAME|) sparse-mode bsr rp-set *
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`rp-set`	PIMv2 bootstrap router RP set
`bsr`	PIMv2 Bootstrap Router
`*`	Clear all RP sets

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip pim sparse-mode bsr rp-set *
```

debug ip pim

Use this command to enable debugging for PIM.

Use the `no` option with this command to deactivate debugging for PIM.

Command Syntax

```
debug ip pim (all|events|mfc|mib|mtrace|nexthop|nsm|packet|state|timer)
debug ip pim (vrf NAME|)(all|events|mfc|mib|mtrace|nexthop|nsm|packet|state|timer)
no debug ip pim (all|events|mfc|mib|mtrace|nexthop|nsm|packet|state|timer)
no debug ip pim (vrf NAME|) (all|events|mfc|mib|mtrace|nexthop|nsm|packet
  |state|timer)
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`all`	Enable debugging for all PIM events
`events`	Enable debugging for general configuration, Virtual Routing (VR), and VRF context
`mfc`	Enable debugging for MFC updates
`mib`	Enable debugging for MIB entries
`mtrace`	Enable debugging for MTRACE messages
`nexthop`	Enable debugging for Reverse Path Forwarding (RPF) neighbor nexthop cache handling
`nsm`	Enable debugging for NSM
`packet`	Enable debugging for PIM packets
`state`	Enable debugging for PIM states
`timer`	Enable debugging for PIM timers

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug ip pim all
```


© 2021 IP Infusion Inc. Proprietary

debug ip pim packet

Use this command to activate debugging of incoming or outgoing PIM packets.

Use the `no` option with this command to deactivate debugging of incoming or outgoing PIM packets.

Command Syntax

```
debug ip pim packet
debug ip pim packet in
debug ip pim packet out
debug ip pim (vrf NAME|) packet
debug ip pim (vrf NAME|) packet in
debug ip pim (vrf NAME|) packet out
no debug ip pim packet
no debug ip pim packet in
no debug ip pim packet out
no debug ip pim (vrf NAME|) packet
no debug ip pim (vrf NAME|) packet in
no debug ip pim (vrf NAME|) packet out
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`in`	Debug incoming packets
`out`	Debug outgoing packets

Default

By default, all debug options are disabled.

Command Mode

Configure and Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ip pim packet in
```

debug pim all

Use this command to enable debugging of all PIM events.

Use the `no` option with this command to disable debugging for PIM.

Command Syntax

```
debug pim all
debug pim (vrf NAME|) all
no debug pim all
no debug pim (vrf NAME|) all
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug pim all
```


© 2021 IP Infusion Inc. Proprietary

debug ip pim timer assert

Use this command to enable debugging of the PIM assert timers.

Use the `no` option with this command to disable debugging for PIM assert timers.

Command Syntax

```
debug ip pim timer assert
debug ip pim timer assert at
debug ip pim (vrf NAME|) timer assert
debug ip pim (vrf NAME|) timer assert at
no debug ip pim timer assert
no debug ip pim timer assert at
no debug ip pim (vrf NAME|) timer assert
no debug ip pim (vrf NAME|) timer assert at
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`at`	Use this option to turn on or off debugging of the PIM Assert Timer

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip pim timer assert at
```

debug ip pim timer bsr

Use this command to enable debugging of PIM BSR time.

Use the `no` option with this command to disable debugging of the PIM BSR timer.

Command Syntax

```
debug ip pim timer bsr
debug ip pim timer bsr bst
debug ip pim timer bsr crp
debug ip pim (vrf NAME|) timer bsr
debug ip pim (vrf NAME|) timer bsr bst
debug ip pim (vrf NAME|) timer bsr crp
no debug ip pim timer bsr
no debug ip pim timer bsr bst
no debug ip pim timer bsr crp
no debug ip pim (vrf NAME|) timer bsr
no debug ip pim (vrf NAME|) timer bsr bst
no debug ip pim (vrf NAME|) timer bsr crp
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`bst`	Turn on or turn off the bootstrap debugging timer
`crp`	Turn on or turn off the Candidate-RP debugging timer

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ip pim timer bsr bst
```


© 2021 IP Infusion Inc. Proprietary

debug ip pim timer hello

Use this command to enable debugging of various PIM Hello timers.

Use the `no` option with this command to disable debugging of the PIM Hello timers.

Command Syntax

```
debug ip pim timer hello
debug ip pim timer hello ht
debug ip pim timer hello nlt
debug ip pim timer hello tht
debug ip pim (vrf NAME|) timer hello
debug ip pim (vrf NAME|) timer hello ht
debug ip pim (vrf NAME|) timer hello nlt
debug ip pim (vrf NAME|) timer hello tht
no debug ip pim timer hello
no debug ip pim timer hello ht
no debug ip pim timer hello nlt
no debug ip pim timer hello tht
no debug ip pim (vrf NAME|) timer hello
no debug ip pim (vrf NAME|) timer hello ht
no debug ip pim (vrf NAME|) timer hello nlt
no debug ip pim (vrf NAME|) timer hello tht
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`ht`	Turn on or turn off the PIM Hello debugging timer (ht)
`nlt`	Turn on or turn off the PIM Neighbor Liveliness debugging timer (nlt)
`tht`	Turn on or turn off the Triggered Hello Timer (tht)

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
```

```
(config)#debug ip pim timer hello ht
```


© 2021 IP Infusion Inc. Proprietary

debug ip pim timer joinprune

Use this command to enable debugging of various PIM JoinPrune timers.

Use the no option with this command to disable the debugging of the PIM JoinPrune timers.

Command Syntax

```
debug ip pim timer joinprune
debug ip pim timer joinprune et
debug ip pim timer joinprune kat
debug ip pim timer joinprune jt
debug ip pim timer joinprune ot
debug ip pim timer joinprune ppt
debug ip pim (vrf NAME|) timer joinprune
debug ip pim (vrf NAME|) timer joinprune et
debug ip pim (vrf NAME|) timer joinprune kat
debug ip pim (vrf NAME|) timer joinprune jt
debug ip pim (vrf NAME|) timer joinprune ot
debug ip pim (vrf NAME|) timer joinprune ppt
no debug ip pim timer joinprune
no debug ip pim timer joinprune et
no debug ip pim timer joinprune kat
no debug ip pim timer joinprune jt
no debug ip pim timer joinprune ot
no debug ip pim timer joinprune ppt
no debug ip pim (vrf NAME|) timer joinprune
no debug ip pim (vrf NAME|) timer joinprune et
no debug ip pim (vrf NAME|) timer joinprune kat
no debug ip pim (vrf NAME|) timer joinprune jt
no debug ip pim (vrf NAME|) timer joinprune ot
no debug ip pim (vrf NAME|) timer joinprune ppt
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`et`	Turn on or turn off the PIM JoinPrune expiry timer (et)
`jt`	Turn on or turn off the PIM JoinPrune upstream Join Timer (jt)
`kat`	Turn on or turn off the PIM JoinPrune Keep Alive timer (kat)
`ot`	Turn on or turn off the PIM JoinPrune Upstream Override Timer (ot)
`ppt`	Turn on or turn off the PIM JoinPrune PrunePending Timer ((ppt)

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip pim timer joinprune et
```


© 2021 IP Infusion Inc. Proprietary

debug ip pim timer register

Use this command to enable the PIM register timer's debugging.

Use the no option with this command to disable the PIM register timer's debugging.

Command Syntax

```
debug ip pim timer register
debug ip pim timer register rst
debug ip pim (vrf NAME|) timer register
debug ip pim (vrf NAME|) timer register rst
no debug ip pim timer register
no debug ip pim timer register rst
no debug ip pim (vrf NAME|) timer register
no debug ip pim (vrf NAME|) timer register rst
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`rst`	Turn on or turn off the PIM Register Stop Timer (rst)

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug ip pim timer register
```

ip pim

Use this command to enable PIM dense-mode or sparse-mode on the current interface.

Use the `no` option with this command to disable PIM dense-mode or sparse-mode or sparse-dense-mode on the interface.

Command Syntax

```
ip pim (dense-mode|sparse-mode)
```

```
no ip pim (dense-mode|sparse-mode)
```

Parameters

`dense-mode`	Enable PIM dense-mode operation
`sparse-mode`	Enable PIM sparse-mode

Default

By default, the ip pim option is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim dense-mode

(config)#interface eth0
(config-if)#no ip pim dense-mode

(config)#interface eth0
(config-if)#ip pim sparse-mode

(config-if)#no ip pim sparse-mode
```


© 2021 IP Infusion Inc. Proprietary

ip pim accept-register

Use this command to configure the ability to filter out multicast sources specified by the given access-list at the RP, so that the RP will accept/refuse to perform the Register mechanism for the packets sent by the specified sources. By default, the RP accepts Register packets from all multicast sources.

Use the no option with this command to revert to default.

Command Syntax

```
ip pim accept-register list WORD
ip pim (vrf NAME|) accept-register list WORD
no ip pim accept-register
no ip pim (vrf NAME|) accept-register
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`WORD`	Name of a standard access list

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim accept-register list xyz

(config)#no ip pim accept-register
```

ip pim anycast-rp

Use this command to configure the Anycast RP in the RP set.

Use the no option with this command to remove the configuration.

Command Syntax

```
ip pim anycast-rp A.B.C.D A.B.C.D
ip pim (vrf NAME|) anycast-rp A.B.C.D A.B.C.D
no ip pim anycast-rp A.B.C.D
no ip pim anycast-rp A.B.C.D A.B.C.D
no ip pim (vrf NAME|) anycast-rp A.B.C.D
no ip pim (vrf NAME|) anycast-rp A.B.C.D A.B.C.D
```

Parameters

`vrf`	The VPN routing/forwarding instance.
`NAME`	Specify the name of the VPN routing/forwarding instance.
`A.B.C.D`	Unicast IP address of the Anycast RP set. An Anycast RP set is a collection of RPs in the same domain.
`A.B.C.D`	Destination IP address where Register messages are copied and sent. A Member RP is an individual RP member in the Anycast RP set.

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows how to configure the Anycast RP in the RP set.

```
#configure terminal
(config)#ip pim anycast-rp 1.1.1.1 10.10.10.10
```

The following example shows how to remove the configuration.

```
#configure terminal
(config)#no ip pim anycast-rp 1.1.1.1 10.10.10.10
```


© 2021 IP Infusion Inc. Proprietary

ip pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface.

When this command is configured on an interface, no PIM Version 2 BSR messages are sent or received through the interface. Use this command to configure an interface bordering another PIM domain to avoid the exchange of BSR messages between the two domains. BSR messages should not be exchanged between different domains, because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in a protocol malfunction or loss of isolation between the domains.

Note: This command does not set up multicast boundaries. It only sets up a PIM domain BSR message border.

Use the `no` option with this command to remove the BSR border configuration.

Command Syntax

```
ip pim bsr-border
no ip pim bsr-border
```

Default

By default, the ip pim bsr-border is disabled.

Parameters

None

Default

Bootstrap router border configuration is disabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures the interface to be the PIM domain border:

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim bsr-border

(config)#interface eth0
(config-if)#no ip pim bsr-border
```

ip pim bsr-candidate

Use this command to give the router the candidate BSR status using the specified IP address of the interface.

Use the `no` option with this command to disable this function.

Command Syntax

```
ip pim bsr-candidate IFNAME
ip pim bsr-candidate IFNAME <0-32>
ip pim bsr-candidate IFNAME <0-32> <0-255>
ip pim (vrf NAME|) bsr-candidate IFNAME
ip pim (vrf NAME|) bsr-candidate IFNAME <0-32>
ip pim (vrf NAME|) bsr-candidate IFNAME <0-32> <0-255>
no ip pim bsr-candidate (IFNAME|)
no ip pim (vrf NAME|) bsr-candidate (IFNAME|)
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`IFNAME`	Specify the name of the interface
`<0-32>`	Specify a hash mask length for RP selection
`<0-255>`	Specify a priority for a BSR candidate

Default

The router is not configured to announce itself as a candidate BSR.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim bsr-candidate eth0 20 30
```


© 2021 IP Infusion Inc. Proprietary

ip pim cisco-register-checksum

Use this command to configure the option to calculate the register checksum over the whole packet. This command is used to inter-operate with older Cisco IOS versions.

Use the no option with this command to revert to the default settings.

Command Syntax

```
ip pim cisco-register-checksum
ip pim cisco-register-checksum group-list WORD
ip pim (vrf NAME|) cisco-register-checksum
ip pim (vrf NAME|) cisco-register-checksum group-list WORD
no ip pim cisco-register-checksum
no ip pim cisco-register-checksum group-list WORD
no ip pim (vrf NAME|) cisco-register-checksum
no ip pim (vrf NAME|) cisco-register-checksum group-list WORD
```

Parameters

`vrf`	The VPN routing/forwarding instance.
`NAME`	Specify the name of the VPN routing/forwarding instance.
`group-list`	Use this parameter to configure the option to calculate the register checksum over the whole packet on multicast groups specified by the access-list.
`WORD`	IP named standard access list.

Default

This command is disabled by default. By default, Register Checksum is calculated only over the header.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim cisco-register-checksum

#configure terminal
(config)#ip pim cisco-register-checksum group-list xyz
(config)#ip access-list 34 permit 224.0.1.3
```

ip pim dr-priority

Use this command to set the designated router's priority value.

Use the `no` option with this command to remove the priority from the DR.

Command Syntax

```
ip pim dr-priority <0-4294967294>
no ip pim dr-priority (<0-4294967294>|)
```

Parameter

`<0-4294967294>` Valid range of values for DR priority, with a higher value resulting in a higher preference

Default

The default DR priority value is 1.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim dr-priority 11234

(config)#interface eth0
(config-if)#no ip pim dr-priority 11234
```


© 2021 IP Infusion Inc. Proprietary

ip pim exclude-genid

Use this command to exclude the GenID (generated ID) option from Hello packets sent by the PIM module on an interface. This command is used to inter-operate with older Cisco IOS versions.

Use the `no` option with this command to restore PIM to its default setting.

Command Syntax

```
ip pim exclude-genid
no ip pim exclude-genid
```

Parameters

None

Default

By default, the ip pim exclude-genid command is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Default

By default, this command is disabled; that is, the GenID option is included.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim exclude-genid

(config)#interface eth0
(config-if)#no ip pim exclude-genid
```

ip pim hello-holdtime

Use this command to configure a hello holdtime other than the default (`3.5 * hello_interval` seconds).

When configuring `hello-holdtime`, if the configured value is less than the current `hello_interval`, it is refused.

When removing a configured `hello_holdtime`, the value is reset to (`3.5 *` current `hello_interval)` value.

Every time the hello_interval is updated, the hello-holdtime is also updated according to rules below:

If the hello_holdtime is not configured, or if the hello_holdtime is configured, but is less than the current hello_interval value, it is modified to (3.5 * hello_interval). Otherwise, the configured value is maintained.

Use the `no` option with this command to remove the configured hello-holdtime.

Command Syntax

```
ip pim hello-holdtime <1-65535>
no ip pim hello-holdtime
```

Parameter

`<1-65535>`	Range of values for hello-holdtime, in seconds

Default

The default hello-holdtime is 105 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim hello-holdtime 123

(config)#interface eth0
(config-if)#no ip pim hello-holdtime
```


© 2021 IP Infusion Inc. Proprietary

ip pim hello-interval

Use this command to configure a hello interval value other than the default. When a hello-interval is configured and hello-holdtime is not configured, or when the hello-holdtime value configured is less than the new hello-interval value, the holdtime value is modified to (3.5 * hello_interval). Otherwise, the hello-holdtime value is the configured value.

Use the `no` option with this command to reset the hello-interval to its default value.

Command Syntax

```
ip pim hello-interval <1-18724>
no ip pim hello-interval
```

Parameter

`<1-18724>`	Range of values for the hello-interval. No fractional values are allowed in seconds.

Default

The default value for hello-interval is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim hello-interval 123

(config)#interface eth0
(config-if)#no ip pim hello-interval
```

ip pim ignore-rp-set-priority

Use this command to ignore the RP-SET priority value, and use only the hashing mechanism for RP selection. This command is used to inter-operate with older Cisco IOS versions.

Use the `no` option with this command to remove this setting.

Command Syntax

```
ip pim ignore-rp-set-priority
ip pim (vrf NAME|) ignore-rp-set-priority
no ip pim ignore-rp-set-priority
no ip pim (vrf NAME|) ignore-rp-set-priority
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim ignore-rp-set-priority

#configure terminal
(config)#no ip pim ignore-rp-set-priority
```


© 2021 IP Infusion Inc. Proprietary

ip pim jp-timer

Use this command to set a PIM join/prune timer.

Use the `no` option with this command to remove the join/prune timer.

Command Syntax

```
ip pim jp-timer <1-65535>
ip pim (vrf NAME|) jp-timer <1-65535>
no ip pim jp-timer
no ip pim jp-timer <1-65535>
no ip pim (vrf NAME|) jp-timer
no ip pim (vrf NAME|) jp-timer <1-65535>
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<1-65535>`	Range of values for the Join/Prune timer, in seconds

Default

The ip pim jp-timer default value is 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim jp-timer 234

#configure terminal
(config)#no ip pim jp-timer 234
```

ip pim neighbor-filter

Use this command to enable filtering of neighbors on the interface. When configuring a neighbor filter, PIM either not establish adjacency with neighbor or terminates adjacency with existing neighbors, when denied by filtering access list.

Use the `no` option with this command to disable filtering of neighbors on the interface.

Command Syntax

```
ip pim neighbor-filter WORD
no ip pim neighbor-filter WORD
```

Parameters

`WORD`	Name of an IP standard access list

Default

By default, the ip pim option is disabled.

Command Mode

Interface mode

Default

This command is disabled by default there is no filtering.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim neighbor-filter xyz
(config-if)#exit
(config)#ip access-list deny 192.168.1.53
(config)#ip access-list permit any
```


© 2021 IP Infusion Inc. Proprietary

ip pim passive

Use this command to enable or disable passive mode operation for local members on the interface. Passive mode essentially stops PIM transactions on the interface, allowing only the Internet Group Management Protocol (IGMP) mechanism to be active.

Use the `no` option with this command to disable the passive mode.

Command Syntax

```
ip pim (dense-mode|sparse-mode) passive
```

```
no ip pim (dense-mode|sparse-mode) passive
```

Parameters

`dense-mode`	Enable passive operation for PIM dense-mode
`sparse-mode`	Enable passive operation for PIM sparse-mode

Default

By default, the ip pim option is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim dense-mode passive

(config)#interface eth0
(config-if)#no ip pim dense-mode passive

#configure terminal
(config)#interface eth0
(config-if)#ip pim sparse-mode passive

(config)#interface eth0
(config-if)#no ip pim sparse-mode passive
```

ip pim propagation-delay

Use this command to configure a propagation delay value for PIM.

Use the no option with this command to return the propagation delay to its default value.

Command Syntax

```
ip pim propagation-delay <0-32767>
no ip pim propagation-delay
```

Parameter

<0-32767>	Range of values for propagation delay, in milliseconds

Default

The default propagation delay is 500 milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim propagation-delay 1000

(config)#interface eth0
(config-if)#no ip pim propagation-delay
```


© 2021 IP Infusion Inc. Proprietary

ip pim register-rate-limit

Use this command to configure the rate of Register packets sent by this designated router (DR), in number of packets per second.

Use the no option to remove the register-rate-limit configuration.

Note: The configured rate is per (S,G) state, and is not a system-wide rate.

Command Syntax

```
ip pim register-rate-limit <1-65535>
ip pim (vrf NAME|) register-rate-limit <1-65535>
no ip pim register-rate-limit <1-65535|>
no ip pim (vrf NAME|) register-rate-limit <1-65535|>
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
<1-65535>	Range of values for packets to send per second

Default

No rate limit is set for PIM-SM register packets.

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim register-rate-limit 3444

#configure terminal
(config)#no ip pim register-rate-limit
```

ip pim register-rp-reachability

Use this command to enable the RP reachability check for PIM Registers at the DR.

Use the no option to reset to disable the RP reachability check for PIM Registers at the DR.

Note: “ip pim register-rp-reachability” is default configuration and it would not be shown in running-configuration, even if admin configures it. If admin does "no" command of this configuration, it would be shown in running-configuration.

Command Syntax

```
ip pim register-rp-reachability
ip pim (vrf NAME|) register-rp-reachability
no ip pim register-rp-reachability
no ip pim (vrf NAME|) register-rp-reachability
```

Parameter

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Default

The default setting is checking for rendezvous point reachability,

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim register-rp-reachability
```


© 2021 IP Infusion Inc. Proprietary

ip pim register-source

Use this command to configure the source address of Register packets sent by this DR, overriding the default source address, which is the address of the RPF interface toward the source host.

Use the `no` option to remove the source address of register packets sent by this DR, and reset it to use the default source address, that is, the address of the RPF interface toward the source host.

The configured address must be a reachable address so the RP can send corresponding Register-Stop messages in response. This address is usually the loopback interface address, but can also be other physical addresses. The address must be advertised by unicast routing protocols on the DR.

Note: The interface configured does not require PIM to be enabled.

Command Syntax

```
ip pim register-source A.B.C.D
ip pim register-source IFNAME
ip pim (vrf NAME|) register-source A.B.C.D
ip pim (vrf NAME|) register-source IFNAME
no ip pim register-source (A.B.C.D|)
no ip pim register-source (IFNAME|)
no ip pim (vrf NAME|) register-source (A.B.C.D|)
no ip pim (vrf NAME|) register-source (IFNAME|)
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`A.B.C.D`	The IP address to use as the source of the register packets
`IFNAME`	The name of the interface to use as the source of the register packets

Default

By default, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of a register message.

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim register-source 3.3.3.2
```

ip pim register-suppression

Use this command to configure the register-suppression time, in seconds, overriding the default value of 60 seconds. Configuring this value modifies register-suppression time at the DR; configuring this value at the RP modifies the RP-keepalive-period value if the `ip pim rp-register-kat` command is not used.

Use the no option to remove the register-suppression setting.

Command Syntax

```
ip pim register-suppression <1-65535>
ip pim (vrf NAME|) register-suppression <1-65535>
no ip pim register-suppression
no ip pim (vrf NAME|) register-suppression
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<1-65535>`	Range of values for register suppression time in seconds

Default

By default, the ip pim option is disabled.

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim register-suppression 555

#configure terminal
(config)#no ip pim register-suppression
```


© 2021 IP Infusion Inc. Proprietary

ip pim router-id

Use this command to configure PIM router-ID to uniquely identify the router.By default, PIM registers for the NSM router-id service. This command will override the router-id received from NSM.

Use the `no` option with this command to unconfigure PIM router-ID. This will make PIM fall back to the NSM router-id

Command Syntax

```
ip pim (vrf NAME|) router-id A.B.C.D
no ip pim (vrf NAME|) router-id A.B.C.D
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`A.B.C.D`	Specify the Router ID

Default

By default, the ip pim option is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim router-id 1.1.1.1

(config)#no ip pim router-id 1.1.1.1
```

ip pim rp-address

Use this command to statically configure Rendezvous Point (RP) address for multicast groups.

Use the `no` option to remove the RP address.

OcNOS PIM supports multiple static RPs. It also supports static-RP and Bootsrtrap Router (BSR) mechanism simultaneously. The following list states the correct usage of this command:

- If RP-address configured through BSR and RP-address configured statically are both available for a group range, the RP-address configured through BSR is chosen over statically configured RP-address.
- One static-RP can be configured for multiple group ranges using Access Lists. However, configuring multiple static RPs (using `ip pim rp-address` command) with the same RP address is not allowed. The static-RP can either be configured for the whole multicast group range `224/4` (without ACL) or for specific group ranges (using ACL). For example, configuring `ip pim rp-address 1.2.3.4` will configure static-RP 1.2.3.4 for the default group range `224/4`. Configuring `ip pim rp-address 5.6.7.8 grp-list` will configure static-RP `5.6.7.8` for all the group ranges represented by `Permit` filters in `grp-list` ACL.
- If multiple static-RPs are available for a group range, then one with the highest IP address is chosen.
- Only `permit` filters in ACL are considered as valid group ranges. The default `Permit` filter `0.0.0.0/0` is converted to default multicast filter `224/4`.
- When selecting static-RPs for a group range, the first element, with the static-RP with highest IP address, is chosen.
- Group mode and RP address mappings learned through BSR take precedence over mappings statistically defined by the `ip pim rp-address` command without the `override` keyword. Commands with the `override` keyword take precedence over dynamically learned mappings.

Command Syntax

```
ip pim rp-address A.B.C.D (override|)
ip pim rp-address A.B.C.D WORD (override|)
ip pim (vrf NAME|) rp-address A.B.C.D (override|)
ip pim (vrf NAME|) rp-address A.B.C.D WORD (override|)
no ip pim rp-address A.B.C.D
no ip pim rp-address A.B.C.D WORD
no ip pim (vrf NAME|) rp-address A.B.C.D
no ip pim (vrf NAME|) rp-address A.B.C.D WORD
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`WORD`	Access-list name
`override`	Static RP overrides dynamically-learned RP

Default

No PIM static group-to-RP mappings are configured.

© 2021 IP Infusion Inc. Proprietary

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#ip pim rp-address 3.3.3.3 xyz
```

ip pim rp-candidate

Use this command to give the router a candidate RP status using the IP address of the specified interface.

The groups specified will operate in PIM sparse mode; group-list specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address.

Use the `no` option along with this command to remove the settings.

Command Syntax

```
ip pim rp-candidate IFNAME (bidir|) ((group-list WORD)|) (interval <0-16383>|)
  (priority <0-255>|)
ip pim (vrf NAME) rp-candidate IFNAME (bidir|) ((group-list WORD)|) (interval <0-
  16383>|) (priority <0-255>|)
no ip pim rp-candidate (IFNAME|)
no ip pim (vrf NAME) rp-candidate (IFNAME|)
```

Parameters

`vrf NAME`	The VPN routing/forwarding instance
`IFNAME`	Specify an interface name
`WORD`	A named standard access list
`group-list`	Group Ranges for this C-RP
`interval`	C-RP advertisement interval
`priority`	Candidate-RP priority
`<0-16383>`	Range of values for candidate-RP advertisement interval, in seconds
`<0-255>`	Range of values for priority of an RP candidate

Default

The ip pim rp-candidate default priority is 192 and interval is 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim rp-candidate eth0

(config)#no ip pim rp-candidate eth0
```


© 2021 IP Infusion Inc. Proprietary

ip pim rp-register-kat

Use this command to configure a Keepalive Timer (KAT) value for (S,G) states at RP to monitor PIM register packets, overriding the generic KAT timer value.

Use the no option to remove this configuration.

Command Syntax

```
ip pim rp-register-kat <1-65535>
ip pim (vrf NAME|) rp-register-kat <1-65535>
no ip pim rp-register-kat
no ip pim (vrf NAME|) rp-register-kat
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
<1-65535>	Range of values for a KAT time in seconds

Default

The ip pim rp-register-kat default is 60 seconds.

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip pim rp-register-kat 3454

(config)#no ip pim rp-register-kat
```

ip pim spt-threshold

Use this command to turn on the ability of the last-hop PIM router to switch to SPT.

Use the `no` option with this command to turn off the ability of the last-hop PIM router to switch to SPT.

Note: This option is binary, meaning that the switching to SPT happens either at the receiving of the first data packet or not at all. It is not rate-based.

Command Syntax

```
ip pim spt-threshold
ip pim spt-threshold group-list WORD
ip pim (vrf NAME|) spt-threshold
ip pim (vrf NAME|) spt-threshold group-list WORD
no ip pim spt-threshold
no ip pim spt-threshold group-list WORD
no ip pim (vrf NAME|) spt-threshold
no ip pim (vrf NAME|) spt-threshold group-list WORD
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`group-list`	Enable the ability for the last-hop PIM router to switch to SPT for multicast group addresses indicated by the given access-list
`WORD`	A named standard access list

Default

When this command is not used, the PIM leaf router joins the shortest path tree immediately after the first packet arrives from a new source.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip pim spt-threshold

#configure terminal
(config)#ip pim spt-threshold group-list LIST1
(config)#ip access-list permit 224.0.1.3

#configure terminal
(config)#no ip pim spt-threshold
```


© 2021 IP Infusion Inc. Proprietary

ip pim ssm

Use this command to configure Source Specific Multicast (SSM) and define the range of multicast IP addresses. The keyword `default` defines the SSM range as 232/8. To define an SSM range other than the default, specify an access-list.

When an SSM range of IP multicast addresses is defined with this command, the no (*,G) or (S,G,rpt) state is initiated for groups in the SSM range.

The messages corresponding to these states are not accepted and originate in the SSM range.

Use the `no` form of this command to disable the SSM range.

Command Syntax

```
ip pim ssm default
ip pim ssm range WORD
ip pim (vrf NAME|) ssm default
ip pim (vrf NAME|) ssm range WORD
no ip pim ssm
no ip pim (vrf NAME|) ssm
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`default`	This keyword defines the 232/8 group range for SSM
`range`	Define an access-list for group range to use for SSM
`WORD`	A named standard access list

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows how to configure SSM service for the IP address range defined by access list 10:

```
#configure terminal
(config)#access-list 10 permit 225.1.1.1
(config)#ip pim ssm range xyz
```

ip pim state-refresh origination-interval

Use this command to configure a PIM-DM State-Refresh origination interval other than the default value. The origination interval is the number of seconds between PIM-DM State Refresh control messages.

Use the `no` option with this command to return the origination interval to its default value.

Command Syntax

```
ip pim state-refresh origination-interval <1-100>
no ip pim state-refresh origination-interval
```

Parameter

`<1-100>`	Range of values for state-refresh origination interval, in seconds

Note: No fractional values are allowed for the interval time.

Default

The default state-refresh origination interval is 60 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim state-refresh origination-interval 65

(config)#interface eth0
(config-if)#no ip pim state-refresh origination-interval
```


© 2021 IP Infusion Inc. Proprietary

ip pim unicast-bsm

Use this command to enable support for sending and receiving unicast Bootstrap Messages (BSM) on an interface. This command supports backward-compatibility with older versions of the Bootstrap Router specification, which specifies unicast BSM to refresh the state of new or restarting neighbors.

Use the `no` option with this command to disable unicast bootstrap messaging on an interface.

Command Syntax

```
ip pim unicast-bsm
```

```
no ip pim unicast-bsm
```

Parameters

None

Default

Unicast bootstrap messaging is disabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim unicast-bsm

(config)#interface eth0
(config-if)#no ip pim unicast-bsm
```

show debugging ip pim

Use this command to display the debug status for the PIM process.

Command Syntax

```
show debugging ip pim
show debugging ip pim (vrf NAME|)
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging ip pim
 PIM Debugging status:
 PIM event debugging is on
 PIM MFC debugging is on
 PIM state debugging is on
 PIM incoming packet debugging is on
 PIM outgoing packet debugging is on
 PIM Hello HT timer debugging is on
 PIM Hello NLT timer debugging is on
 PIM Hello THT timer debugging is on
 PIM Join/Prune JT timer debugging is on
 PIM Join/Prune ET timer debugging is on
 PIM Join/Prune PPT timer debugging is on
 PIM Join/Prune KAT timer debugging is on
 PIM Join/Prune OT timer debugging is on
 PIM Assert AT timer debugging is on
 PIM Register RST timer debugging is on
 PIM Bootstrap BST timer debugging is on
 PIM Bootstrap CRP timer debugging is on
 PIM mib debugging is on
 PIM nexthop debugging is on
 PIM mtrace debugging is on
 PIM NSM debugging is on
```


© 2021 IP Infusion Inc. Proprietary

show debugging pim

Use this command to display the status of debugging for PIM.

Command Syntax

```
show debugging pim
```

Parameters

None

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This command displays one of several status:

```
#show debugging pim
PIM Debugging status:
  PIM event debugging is on
  PIM MFC debugging is on
  PIM state debugging is on
  PIM incoming packet debugging is on
  PIM outgoing packet debugging is on
  PIM Hello HT timer debugging is on
  PIM Hello NLT timer debugging is on
  PIM Hello THT timer debugging is on
  PIM Join/Prune JT timer debugging is on
  PIM Join/Prune ET timer debugging is on
  PIM Join/Prune PPT timer debugging is on
  PIM Join/Prune KAT timer debugging is on
  PIM Join/Prune OT timer debugging is on
  PIM Assert AT timer debugging is on
  PIM Register RST timer debugging is on
  PIM Bootstrap BST timer debugging is on
  PIM Bootstrap CRP timer debugging is on
  PIM mib debugging is on
  PIM nexthop debugging is on
  PIM mtrace debugging is on
  PIM NSM debugging is on
```

© 2021 IP Infusion Inc. Proprietary

show ip pim bsr-router

Use this command to show the bootstrap router PIMv2 address.

Command Syntax

```
show ip pim bsr-router
show ip pim (vrf NAME|) bsr-router
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 10.10.11.35 (?)
  Uptime:      00:00:38, BSR Priority: 0, Hash mask length: 10
  Expires:     00:01:32
  Role: Non-candidate BSR
  State: Accept Preferred

#show ip pim bsr-router
PIMv2 Bootstrap information
 BSR address: 20.0.1.21
 Uptime:      00:40:20, BSR Priority: 64, Hash mask length: 10
 Expires:     00:02:07
 Role: Candidate BSR
 State: Candidate BSR
```

Table 4-202: show ip pim bsr-router output

Entry	Description
BSR address	Bootstrap Router's IP address.
Uptime	As stated
BSR Priority	BSR election priority; can be set manually, but default is 64.
Hash mask length	As stated.
Expires	Group-to-C-RP mapping Expiry Timer.

© 2021 IP Infusion Inc. Proprietary

Table 4-202: show ip pim bsr-router output (Continued)

Entry	Description
Role	Specifies whether the BSR is the Candidate BSR or a Non-candidate BSR
State	• The current state of a Candidate BSR, one of the following: Candidate-BSR, Pending-BSR, or Elected-BSR. • The current state of a Non-candidate BSR, one of the following: Accept Any or Accept Preferred.

show ip pim interface

Use this command to display PIM interface information.

Command Syntax

```
show ip pim interface
show ip pim interface detail
show ip pim (vrf NAME|) interface
show ip pim (vrf NAME|) interface detail
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`detail`	Display detailed information about a PIM interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
Router_E#show ip pim interface
Address         Interface  VIFindex Ver/   Nbr      DR      DR
                                    Mode   Count   Prior
192.168.1.10      eth1      0       v2/S   1         1     192.168.1.10
172.16.1.10       eth2      2       v2/S   1         1     172.16.1.10
```

The output for PIM ECMP Redirect is as below:

```
rtr6#show  ip pim  interface detail
eth1 (vif 0):
  Address 192.168.10.57, DR 192.168.10.57
  Hello period 30 seconds, Next Hello in 18 seconds
  Triggered Hello period 5 seconds
  Propagation delay is 1000 milli-seconds
  Interface ID: Router-ID:1.1.1.57 Local-ID 3
  Neighbors:
   192.168.10.52

eth2 (vif 2):
  Address 192.168.1.57, DR 192.168.1.152
  Hello period 30 seconds, Next Hello in 20 seconds
  Triggered Hello period 5 seconds
  Propagation delay is 1000 milli-seconds
  Interface ID: Router-ID:1.1.1.57 Local-ID 4
  ECMP REDIRECT, bundle : ecmpbundle, status :  allowed
  Neighbors:
```


© 2021 IP Infusion Inc. Proprietary

```
192.168.1.149
192.168.1.150
192.168.1.152
```

Table 4-203: show ip pim interface output

Entry	Description
Address	IP address of the interface
Interface	Interface name (eth1, xe3, ge4/1, etc.).
VIFindex	The index number of the Virtual Host Interface (vif).
Ver/Mode	PIM version (either v1, v2, or v3) / PIM Mode – Either S (sparse mode) or D (dense mode).
Nbr Count	Neighbor Count.
DR Prior	Designated Router Priority.
DR	Address of the Designated Router.
Hello Period	Routing devices send hello messages at a fixed interval on all PIM-enabled interfaces. By using hello messages, routing devices advertise their existence as PIM routing devices on the subnet.
Next Hello	When the interval counts down to 0, the routing device sends another hello message, and the timer is reset. A routing device that receives no response from a neighbor in 3.5 times the interval value drops the neighbor.
Propagation Delay	Vif Hello LAN Delay – propagation delay in milliseconds.
ECMP Redirect, bundle	An ECMP bundle is a set of PIM-enabled interfaces on a router, where all interfaces belonging to the same bundle share the same routing metric. The next hops for the ECMP are all one hop away. There can be one or more ECMP bundles on any router, while one individual interface can only belong to a single bundle. ECMP bundles are created on a router via configuration.
Neighbors	A list of the addresses of PIM multicast neighbors.

show ip pim local-members

Use this command to display information about local membership for PIM interfaces.

Command Syntax

```
show ip pim local-members
show ip pim local-members IFNAME
show ip pim (vrf NAME|) local-members
show ip pim (vrf NAME|) local-members IFNAME
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`IFNAME`	Display local membership for an interface name

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip pim vrf q local-members p8p1
PIM Local membership information

p8p1:
  (*, 233.5.5.5) : Include
  (*, 233.7.7.7) : Include
```

Table 4-204: show ip pim local-members output

Entry	Description
NAME:	Interface name
(*,G)	The local members in the form (Source/Group). Shows state – either Include or Exclude.

© 2021 IP Infusion Inc. Proprietary

show ip pim mroute

Use this command to display information in the IP PIM multicast routing table.

Command Syntax

```
show ip pim mroute (detail|)
show ip pim mroute A.B.C.D (detail|)
show ip pim mroute A.B.C.D A.B.C.D (detail|)
show ip pim (vrf NAME|) mroute (detail|)
show ip pim (vrf NAME|) mroute A.B.C.D (detail|)
show ip pim (vrf NAME|) mroute A.B.C.D A.B.C.D (detail|)
```

Parameter

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`A.B.C.D`	Display all entries for this group IP address
`A.B.C.D`	Display all entries for this source IP address

Note: A group IP address and a source IP address cannot be simultaneously

`detail`	Display detailed PIM multicast routing table information

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip pim mroute

IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
 Local     ..............................
 Joined    j..............................
 Asserted  ..............................
 Outgoing  o..............................
```

Table 4-205: show ip pim mroute output

Entry	Description
(*, *, RP) Entries:	Source, Group, Rendezvous Point Include entries.
(*, G) Entries:	PIM Include entries
(S, G) Entries:	PIM Include entries (Source, Group)
(S, G, rpt) Entries:	The RPT is the path between the RP and receivers (hosts) in a multicast group. The RPT is built by means of a PIM join message from a receiver's DR.
RP:	Rendezvous Point
RPF nbr:	Reverse Path Forwarding neighbor.
RPF idx:	Reverse Path Forwarding index.
Upstream State:	As stated.

© 2021 IP Infusion Inc. Proprietary

show ip pim neighbor

Use this command to display PIM neighbor information.

Command Syntax

```
show ip pim neighbor (detail|)
show ip pim neighbor IFNAME (detail|)
show ip pim neighbor IFNAME A.B.C.D (detail|)
show ip pim (vrf NAME|) neighbor (detail|)
show ip pim (vrf NAME|) neighbor IFNAME (detail|)
show ip pim (vrf NAME|) neighbor IFNAME A.B.C.D (default|)
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
IFNAME	Name of the interface
A.B.C.D	IPv4 address of the neighbor interface
detail	Display detailed information for a PIM neighbor

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ip pim neighbor
Neighbor      Interface    Uptime/Expires     Ver          DR
Address                                                 Priority/Mode
10.10.14.11    eth3       00:14:30/00:01:45    v2         1 / DR
```

The validation command to view PIM ECMP Redirect is as below:

```
rtr6#show  ip pim  neighbor detail
Nbr 192.168.10.52 (eth1)
Expires in 83 seconds, uptime 00:21:52
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 1048865461,

Nbr 192.168.1.149 (eth2)
Expires in 99 seconds, uptime 00:22:06
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 2102076842,
Interface ID: Router-ID: 1.1.1.149 Local-ID: 4,
ECMP REDIRECT enabled
```

```
Nbr 192.168.1.150 (eth2)
Expires in 77 seconds, uptime 00:22:02
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 1306457151,
Interface ID: Router-ID: 1.1.1.153 Local-ID: 4,
ECMP REDIRECT enabled

Nbr 192.168.1.152 (eth2), DR
Expires in 86 seconds, uptime 00:22:06
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 170629600,
Interface ID: Router-ID: 1.1.1.152 Local-ID: 4,
ECMP REDIRECT enabled
```

Table 4-206: show ip pim neighbor output

Entry	Description
Neighbor	Neighbor IP address
Interface	Name of the interface (eth1, xe3, xe5/1 etc.).
Uptime/Expires	Neighbor’s uptime / time until uptime expires and starts sending hello messages.
Ver	PIM version (version1 =v1, version2 - v2, version3 = v3).
DR Priority/mode	Priority and Mode of neighbor as Designated Router.
Nbr	NEighbor IP address and interface name (eth1, xe3, xe5/1 etc.).
Expires in	Time before the Hello timer expires and must retransmit.
uptime	Neighbor uptime.
Holdtime:	Before an interface goes down or changes primary IP address, a Hello message with a zero HoldTime should be sent immediately (with the old IP address if the IP address changed). This will cause PIM neighbors to remove this neighbor (or its old IP address) immediately. After an interface has changed its IP address, it MUST send a Hello message with its new IP address. If an interface changes one of its secondary IP addresses, a Hello message with an updated Address_List option and a non-zero HoldTime should be sent immediately. This will cause PIM neighbors to update this neighbor's list of secondary addresses immediately.
T-bit:	RPT-bit is a 1-bit value. The RPT-bit is set to 1 for Assert(*,G) messages and 0 for Assert(S,G) messages.

© 2021 IP Infusion Inc. Proprietary

Table 4-206: show ip pim neighbor output

Entry	Description
Lan delay:	In addition to the information recorded for the DR Election, the following per neighbor information is obtained from the LAN Prune Delay Hello option: In addition to the information recorded for the DR Election, the following per neighbor information is obtained from the LAN Prune Delay Hello option: neighbor.lan_prune_delay_present A flag indicating if the LAN Prune Delay option was present in the Hello message. neighbor.tracking_support A flag storing the value of the T bit in the LAN Prune Delay option if it is present in the Hello message. This indicates the neighbor's capability to disable Join message suppression. neighbor.propagation_delay The Propagation Delay field of the LAN Prune Delay option (if present) in the Hello message. neighbor.override_interval The Override_Interval field of the LAN Prune Delay option (if present) in the Hello message. The additional state described above is deleted along with the DR neighbor state when the neighbor timeout expires.
Override interval:	Hello Override Interval
DR priority:	The DR_Priority Option allows a network administrator to give preference to a particular router in the DR election process by giving it a numerically larger DR Priority.The DR_Priority Option SHOULD be included in every Hello message, even if no DR Priority is explicitly configured on that interface. This is necessary because priority-based DR election is only enabled when all neighbors on an interface advertise that they are capable of using the DR_Priority Option. The default priority is 1.
Gen ID:	Generation Identifier, used to detect reboots.
Interface ID:	As stated.
Router-ID:	As stated.
Local-ID:	As stated.
ECMP REDIRECT	Whether ECMP Redirect is enabled or disabled.

show ip pim nexthop

Displays the nexthop information from NSM as used by PIM.

Command Syntax

```
show ip pim nexthop
show ip pim (vrf NAME|) nexthop
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip pim nexthop
```


© 2021 IP Infusion Inc. Proprietary

show ip pim rp-hash

Use this command to display the rendezvous point (RP) to chose based on the group selected.

Command Syntax

```
show ip pim rp-hash A.B.C.D
show ip pim (vrf NAME|) rp-hash A.B.C.D
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
A.B.C.D	Specify a group address

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

A.B.C.D in command refers to the group address to be hashed.

```
#show ip pim rp-hash 224.0.1.3
Group(s): 224.0.0.0/4
    RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap
```

Table 4-207: Show ip PIM rp-hash output

Entry	Description
Group(s)	The group address to be hashed.
RP	Rendezvous Point
Info source	The address and identity from which this information was received. In the example above, it was learned from the bootstrap router.

show ip pim rp mapping

Use this command to show group-to-RP (rendezvous point) mappings, and the RP set.

Command Syntax

```
show ip pim rp mapping
show ip pim (vrf NAME|) rp mapping
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip pim rp mapping
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
 RP: 10.10.1.5
    Info source: 172.16.1.2, via bootstrap, priority 192
         Uptime: 00:00:13, expires: 00:02:29
 RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap, priority 2
         Uptime: 00:34:42, expires: 00:01:49
```

Table 4-208: Show ip PIM rp mapping output

Entry	Description
Identity declaration	This system is the Bootstrap Router (PIM version number v1, v2. or, v3) or not the Bootstrap Router.
Group(s):	The Multicast address of this multicast Group.
RP	Addresses of the Rendezvous Points.
Info source:	Address of the info source, whether it was learned from the Bootstrap Router, and the configured priority.

© 2021 IP Infusion Inc. Proprietary

snmp restart pim

Use this command to restart SNMP in (PIM).

Note: This command restarts IPv4 PIM daemon

Command Syntax

```
snmp restart pim
```

Parameters

None

Default

By default, the snmp restart pim is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart pim
```

undebug all ip pim

Use this command to disable all PIM debugging from Configure mode.

Command Syntax

```
undebug all ip pim
undebug (vrf NAME|) all ip pim
```

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#undebug all ip pim
```


© 2021 IP Infusion Inc. Proprietary

SECTION 8

Carrier Ethernet

Carrier Ethernet Configuration Guide

Contents

This document contains these chapters and appendices:

- Chapter 1, *Link Layer Discovery Protocol Configuration*
- Chapter 2, *G.8032 ERPS Version 2*
- Chapter 3, *Ethernet CFM Configurations*
- Chapter 4, *Provider Bridging Configuration*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Link Layer Discovery Protocol Configuration

This chapter contains a complete sample Link Layer Discovery Protocol (LLDP) configuration.

LLDP is a neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise themselves to other devices on the same physical LAN, and then to store information about the network. It allows a device to learn higher-layer management reachability and connection endpoint information from adjacent devices. Using LLDP, a network device is able to advertise its identity, its capabilities and its media-specific configuration, as well as learn the same information from other connected devices.

Note: The `lldp-agent` command is not supported for SVLAN, VLAN, and loop-back interfaces.

Topology

Figure 1-18 displays a sample LLDP topology.

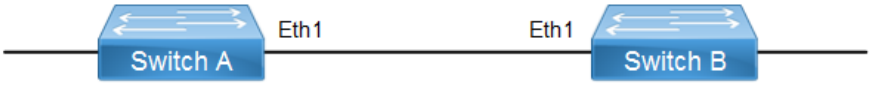


Figure 1-18: LLDP Topology

Interface Mode TLV

Default Agent

All configuration commands in the table below should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the `port-description TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the `system-name TLV` to be transmitted on the port

`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the `system-capabilities TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the `system-description TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the `management-address TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the `VLAN-id TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the `VLAN-NAME TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the `Port and Protocol VLAN id TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the `Protocol Identity TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the `VID Usage Digest TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the `Management VID TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the `Link Aggregation TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLDPDUs that are transmitted during a fast transmission period
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch

```
#show running-config lldp
!
interface eth1
lldp-agent
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
```


© 2021 IP Infusion Inc. Proprietary

```
  lldp tlv ieee-8021-org-specific mgmt-vid select
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6
!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 nearest-bridge

Agent Mode                    : Nearest bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 5
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Not Defined
 Traffic statistics           :
  Total frames transmitted    : 4
  Total entries aged          : 0
  Total frames received       : 3
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
```

Customer Bridge

All configuration commands in the table below should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent customer-bridge`	Enter into the Customer Bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the port-description TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the system-name TLV to be transmitted on the port.

`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the system-capabilities TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the system-description TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the management-address TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the VLAN-id TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the VLAN-NAME TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the Protocol Identity TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the Management VID TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the Link Aggregation TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port.
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods.
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLD PDUs that are transmitted during a fast transmission period.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch:

```
#show #show running-config lldp
!
interface eth1
lldp-agent customer-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
  lldp tlv ieee-8021-org-specific mgmt-vid select
```


© 2021 IP Infusion Inc. Proprietary

```
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6
!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 customer-bridge

Agent Mode                    : Customer-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 5
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Not Defined
 Traffic statistics           :
  Total frames transmitted    : 8
  Total entries aged          : 0
  Total frames received       : 7
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
```

Non-Tpmr-Bridge

The below configurations should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the Non tpmr Bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the port-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the system-name TLV to be transmitted on the port

`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the system-capabilities TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the system-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the management-address TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the VLAN-id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the VLAN-NAME TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the Protocol Identity TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the Management VID TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the Link Aggregation TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLD PDUs that are transmitted during a fast transmission period
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch:

```
#show running-config lldp
lldp-agent non-tpmr-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
  lldp tlv ieee-8021-org-specific mgmt-vid select
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
```


© 2021 IP Infusion Inc. Proprietary

```
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6

!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 non-tmpr-bridge

Agent Mode                    : Non-TPMR-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 5
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : Not Defined
 Traffic statistics           :
  Total frames transmitted    : 17
  Total entries aged          : 0
  Total frames received       : 6
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
```

Media Endpoint Devices TLV

Switch A

`(config)#interface eth1`	Enter interface mode.
`(config-if)#lldp-agent`	Enter the default agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#lldp-agent customer-bridge`	Enter the customer-bridge agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#lldp-agent non-tpmr-bridge`	Enter the non-tpmr-bridge agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#set lldp med-devtype net-connect`	Enter the med-devtype agent and set the device type to network connectivity.
`(config-if)#exit`	Exit agent mode.

Validation

```
#show run lldp
!
!
interface eth1
 lldp-agent
```

```
  set lldp enable txrx
 set lldp med-devtype net-connect
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
 lldp-agent customer-bridge
  set lldp enable txrx
!
#

#show lldp interface eth1
Agent Mode                    : Customer-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : Network Connectivity
 Traffic statistics           :
  Total frames transmitted    : 97
  Total entries aged          : 1
  Total frames received       : 92
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
Agent Mode                    : Non-TPMR-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Network Connectivity
 Traffic statistics           :
  Total frames transmitted    : 89
  Total entries aged          : 0
  Total frames received       : 0
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
Agent Mode                    : Nearest bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Network Connectivity
 Traffic statistics           :
  Total frames transmitted    : 90
  Total entries aged          : 0
```


© 2021 IP Infusion Inc. Proprietary

```
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
#
```

Switch B

(config)#interface eth1	Enter interface mode.
(config-if)#lldp-agent	Enter the default agent.
(if-lldp-agent)#set lldp enable txrx	Set the admin status of the LLDP agent.
(if-lldp-agent)#exit	Exit agent mode.
(config-if)#lldp-agent customer-bridge	Enter the customer-bridge agent.
(if-lldp-agent)#set lldp enable txrx	Set the admin status of the LLDP agent.
(if-lldp-agent)#exit	Exit agent mode.
(config-if)#lldp-agent non-tpmr-bridge	Enter the non-tpmr-bridge agent.
(if-lldp-agent)#set lldp enable txrx	Set the admin status of the LLDP agent.
(if-lldp-agent)#exit	Exit agent mode.
(config-if)#set lldp med-devtype ep-class3	Enter the med-devtype agent and set the device type to endpoint class 3.
(config-if)#exit	Exit agent mode.

Validation

```
#show running-config lldp
!
!
interface eth1
 lldp-agent
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
 set lldp med-devtype ep-class3
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
 lldp-agent customer-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
!
#

#show lldp interface eth1
Agent Mode                   : Customer-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
```

```
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 11
  Total entries aged         : 0
  Total frames received      : 12
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 7
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Nearest bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 8
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
#
```

Global Mode TLV

LLDPv2 TLVs can be configured globally, making it applicable for all interfaces where LLDP is enabled.

© 2021 IP Infusion Inc. Proprietary

Topology

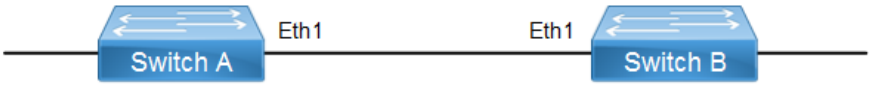


Figure 1-19: LLDP topology

SW1

`SW1#configure terminal`	Enter Configure mode
`SW1(config)#lldp tlv-select basic-mgmt port-description`	Enable LLDP port description TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-name`	Enable LLDP system name TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-capabilities`	Enable LLDP system capabilities TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-description`	Enable LLDP system description TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt management-address`	Enable LLDP management address TLV in global mode
`SW1(config)#interface eth1`	Enter interface mode
`SW1(config-if)#lldp-agent`	Enter LLDP interface mode
`SW1(if-lldp-agent)#set lldp enable txrx`	Enable LLDP TLV transmit and receive for the nearest bridge
`SW1(if-lldp-agent)#exit`	Exit LLDP mode
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#end`	Exit the configure mode

SW2

`SW2#configure terminal`	Enter Configure mode
`SW2(config)#lldp tlv-select basic-mgmt port-description`	Enable LLDP port description TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-name`	Enable LLDP system name TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-capabilities`	Enable LLDP system capabilities TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-description`	Enable LLDP system description TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt management-address`	Enable LLDP management address TLV in global mode
`SW2(config)#interface eth1`	Enter interface mode
`SW2(config-if)#lldp-agent`	Enter LLDP interface mode
`SW2(if-lldp-agent)#set lldp enable txrx`	Enable LLDP TLV transmit and receive for the nearest bridge
`SW2(if-lldp-agent)#exit`	Exit LLDP mode
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#end`	Exit the configure mode

© 2021 IP Infusion Inc. Proprietary

Validation

```
SW1#show running-config lldp
!
lldp tlv-select basic-mgmt port-description
lldp tlv-select basic-mgmt system-name
lldp tlv-select basic-mgmt system-capabilities
lldp tlv-select basic-mgmt system-description
lldp tlv-select basic-mgmt management-address
!
interface eth1
 lldp-agent
  set lldp enable txrx


SW1#show lldp neighbors

Loc PortID      Rem Host Name      Rem Chassis Id     Rem Port Id       Agent Mode

--------------------------------------------------------------------------------
Eth1           OcNOS              cc37.ab56.6d80     cc37.abbb.ed81   Nearest bridge


SW1#show lldp neighbors detail

--------------------------------------------------------------------------------

Nearest bridge Neighbors
Interface Name              : eth1
 Mandatory TLVs
 Chassis id type          : MAC address [cc37.ab56.6d80]
 Port id type             : MAC address [cc37.abbb.ed81]
 Time to live             : 121
 Basic Management TLVs
 System Name              : SW2
 System Description       : Hardware Model:EC_AS4610-54, Software version: Oc
NOS,1.3.6.241a
 Port Description          : eth1
 Remote System Capabilities : Bridge
                              Router
 Capabilities Enabled     : Router
 Management Address        : MAC Address [cc37.abbb.ed81]
 Interface Number subtype  : ifindex
 Interface Number          10046
 OID Number              : 0
 802.1 Org specific TLVs
 Port vlan id              : 0
 Port & Protocol vlan id   : 0
 Remote Configured VLANs   : None
 Remote Protocols Advertised: None
```

 © 2021 IP Infusion Inc. Proprietary

```
 Remote VID Usage Digest   : 0
 Remote Management Vlan    : 0
 Link Aggregation Capability: not capable of being aggregated
 Link Aggregation Status   : not currently in aggregation
 Link Aggregation Port ID  :
 802.3 Org specific TLVs
 AutoNego Support          : Not-Supported
 AutoNego Status           : Disabled
 AutoNego Capability       : 0
 Operational MAU Type      : 0 [unknown]
  Max Frame Size            :
SW1#
```

LLDP-MED

LLDP extensions and behavior requirements are described specifically in the areas of network Configuration and policy, device location (including for Emergency Call Service / E911), Power over Ethernet management, and inventory management.

Based on the device type, different TLVs are advertised by the Station.

LLDP-MED Network Connectivity Device

LLDP-MED Network Connectivity Devices, as defined in this Standard, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

- LAN Switch/Router
- IEEE 802.1 Bridge
- IEEE 802.3 Repeater (included for historical reasons)
- IEEE 802.11 Wireless Access Point
- Any device that supports the IEEE 802.1AB and MED extensions defined by this Standard and can relay IEEE 802 frames via any method.

Configuration Command

```
set lldp med-devtype net-connect
```

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services.

Configuration command:

```
set lldp med-devtype ep-class1
```

LLDP-MED Generic Endpoint (Class 2)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar

Configuration command:

```
set lldp med-devtype ep-class2
```

LLDP-MED Generic Endpoint (Class 3)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Configuration command:

```
set lldp med-devtype ep-class3
```

Switch A

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(if-config-if)#lldp-agent customer-bridge`	Enter into the customer-bridge agent.
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the non-tpmr-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.

© 2021 IP Infusion Inc. Proprietary

`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#set lldp med-devtype net-connect`	Configure the med device type
`(config-if)#exit`	Exit interface mode.

Switch B

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent customer-bridge`	Enter into the customer-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the non-tpmr-bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#set lldp med-devtype ep-class3`	Configure the med device type
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations on Switch A:

```
#show running-config lldp
!
!
interface eth1
 lldp-agent
  set lldp enable txrx
 set lldp med-devtype net-connect
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
 lldp-agent customer-bridge
  set lldp enable txrx
!
```

2. Verify the LLDP port statistics on Switch A:

```
#show lldp interface eth1
Agent Mode                    : Customer-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : Network Connectivity
 Traffic statistics           :
  Total frames transmitted    : 11
  Total entries aged          : 0
  Total frames received       : 10
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
Agent Mode                    : Non-TPMR-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Network Connectivity
 Traffic statistics           :
  Total frames transmitted    : 7
  Total entries aged          : 0
  Total frames received       : 0
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
Agent Mode                    : Nearest bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Network Connectivity
 Traffic statistics           :
  Total frames transmitted    : 7
  Total entries aged          : 0
  Total frames received       : 0
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0

#show lldp interface eth1 non-tpmr-bridge
Agent Mode                    : Non-TPMR-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 5
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Not Defined
 Traffic statistics           :
  Total frames transmitted    : 4
```

 © 2021 IP Infusion Inc. Proprietary

```
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
```

3. Verify the LLDP configurations for end device ep-class3 on Switch B:

```
#show running-config lldp
!
interface eth1
 set lldp med-devtype ep-class3
 lldp-agent
  set lldp enable txrx
  lldp tlv med network-policy select
lldp-agent non-TPMR-bridge
  set lldp enable txrx
  lldp tlv med network-policy select
lldp-agent customer-bridge
  set lldp enable txrx
  lldp tlv med network-policy select
!
```

4. Verify the LLDP port statistics on Switch B:

```
#show lldp interface eth1
Agent Mode                  : Customer-bridge
 Enable (tx/rx)             : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 124
  Total entries aged         : 0
  Total frames received      : 125
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                  : Non-TPMR-bridge
 Enable (tx/rx)             : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 120
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                  : Nearest bridge
```

```
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : End Point Class-3
 Traffic statistics           :
  Total frames transmitted    : 120
  Total entries aged          : 0
  Total frames received       : 0
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
#
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 G.8032 ERPS Version 2

G.8032 is an International Telecommunication Union (ITU) standard for ERPS. It prevents loops on a per-VLAN basis with networks that are wired in a simple ring topology. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

G.8032 Version 2 provides enhancements in support of multiple ring and ladder topologies. G.8032 offers a rapid detection and recovery time if a link or node.

This guide contains topologies and examples on how to configure g8032 ERPS configuration.

Topology

Figure 2-20 displays a sample Ring Protection topology on which protection switching is configured with four bridges. The Ring Protection Link (RPL) owner is the link between Bridge 3 and Bridge 4 (xe16), on which one side of the link is defined explicitly as RPL owner (Bridge 4) and RPL neighbor (Bridge 3). The rest of the bridges are explicitly configured RPL non owner to enable ERPS in the ring.

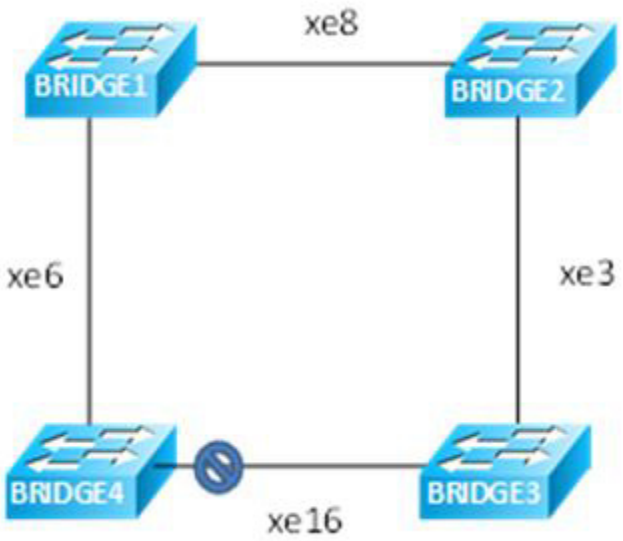


Figure 2-20: Major Ring Topology

Bridge 1

`Bridge1#configure terminal`	Enter configure mode
`Bridge1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge1((config)#vlan database`	Configure VLAN database
`Bridge1(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge1(config-vlan)#interface xe6`	Configure interface xe6

`Bridge1(config-if)#switchport`	Configure xe6 as a layer 2 port
`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe6 interface
`Bridge1(config-if)#interface xe8`	Configure interface xe8
`Bridge1(config-if)#switchport`	Configure xe8 as a layer 2 port
`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe8 interface
`Bridge1(config-if)#ethernet cfm domain-type character-string domain-name nod12 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod12 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 12 active true local-vid 200 xe8`	Create down mep 12 with local vid 200 for xe8 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 21`	Configure crosscheck to remote MEP with value 21
`Bridge1(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod41 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod41 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 14 active true local-vid 200 xe6`	Create down mep 14 with local vid 200 for xe6 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode

© 2021 IP Infusion Inc. Proprietary

`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 41`	Configure crosscheck to remote MEP with value 41
`Bridge1(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#g8032 physical-ring RING1 bridge 1`	Create g8032 physical ring with name RING1 on bridge 1
`Bridge1(g8032-ring-config)#east-interface xe6`	Associate xe6 interface as east-interface
`Bridge1(g8032-ring-config)#west-interface xe8`	Associate xe8 interface as west-interface
`Bridge1(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge1(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge1(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge1(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge1(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge1(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge1(g8032-config-switch)#physical-ring RING1`	Associate Physical ring RING1 to erp1 instance
`Bridge1(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge1(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge1(g8032-config-switch)#level 7`	Configure level as 7
`Bridge1(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge1(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge1(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge1(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 2

`Bridge2#config terminal`	Enter configure mode
`Bridge2(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge2((config)#vlan database`	Configure VLAN database
`Bridge2(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge2(config-vlan)#interface xe3`	Configure interface xe3

`Bridge2(config-if)#switchport`	Configure xe3 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe3 interface
`Bridge2(config-if)#interface xe8`	Configure interface xe8
`Bridge2(config-if)#switchport`	Configure xe8 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe8 interface
`Bridge2(config-if)#ethernet cfm domain-type character-string domain-name nod23 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod23 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 23 active true local-vid 200 xe3`	Create down mep 23 with local vid 200 for xe3 interface
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 32`	Configure crosscheck to remote MEP with value 32
`Bridge2(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod12 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod12 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 21 active true local-vid 200 xe8`	Create down mep 21 with local vid 200 for xe8 interface
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 12`	Configure crosscheck to remote MEP with value 12
`Bridge2(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3

© 2021 IP Infusion Inc. Proprietary

`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#g8032 physical-ring RING1 bridge 1`	Create g8032 physical ring with name RING1 on bridge 1
`Bridge2(g8032-ring-config)#east-interface xe8`	Associate xe8 interface as east-interface
`Bridge2(g8032-ring-config)#west-interface xe3`	Associate xe3 interface as west-interface
`Bridge2(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge2(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge2(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge2(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge2(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge2(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge2(g8032-config-switch)#physical-ring RING1`	Associate Physical ring RING1 to erp1 instance
`Bridge2(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge2(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge2(g8032-config-switch)#level 7`	Configure level as 7
`Bridge2(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge2(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge2(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge2(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 3

`Bridge3#config terminal`	Enter configure mode
`Bridge3(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge3((config)#vlan database`	Configure VLAN database
`Bridge3(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge3(config-vlan)#interface xe3`	Configure interface xe3
`Bridge3(config-if)#switchport`	Configure xe3 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface

`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe3 interface
`Bridge3(config-if)#interface xe16`	Configure interface xe16
`Bridge3(config-if)#switchport`	Configure xe16 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe16 interface
`Bridge3(config-if)#ethernet cfm domain-type character-string domain-name nod23 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod23 and set mip creation criteria to default with level 7 on bridge 1
`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 32 active true local-vid 200 xe3`	Create down mep 32 with local vid 200 for xe3 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 23`	Configure crosscheck to remote MEP with value 23
`Bridge3(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod34 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod34 and set mip creation criteria to default with level 7 on bridge 1
`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 34 active true local-vid 200 xe16`	Create down mep 34 with local vid 200 for xe16 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 43`	Configure crosscheck to remote MEP with value 43
`Bridge3(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#g8032 physical-ring RING1 bridge 1`	Create g8032 physical ring with name RING1 on bridge 1

© 2021 IP Infusion Inc. Proprietary

`Bridge3(g8032-ring-config)#east-interface xe3`	Associate xe3 interface as east-interface
`Bridge3(g8032-ring-config)#west-interface xe16`	Associate xe16 interface as west-interface
`Bridge3(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge3(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge3(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge3(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge3(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge3(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge3(g8032-config-switch)#physical-ring RING1`	Associate Physical ring RING1 to erp1 instance
`Bridge3(g8032-config-switch)#rpl role neighbor west-interface`	Configure RPL node as neighbor node on west-interface
`Bridge3(g8032-config-switch)#profile profile1`	Associate profile profile1 to erp1 instance
`Bridge3(g8032-config-switch)#level 7`	Configure level as 7
`Bridge3(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge3(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge3(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge3(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 4

`Bridge4#config term`	Enter configure mode
`Bridge4(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge4((config)#vlan database`	Configure VLAN database
`Bridge4(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge4(config-vlan)#interface xe6`	Configure interface xe6
`Bridge4(config-if)#switchport`	Configure xe6 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe6 interface
`Bridge4(config-if)#interface xe16`	Configure interface xe16

`Bridge4(config-if)#switchport`	Configure xe16 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe16 interface
`Bridge4(config-if)#ethernet cfm domain-type character-string domain-name nod34 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod34 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 43 active true local-vid 200 xe16`	Create down mep 43 with local vid 200 for xe16 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 34`	Configure crosscheck to remote MEP with value 34
`Bridge4(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod41 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod41 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200.
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 41 active true local-vid 200 xe6`	Create down mep 41 with local vid 200 for xe6 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 14`	Configure crosscheck to remote MEP with value 14
`Bridge4(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#g8032 physical-ring RING1 bridge 1`	Create g8032 physical ring with name RING1 on bridge 1
`Bridge4(g8032-ring-config)#east-interface xe16`	Associate xe16 interface as east-interface
`Bridge4(g8032-ring-config)#west-interface xe6`	Associate xe6 interface as west-interface

© 2021 IP Infusion Inc. Proprietary

`Bridge4(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge4(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge4(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge4(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge4(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge4(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge4(g8032-config-switch)#physical-ring RING1`	Associate Physical ring RING1 to erp1 instance
`Bridge4(g8032-config-switch)#rpl role owner east-interface`	Configure the node as owner node on east-interface
`Bridge4(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge4(g8032-config-switch)#level 7`	Configure level as 7
`Bridge4(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge4(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge4(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge4(g8032-config-switch)#end`	Exit g8032 erp instance mode

Validation

```
Bridge1:
show g8032 aps-statistics erp1 bridge 1

Instance   : erp1
==========
Tx   : 3205
Rx   : 27

show g8032 physical-ring RING1 bridge 1

Ring          : RING1
===============
Description   :
East          : xe16
West          : xe6
ERP Inst      : erp1

show g8032 profile profile1 bridge 1

Profile : profile1
=========
 Wait-To-Restore : 1 mins
 Hold Off Timer  : 0.00 secs
```

```
 Guard Timer     : 10 ms
 Wait-To-Block   : 5010 ms
 Protection Type : Revertive

Bridge1:
show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : RING1
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : 3c:2c:99:26:e6:80
-------------------------------------------------------
                   East Link           West Link
=======================================================
Interface       :  xe6                 xe8
State           :  Unblocked           Unblocked
Remote NodeId   :  34:17:eb:e4:af:11   -
Remote BPR      :  1                   -
Endpoint Info
-------------
Domain Name     :  nod41               nod12
MEP ID          :  14                  12
MA Name         :  43982               43982
=======================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   1)         |
===========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge2:
show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : RING1
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : d8:9e:f3:5e:f8:29
-------------------------------------------------------
                   East Link           West Link
=======================================================
Interface       :  xe8                 xe3
State           :  Unblocked           Unblocked
Remote NodeId   :  34:17:eb:e4:af:11   -
Remote BPR      :  1                   -
Endpoint Info
-------------
Domain Name     :  nod12               nod23
```


© 2021 IP Infusion Inc. Proprietary

```
MEP ID          :  21                  23
MA Name         :  43982               43982
============================================================
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 201-205
Profile : profile1

sBridge3:
show g8032 erp-instance erp1 bridge 1
Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : RING1
Ring Type       : MAJOR-RING
Role            : NEIGHBOR (WEST)
Node ID         : 3c:2c:99:1a:da:7d
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  xe3                 xe16
State           :  Unblocked           Blocked
Remote NodeId   :  34:17:eb:e4:af:11   34:17:eb:e4:af:11
Remote BPR      :  1                   1
Endpoint Info
-------------
Domain Name     :  nod23               nod34
MEP ID          :  32                  34
MA Name         :  43982               43982
============================================================
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge4:
show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : RING1
Ring Type       : MAJOR-RING
Role            : OWNER (EAST)
Node ID         : 34:17:eb:e4:af:11
------------------------------------------------------------
                   East Link           West Link
```

```
============================================================
Interface       :  xe16                 xe6
State           :  Blocked              Unblocked
Remote NodeId   :  -                    -
Remote BPR      :  -                    -
Endpoint Info
-------------
Domain Name     :  nod34                nod41
MEP ID          :  43                   41
MA Name         :  43982                43982
============================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   1)         |
===========================

DataTraffic vlan: 201-205
Profile : profile1
```


© 2021 IP Infusion Inc. Proprietary

Sub-ring with Virtual Channel

An ethernet ring that is connected to a Major Ring at the Interconnection Nodes. By itself, the Sub-Ring does not constitute a closed ring. A Sub-Ring is connected to the Interconnection nodes on only one port which is configured as east-interface.

Topology

Figure 2-21 displays a sample Ring Protection topology on which protection switching is configured with six bridges. This constitutes of one major ring (Bridge2, Bridge3, Bridge4 and Bridge 5) and one sub-ring (Bridge2, Bridge1, Bridge6 and Bridge5).

Major ring's RPL in enabled between Bridge 3(owner node) and Bridge 4(neighbor node) on xe4 and other devices are non-owner nodes for that ring. Sub-ring's RPL is enabled between bridge 1(owner node) and bridge 2 (neighbor node) on link xe2 and other devices on the non-owner nodes. Bridge 2 and Bridge 5 are called interconnected nodes since they are common node between major ring and subring. Virtual channel is enabled for this Subring on interconnected nodes on vlan 100 and tcn propagation is enabled.

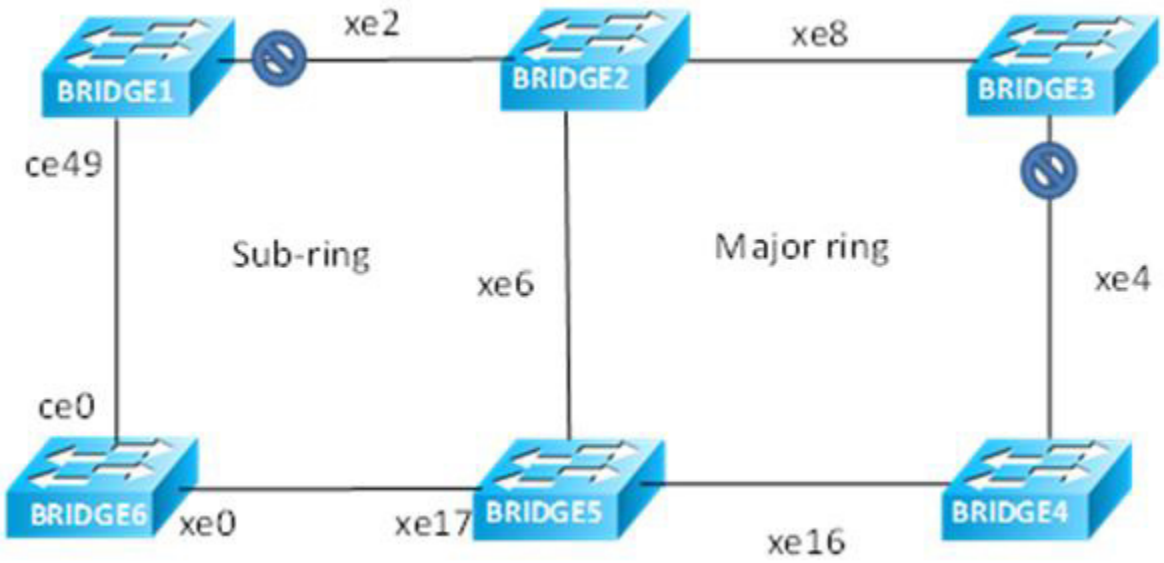


Figure 2-21: Major ring and Sub-ring with Virtual Channel Topology

Bridge 1

`Bridge1#config term`	Enter configure mode
`Bridge1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge1((config)#vlan database`	Configure VLAN database
`Bridge1(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge1(config)#interface ce49`	Configure interface ce49
`Bridge1(config-if)#switchport`	Configure ce49 as a layer 2 port

`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on ce49 interface
`Bridge1(config-if)#interface xe2`	Configure interface xe2
`Bridge1(config-if)#switchport`	Configure xe2 as a layer 2 port
`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe2 interface
`Bridge1(config-if)#ethernet cfm domain-type character-string domain-name 00061 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00061 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201.
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 16 active true local-vid 201 ce49`	Create down mep 16 with local vid 201 for ce49 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 61`	Configure crosscheck to remote MEP with value 61
`Bridge1(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00012 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00012 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 12 active true local-vid 201 xe2`	Create down mep 12 with local vid 201 for xe2 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 21`	Configure crosscheck to remote MEP with value 21
`Bridge1(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3

© 2021 IP Infusion Inc. Proprietary

`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#g8032 physical-ring subring bridge 1`	Create g8032 physical ring with name subring on bridge 1
`Bridge1(g8032-ring-config)#east-interface ce49`	Associate ce49 interface as east-interface
`Bridge1(g8032-ring-config)#west-interface xe2`	Associate xe2 interface as west-interface
`Bridge1(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge1(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge1(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge1(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge1(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge1(g8032-profile-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge1(g8032-config-switch)#ring-type sub-ring`	Configure ring type as subring
`Bridge1(g8032-config-switch)#physical-ring subring`	Associate Physical ring subring to erp2 instance
`Bridge1(g8032-config-switch)#rpl role owner west-interface`	Configure the node as owner node on west-interface
`Bridge1(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge1(g8032-config-switch)#level 7`	Configure level as 7
`Bridge1(g8032-config-switch)#raps-channel-vlan 201`	Configure RAPS channel vlan as 201
`Bridge1(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge1(g8032-config-switch)#ring-id 1`	Configure ring-id as 1

Bridge 2

`Bridge2#config term`	Enter configure mode
`Bridge2(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge2((config)#vlan database`	Configure VLAN database
`Bridge2(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100 on bridge 1
`Bridge2(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge2(config)#interface xe2`	Configure interface xe2
`Bridge2(config-if)#switchport`	Configure xe2 as a layer 2 port

`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe2 interface
`Bridge2(config-if)#interface xe6`	Configure interface xe6
`Bridge2(config-if)#switchport`	Configure xe6 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe6 interface
`Bridge2(config-if)#interface xe8`	Configure interface xe8
`Bridge2(config-if)#switchport`	Configure xe8 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe8 interface
`Bridge2(config-if)#ethernet cfm domain-type character-string domain-name 00012 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00012 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 21 active true local-vid 201 xe2`	Create down mep 21 with local vid 201 for xe2 interface
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 12`	Configure crosscheck to remote MEP with value 12
`Bridge2(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00052 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00052 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 25 active true local-vid 200 xe6`	Create down mep 25 with local vid 200 for xe6 interface

© 2021 IP Infusion Inc. Proprietary

`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 52`	Configure crosscheck to remote MEP with value 52
`Bridge2(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00023 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00023 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 23 active true local-vid 200 xe8`	Create down mep 23 with local vid 200 for xe8 interface
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 32`	Configure crosscheck to remote MEP with value 32
`Bridge2(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#g8032 physical-ring ring bridge 1`	Create g8032 physical ring with name ring on bridge 1
`Bridge2(g8032-ring-config)#east-interface xe6`	Associate xe6 interface as east-interface
`Bridge2(g8032-ring-config)#west-interface xe8`	Associate xe8 interface as west-interface
`Bridge2(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge2(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge2(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge2(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge2(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge2(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge2(g8032-config-switch)#physical-ring ring`	Associate Physical ring RING1 to erp1 instance
`Bridge2(g8032-config-switch)#ring-type major-ring`	Configure ring-type as major ring

`Bridge2(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge2(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge2(g8032-config-switch)#level 7`	Configure level as 7
`Bridge2(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge2(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge2(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge2(g8032-config-switch)#g8032 physical-ring subring bridge 1`	Create g8032 physical ring with name subring on bridge 1
`Bridge2(g8032-ring-config)#east-interface xe2`	Associate xe2 interface as east-interface
`Bridge2(g8032-ring-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge2(g8032-config-switch)#ring-type sub-ring`	Configure ring-type as sub-ring
`Bridge2(g8032-config-switch)#physical-ring subring`	Associate Physical ring RING1 to erp2 instance
`Bridge2(g8032-config-switch)#rpl role neighbor east-interface`	Configure the node as neighbor node on east interface
`Bridge2(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge2(g8032-config-switch)#level 7`	Configure level as 7
`Bridge2(g8032-config-switch)#raps-channel-vlan 201`	Configure RAPS channel vlan as 201
`Bridge2(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge2(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge2(g8032-config-switch)#virtual-channel 100 attached-to-instance erp1`	Configure virtual channel with vlan 100 and attach erp2 to erp1
`Bridge2(g8032-config-switch)#tcn-propogation enable`	Enable tcn propogation
`Bridge2(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 3

`Bridge3#config term`	Enter configure mode
`Bridge3(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge3((config)#vlan database`	Configure VLAN database
`Bridge3(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100 on bridge 1
`Bridge3(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge3(config)#interface xe8`	Configure interface xe8

© 2021 IP Infusion Inc. Proprietary

`Bridge3(config-if)#switchport`	Configure xe8 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe8 interface
`Bridge3(config-if)#interface xe4`	Configure interface xe4
`Bridge3(config-if)#switchport`	Configure xe4 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe4 interface
`Bridge3(config-if)#ethernet cfm domain-type character-string domain-name 00023 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00023 and set mip creation criteria to default with level 7 on bridge 1
`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 32 active true local-vid 200 xe8`	Create down mep 32 with local vid 200 for xe8 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 23`	Configure crosscheck to remote MEP with value 23
`Bridge3(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00034 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00034 and set mip creation criteria to default with level 7 on bridge 1
`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 34 active true local-vid 200 xe4`	Create down mep 34 with local vid 200 for xe4 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 43`	Configure crosscheck to remote MEP with value 43
`Bridge3(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3

`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#g8032 physical-ring ring bridge 1`	Create g8032 physical ring with name ring on bridge 1
`Bridge3(g8032-ring-config)#east-interface xe8`	Associate xe8 interface as east-interface
`Bridge3(g8032-ring-config)#west-interface xe4`	Associate xe4 interface as west-interface
`Bridge3(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge3(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge3(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge3(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge3(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge3(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge3(g8032-config-switch)#physical-ring ring`	Associate Physical ring ring to erp1 instance
`Bridge3(g8032-config-switch)#ring-type major-ring`	Configure ring-type as major ring
`Bridge3(g8032-config-switch)#rpl role owner west-interface`	Configure the node as owner node on west interface
`Bridge3(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge3(g8032-config-switch)#level 7`	Configure level as 7
`Bridge3(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge3(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge3(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge3(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 4

`Bridge4#config term`	Enter configuration mode
`Bridge4(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge4((config)#vlan database`	Configure VLAN database
`Bridge4config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100 on bridge 1
`Bridge4(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge4(config)#interface xe4`	Configure interface xe4

© 2021 IP Infusion Inc. Proprietary

`Bridge4(config-if)#switchport`	Configure xe4 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe4 interface
`Bridge4(config-if)#interface xe16`	Configure interface xe16
`Bridge4(config-if)#switchport`	Configure xe4 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe16 interface
`Bridge4(config-if)#ethernet cfm domain-type character-string domain-name 00034 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00023 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 43 active true local-vid 200 xe4`	Create down mep 43 with local vid 200 for xe4 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 34`	Configure crosscheck to remote MEP with value 34
`Bridge4(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00045 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00045 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 45 active true local-vid 200 xe16`	Create down mep 45 with local vid 200 for xe16 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 54`	Configure crosscheck to remote MEP with value 54
`Bridge4(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3

`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#g8032 physical-ring ring bridge 1`	Create g8032 physical ring with name ring on bridge 1
`Bridge4(g8032-ring-config)#east-interface xe4`	Associate xe4 interface as east-interface
`Bridge4(g8032-ring-config)#west-interface xe16`	Associate xe16 interface as west-interface
`Bridge4(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge4(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge4(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge4(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge4(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge4(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge4(g8032-config-switch)#ring-type major-ring`	Configure ring-type as major ring
`Bridge4(g8032-config-switch)#physical-ring ring`	Associate Physical ring ring to erp1 instance
`Bridge4(g8032-config-switch)#rpl role neighbor east-interface`	Configure the node as neighbor node on east interface
`Bridge4(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge4(g8032-config-switch)#level 7`	Configure level as 7
`Bridge4(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge4(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge4(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge4(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 5

`Bridge5#config term`	Enter configure mode
`Bridge5(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge5((config)#vlan database`	Configure VLAN database
`Bridge5(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100 on bridge 1
`Bridge5(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge5(config)#interface xe16`	Configure interface xe16

© 2021 IP Infusion Inc. Proprietary

`Bridge5(config-if)#switchport`	Configure xe16 as a layer 2 port
`Bridge5(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge5(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge5(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge5(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe16 interface
`Bridge5(config-if)#interface xe6`	Configure interface xe6
`Bridge5(config-if)#switchport`	Configure xe6 as a layer 2 port
`Bridge5(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge5(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge5(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge5(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe6 interface
`Bridge5(config-if)#interface xe17`	Configure interface xe17
`Bridge5(config-if)#switchport`	Configure xe17 as a layer 2 port
`Bridge5(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge5(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge5(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge5(config-if)#switchport trunk allowed vlan add 100,200-205`	Allow vlan 100,200-205 on xe17 interface
`Bridge5(config-if)#ethernet cfm domain-type character-string domain-name 00045 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00045 and set mip creation criteria to default with level 7 on bridge 1
`Bridge5(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 54 active true local-vid 200 xe16`	Create down mep 54 with local vid 200 for xe16 interface
`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 45`	Configure crosscheck to remote MEP with value 45
`Bridge5(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge5(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00052 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00052 and set mip creation criteria to default with level 7 on bridge 1
`Bridge5(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200

`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 52 active true local-vid 200 xe6`	Create down mep 52 with local vid 200 for xe6 interface
`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 25`	Configure crosscheck to remote MEP with value 25
`Bridge5(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge5(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00056 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00056 and set mip creation criteria to default with level 7 on bridge 1
`Bridge5(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201
`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 56 active true local-vid 201 xe17`	Create down mep 56 with local vid 201 for xe17 interface
`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 65`	Configure crosscheck to remote MEP with value 65
`Bridge5(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge5(config-ether-cfm)#g8032 physical-ring ring bridge 1`	Create g8032 physical ring with name ring on bridge 1
`Bridge5(g8032-ring-config)#east-interface xe16`	Associate xe16 interface as east-interface
`Bridge5(g8032-ring-config)#west-interface xe6`	Associate xe6 interface as west-interface
`Bridge5(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge5(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge5(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge5(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge5(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge5(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1

© 2021 IP Infusion Inc. Proprietary

`Bridge5(g8032-config-switch)#physical-ring ring`	Associate Physical ring ring to erp1 instance
`Bridge5(g8032-config-switch)#ring-type major-ring`	Configure ring-type as major ring
`Bridge5(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge5(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge5(g8032-config-switch)#level 7`	Configure level as 7
`Bridge5(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge5(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge5(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge5(g8032-config-switch)#g8032 physical-ring subring bridge 1`	Create g8032 physical ring with name subring on bridge 1
`Bridge5(g8032-ring-config)#east-interface xe17`	Associate xe17 interface as east-interface
`Bridge5(g8032-profile-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge5(g8032-config-switch)#ring-type sub-ring`	Configure ring-type as sub-ring
`Bridge5(g8032-config-switch)#physical-ring subring`	Associate Physical ring subring to erp2 instance
`Bridge5(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge5(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge5(g8032-config-switch)#level 7`	Configure level as 7
`Bridge5(g8032-config-switch)#raps-channel-vlan 201`	Configure RAPS channel vlan as 201
`Bridge5(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge5(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge5(g8032-config-switch)#virtual-channel 100 attached-to-instance erp1`	Configure virtual channel with vlan 100 and attach erp2 to erp1
`Bridge5(g8032-config-switch)#tcn-propogation enable`	Enable tcn propogation
`Bridge5(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 6

`Bridge6#config term`	Enter configuration mode
`Bridge6(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge6((config)#vlan database`	Configure VLAN database

`Bridge6(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge6(config)#interface xe0`	Configure interface xe0
`Bridge6(config-if)#switchport`	Configure xe0 as a layer 2 port
`Bridge6(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge6(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge6(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge6(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on xe0 interface
`Bridge6(config-if)#interface ce0`	Configure interface ce0
`Bridge6(config-if)#switchport`	Configure ce0 as a layer 2 port
`Bridge6(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge6(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge6(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge6(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on ce0 interface
`Bridge6(config-if)#ethernet cfm domain-type character-string domain-name 00056 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00056 and set mip creation criteria to default with level 7 on bridge 1
`Bridge6(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201.
`Bridge6(config-ether-cfm-ma)#ethernet cfm mep down mpid 65 active true local-vid 201 xe0`	Create down mep 65 with local vid 201 for xe0 interface
`Bridge6(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge6(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge6(config-ether-cfm-ma)#mep crosscheck mpid 56`	Configure crosscheck to remote MEP with value 56
`Bridge6(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge6(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge6(config-ether-cfm)#ethernet cfm domain-type character-string domain-name 00061 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name 00061 and set mip creation criteria to default with level 7 on bridge 1
`Bridge6(config-ether-cfm)#service ma-type string ma-name 43982 vlan 201 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 201
`Bridge6(config-ether-cfm-ma)#ethernet cfm mep down mpid 61 active true local-vid 201 ce0`	Create down mep 61 with local vid 201 for ce0 interface
`Bridge6(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge6(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode

© 2021 IP Infusion Inc. Proprietary

`Bridge6(config-ether-cfm-ma)#mep crosscheck mpid 16`	Configure crosscheck to remote MEP with value 16
`Bridge6(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge6(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge6(config-ether-cfm)#g8032 physical-ring subring bridge 1`	Create g8032 physical ring with name subring on bridge 1
`Bridge6(g8032-ring-config)#east-interface xe0`	Associate xe0 interface as east-interface
`Bridge6(g8032-ring-config)#west-interface ce0`	Associate ce0 interface as west-interface
`Bridge6(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge6(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge6(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge6(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge6(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge6(g8032-profile-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge6(g8032-config-switch)#ring-type sub-ring`	Configure ring type as subring
`Bridge6(g8032-config-switch)#physical-ring subring`	Associate Physical ring subring to erp2 instance
`Bridge6(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge6(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge6(g8032-config-switch)#level 7`	Configure level as 7
`Bridge6(g8032-config-switch)#raps-channel-vlan 201`	Configure RAPS channel vlan as 201
`Bridge6(g8032-config-switch)#data-traffic-vlan 202-205`	Configure traffic vlan from 202-205
`Bridge6(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge6(g8032-config-switch)#end`	Exit g8032 erp instance mode

Validation

```
Bridge1#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : subring
Ring Type       : SUB-RING
Role            : OWNER (WEST)
Node ID         : 6c:b9:c5:67:72:1d
```

```
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  ce49                xe2
State           :  Unblocked           Blocked
Remote NodeId   :  -                   -
Remote BPR      :  -                   -
Endpoint Info
-------------
Domain Name     :  00061               00012
MEP ID          :  16                  12
MA Name         :  43982               43982
============================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    201,   1)         |
===========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge2#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : subring
Ring Type       : SUB-RING (VIRTUAL)
Role            : NEIGHBOR (EAST)
Node ID         : 3c:2c:99:26:e6:7c
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  xe2                 -
State           :  Blocked             -
Remote NodeId   :  6c:b9:c5:67:72:1d   -
Remote BPR      :  0                   -
Endpoint Info
-------------
Domain Name     :  00012               -
MEP ID          :  21                  -
MA Name         :  43982               -
============================================================
TCN Propagation : Enabled
Attached        : -
Attached To     : erp1,
Virtual ID      : 100 : 1
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    201,   1)         |
===========================
```


© 2021 IP Infusion Inc. Proprietary

```
DataTraffic vlan: 202-205
Profile : profile1


Bridge2#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : ring
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : 3c:2c:99:26:e6:80
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  xe6                 xe8
State           :  Unblocked           Unblocked
Remote NodeId   :  -                   d8:9e:f3:5e:f8:29
Remote BPR      :  -                   0
Endpoint Info
-------------
Domain Name     :  00052               00023
MEP ID          :  25                  23
MA Name         :  43982               43982
============================================================
TCN Propagation : Disabled
Attached        : erp2,
Attached To     : -
Virtual ID      : -:-
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   1)         |
===========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge3#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : ring
Ring Type       : MAJOR-RING
Role            : OWNER (WEST)
Node ID         : d8:9e:f3:5e:f8:29
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  xe8                 xe4
State           :  Unblocked           Blocked
Remote NodeId   :  -                   -
Remote BPR      :  -                   -
```

```
Endpoint Info
-------------
Domain Name     :  00023               00034
MEP ID          :  32                  34
MA Name         :  43982               43982
============================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   1)         |
===========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge4#show  g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : ring
Ring Type       : MAJOR-RING
Role            : NEIGHBOR (EAST)
Node ID         : 3c:2c:99:1a:da:7e
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  xe4                 xe16
State           :  Blocked             Unblocked
Remote NodeId   :  d8:9e:f3:5e:f8:29   d8:9e:f3:5e:f8:29
Remote BPR      :  0                   0
Endpoint Info
-------------
Domain Name     :  00034               00045
MEP ID          :  43                  45
MA Name         :  43982               43982
============================================================
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    200,   1)         |
===========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge5#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : subring
Ring Type       : SUB-RING (VIRTUAL)
```


© 2021 IP Infusion Inc. Proprietary

```
Role            : NON-OWNER
Node ID         : 34:17:eb:e4:af:12
-------------------------------------------------------
                   East Link           West Link
=======================================================
Interface       :  xe17                -
State           :  Unblocked           -
Remote NodeId   :  6c:b9:c5:67:72:1d   -
Remote BPR      :  0                   -
Endpoint Info
-------------
Domain Name     :  00056               -
MEP ID          :  56                  -
MA Name         :  43982               -
=======================================================
TCN Propagation : Enabled
Attached        : -
Attached To     : erp1,
Virtual ID      : 100 : 1
---------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
===========================
 (7,    201,   1)         |
===========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge5#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : ring
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : 34:17:eb:e4:af:11
-------------------------------------------------------
                   East Link           West Link
=======================================================
Interface       :  xe16                xe6
State           :  Unblocked           Unblocked
Remote NodeId   :  -                   d8:9e:f3:5e:f8:29
Remote BPR      :  -                   0
Endpoint Info
-------------
Domain Name     :  00045               00052
MEP ID          :  54                  52
MA Name         :  43982               43982
=======================================================
TCN Propagation : Disabled
Attached        : erp2,
Attached To     : -
Virtual ID      : -:-
---------------------------
```

```
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 202-205
Profile : profile1


Bridge6#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : subring
Ring Type       : SUB-RING
Role            : NON-OWNER
Node ID         : b8:6a:97:d2:27:c6
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  xe0                 ce0
State           :  Unblocked           Unblocked
Remote NodeId   :  -                   6c:b9:c5:67:72:1d
Remote BPR      :  -                   0
Endpoint Info
-------------
Domain Name     :  00056               00061
MEP ID          :  65                  61
MA Name         :  43982               43982
============================================================
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    201,   1)         |
==========================

DataTraffic vlan: 202-205
Profile : profile1
```


© 2021 IP Infusion Inc. Proprietary

Sub-ring without Virtual Channel on a LAG interface

Figure 3 displays a sample Ring Protection topology on which protection switching is configured with 5 bridges on lag interfaces. The topology contains one major ring and one subring with non-virtual channel. The Ring Protection Link (RPL) for major ring is the link between Bridge 4 (owner) and Bridge 3 (neighbor) on lag interface po3. The subring is configured with no virtual channel and it's RPL link is configured between bridge 1 (neighbor) and bridge 5 (owner) on lag interface po6. The rest of the bridges are explicitly configured RPL non owner to enable ERPS in the ring in both major and subring.

Topology

Figure 2-22 displays a sample Ethernet Ring Protection Switching topology.

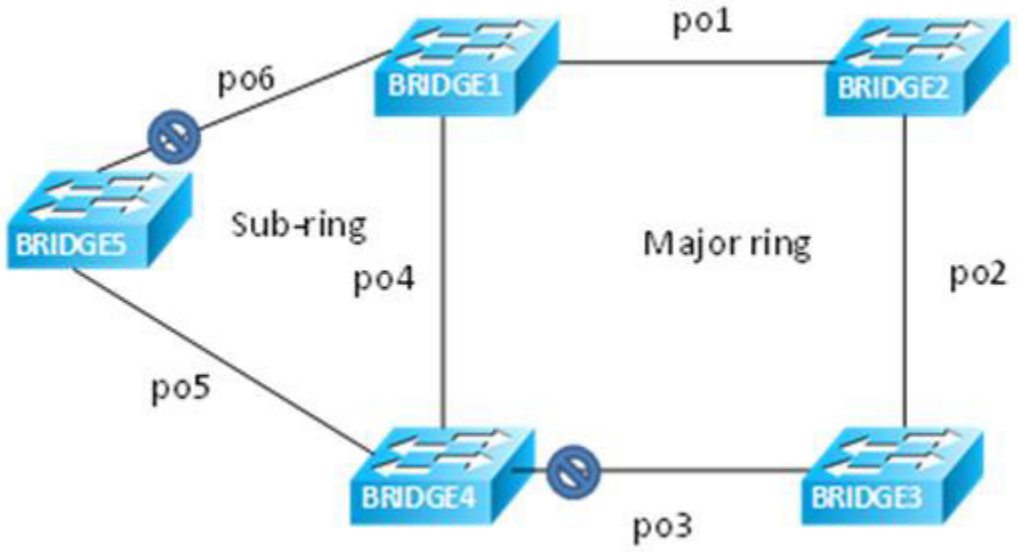


Figure 2-22: Major ring and sub-ring topology using LAG interface without a virtual channel

Bridge 1

`Bridge1#config term`	Enter configure mode
`Bridge1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge1((config)#vlan database`	Configure VLAN database
`Bridge1(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge1(config-vlan)#interface po1`	Configure lag interface po1
`Bridge1(config-if)#switchport`	Configure po1 as a layer 2 port
`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port

`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po1 interface
`Bridge1(config-if)#interface po4`	Configure lag interface po4
`Bridge1(config-if)#switchport`	Configure po4 as a layer 2 port
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Configure interface in bridge group 1
`Bridge1(config-if)#switchport mode trunk`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po4 interface
`Bridge1(config-if)#interface po6`	Configure lag interface po6
`Bridge1(config-if)#switchport`	Configure po6 as a layer 2 port
`Bridge1(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge1(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge1(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po6 interface
`Bridge1(config-if)#interface xe1`	Configure interface xe1
`Bridge1(config-if)#channel-group 6 mode active`	Configure xe1 as part of po6
`Bridge1(config-if)#interface xe2`	Configure interface xe2
`Bridge1(config-if)#channel-group 6 mode active`	Configure xe2 as part of po6
`Bridge1(config-if)#interface xe6`	Configure interface xe6
`Bridge1(config-if)#channel-group 4 mode active`	Configure xe6 as part of po4
`Bridge1(config-if)#interface xe7`	Configure interface xe7
`Bridge1(config-if)#channel-group 4 mode active`	Configure xe7 as part of po4
`Bridge1(config-if)#interface xe8`	Configure interface xe8
`Bridge1(config-if)#channel-group 1 mode active`	Configure xe8 as part of po1
`Bridge1(config-if)#interface xe9`	Configure interface xe9
`Bridge1(config-if)#channel-group 1 mode active`	Configure xe9 as part of po1
`Bridge1(config-if)#ethernet cfm domain-type character-string domain-name nod12 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod12 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 12 active true local-vid 200 po1`	Create down mep 12 with local vid 200 for po1 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode

© 2021 IP Infusion Inc. Proprietary

`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 21`	Configure crosscheck to remote MEP with value 21
`Bridge1(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod41 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod41 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 14 active true local-vid 200 po4`	Create down mep 14 with local vid 200 for po4 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 41`	Configure crosscheck to remote MEP with value 41
`Bridge1(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod15 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod15 and set mip creation criteria to default with level 7 on bridge 1
`Bridge1(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 51 active true local-vid 200 po6`	Create down mep 51 with local vid 200 for po6 interface
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 15`	Configure crosscheck to remote MEP with value 15
`Bridge1(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge1(config-ether-cfm)#g8032 physical-ring lagring bridge 1`	Create g8032 physical ring with name lagring on bridge 1
`Bridge1(g8032-ring-config)#east-interface po4`	Associate po4 interface as east-interface
`Bridge1(g8032-ring-config)#west-interface po1`	Associate po1 interface as west-interface
`Bridge1(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge1(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min

`Bridge1(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge1(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge1(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge1(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge1(g8032-config-switch)#physical-ring lagring`	Associate Physical ring lagring to erp1 instance
`Bridge1(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge1(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge1(g8032-config-switch)#level 7`	Configure level as 7
`Bridge1(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge1(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge1(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge1(g8032-config-switch)#g8032 physical-ring lagsubring bridge 1`	Create g8032 physical ring with name lagsubring on bridge 1
`Bridge1(g8032-ring-config)#east-interface po6`	Associate po6 interface as east-interface
`Bridge1(g8032-ring-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge1(g8032-config-switch)#ring-type sub-ring`	Configure ring-type as sub-ring
`Bridge1(g8032-config-switch)#physical-ring lagsubring`	Associate Physical ring lagsubring to erp2 instance
`Bridge1(g8032-config-switch)#rpl role neighbor east-interface`	Configure the node as neighbor node on east interface
`Bridge1(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge1(g8032-config-switch)#level 7`	Configure level as 7
`Bridge1(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge1(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge1(g8032-config-switch)#ring-id 2`	Configure ring-id as 2
`Bridge1(g8032-config-switch)# tcn-propogation enable`	Enable tcn propogation
`Bridge1(g8032-config-switch)# tcn-to-instance erp1`	Attach erp1 instance to erp2 instance to notify any changes in subring to major ring
`Bridge5(g8032-config-switch)#end`	Exit g8032 erp instance mode

© 2021 IP Infusion Inc. Proprietary

Bridge 2

`Bridge2#config term`	Enter configure mode
`Bridge2(config)#bridge 1 protocol rstp vlan-bridge`	Enable CFM domain name as string
`Bridge2((config)#vlan database`	Configure VLAN database
`Bridge2(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge2(config-vlan)#interface po1`	Configure lag interface po1
`Bridge2(config-if)#switchport`	Configure po1 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po1 interface
`Bridge2(config-if)#interface po2`	Configure lag interface po2
`Bridge2(config-if)#switchport`	Configure po2 as a layer 2 port
`Bridge2(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge2(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge2(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po2 interface
`Bridge2(config-if)#interface xe8`	Configure interface xe8
`Bridge2(config-if)#channel-group 1 mode active`	Configure xe8 as part of po1
`Bridge2(config-if)#interface xe9`	Configure interface xe9
`Bridge2(config-if)#channel-group 1 mode active`	Configure xe9 as part of po1
`Bridge2(config-if)#interface xe3`	Configure interface xe3
`Bridge2(config-if)#channel-group 2 mode active`	Configure xe3 as part of po2
`Bridge2(config-if)#interface xe4`	Configure interface xe4
`Bridge2(config-if)#channel-group 2 mode active`	Configure xe4 as part of po2
`Bridge2(config-if)#ethernet cfm domain-type character-string domain-name nod12 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod12 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 21 active true local-vid 200 po1`	Create down mep 21 with local vid 200 for po1 interface
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast

`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 12`	Configure crosscheck to remote MEP with value 12
`Bridge2(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod23 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod23 and set mip creation criteria to default with level 7 on bridge 1
`Bridge2(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 23 active true local-vid 200 po2`	Create down mep 23 with local vid 200 for po2 interface
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 32`	Configure crosscheck to remote MEP with value 32
`Bridge2(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge2(config-ether-cfm)#g8032 physical-ring lagring bridge 1`	Create g8032 physical ring with name lagring on bridge 1
`Bridge2(g8032-ring-config)#east-interface po1`	Associate po1 interface as east-interface
`Bridge2(g8032-ring-config)#west-interface po2`	Associate po2 interface as west-interface
`Bridge2(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge2(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge2(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge2(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge2(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge2(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge2(g8032-config-switch)#physical-ring lagring`	Associate Physical ring lagring to erp1 instance
`Bridge2(g8032-config-switch)#rpl role non-owner`	Configure the node as non-owner node
`Bridge2(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge2(g8032-config-switch)#level 7`	Configure level as 7

© 2021 IP Infusion Inc. Proprietary

`Bridge2(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge2(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge2(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge2(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 3

`Bridge3#config term`	Enter configuration mode
`Bridge3(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge3((config)#vlan database`	Configure VLAN database
`Bridge3(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge3(config-vlan)#interface po2`	Configure lag interface po2
`Bridge3(config-if)#switchport`	Configure po2 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po2 interface
`Bridge3(config-if)#interface po3`	Configure lag interface po3
`Bridge3(config-if)#switchport`	Configure po3 as a layer 2 port
`Bridge3(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge3(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge3(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge3(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po3 interface
`Bridge3(config-if)#interface xe3`	Configure interface xe3
`Bridge3(config-if)#channel-group 2 mode active`	Configure xe3 as part of po2
`Bridge3(config-if)#interface xe4`	Configure interface xe4
`Bridge3(config-if)#channel-group 2 mode active`	Configure xe4 as part of po2
`Bridge3(config-if)#interface xe15`	Configure interface xe3
`Bridge3(config-if)#channel-group 3 mode active`	Configure xe3 as part of po3
`Bridge3(config-if)#interface xe16`	Configure interface xe16
`Bridge3(config-if)#channel-group 3 mode active`	Configure xe16 as part of po3
`Bridge3(config-if)#ethernet cfm domain-type character-string domain-name nod23 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod23 and set mip creation criteria to default with level 7 on bridge 1

`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 32 active true local-vid 200 po2`	Create down mep 32 with local vid 200 for po2 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 23`	Configure crosscheck to remote MEP with value 23
`Bridge3(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod34 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod34 and set mip creation criteria to default with level 7 on bridge 1
`Bridge3(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 34 active true local-vid 200 po3`	Create down mep 34 with local vid 200 for po3 interface
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 43`	Configure crosscheck to remote MEP with value 43
`Bridge3(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge3(config-ether-cfm)#g8032 physical-ring lagring bridge 1`	Create g8032 physical ring with name lagring on bridge 1
`Bridge3(g8032-ring-config)#east-interface po2`	Associate po2 interface as east-interface
`Bridge3(g8032-ring-config)#west-interface po3`	Associate po3 interface as west-interface
`Bridge3(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge3(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge3(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge3(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge3(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge3(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1

© 2021 IP Infusion Inc. Proprietary

`Bridge3(g8032-config-switch)#physical-ring lagring`	Associate Physical ring lagring to erp1 instance
`Bridge3(g8032-config-switch)#rpl role neighbor west-interface`	Configure the node as neighbor node on west interface
`Bridge3(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge3(g8032-config-switch)#level 7`	Configure level as 7
`Bridge3(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge3(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge3(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge3(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 4

`Bridge4#config term`	Enter configure mode
`Bridge4(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge4((config)#vlan database`	Configure VLAN database
`Bridge4(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge4(config-vlan)#interface po3`	Configure lag interface po3
`Bridge4(config-if)#switchport`	Configure po3 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po3 interface
`Bridge4(config-if)#interface po4`	Configure lag interface po4
`Bridge4(config-if)#switchport`	Configure po4 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge4(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po4 interface
`Bridge4(config-if)#interface po5`	Configure lag interface po5
`Bridge4(config-if)#switchport`	Configure po5 as a layer 2 port
`Bridge4(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge4(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge4(config-if)#switchport mode trunk`	Configure port as trunk port

`Bridge4(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po5 interface
`Bridge4(config-if)#interface xe6`	Configure interface xe6
`Bridge4(config-if)#channel-group 4 mode active`	Configure xe6 as part of po4
`Bridge4(config-if)#interface xe7`	Configure interface xe7
`Bridge4(config-if)#channel-group 4 mode active`	Configure xe7 as part of po4
`Bridge4(config-if)#interface xe10`	Configure interface xe10
`Bridge4(config-if)#channel-group 5 mode active`	Configure xe10 as part of po5
`Bridge4(config-if)#interface xe11`	Configure interface xe11
`Bridge4(config-if)#channel-group 5 mode active`	Configure xe11 as part of po5
`Bridge4(config-if)#interface xe15`	Configure interface xe15
`Bridge4(config-if)#channel-group 3 mode active`	Configure xe15 as part of po3
`Bridge4(config-if)#interface xe16`	Configure interface xe16
`Bridge4(config-if)#channel-group 3 mode active`	Configure xe16 as part of po3
`Bridge4(config-if)#ethernet cfm domain-type character-string domain-name nod34 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod34 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 43 active true local-vid 200 po3`	Create down mep 43 with local vid 200 for po3 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 34`	Configure crosscheck to remote MEP with value 34
`Bridge4(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod41 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod41 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 41 active true local-vid 200 po4`	Create down mep 41 with local vid 200 for po4 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast

© 2021 IP Infusion Inc. Proprietary

`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 14`	Configure crosscheck to remote MEP with value 14
`Bridge4(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod45 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod45 and set mip creation criteria to default with level 7 on bridge 1
`Bridge4(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 54 active true local-vid 200 po5`	Create down mep 54 with local vid 200 for po5 interface
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 45`	Configure crosscheck to remote MEP with value 45
`Bridge4(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge4(config-ether-cfm)#g8032 physical-ring lagring bridge 1`	Create g8032 physical ring with name lagring on bridge 1
`Bridge4(g8032-ring-config)#east-interface po3`	Associate po3 interface as east-interface
`Bridge4(g8032-ring-config)#west-interface po4`	Associate po4 interface as west-interface
`Bridge4(g8032-ring-config)#g8032 physical-ring lagsubring bridge 1`	Create g8032 physical ring with name lagsubring on bridge 1
`Bridge4(g8032-ring-config)#east-interface po5`	Associate po5 interface as east-interface
`Bridge4(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge4(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge4(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge4(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge4(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge4(g8032-profile-config)#g8032 erp-instance erp1 bridge 1`	Create g8032 erp instance erp1 on bridge 1
`Bridge4(g8032-config-switch)#physical-ring lagring`	Associate Physical ring lagring to erp1 instance

`Bridge4(g8032-config-switch)#rpl role owner east-interface`	Configure the node as owner node on east interface
`Bridge4(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp1 instance
`Bridge4(g8032-config-switch)#level 7`	Configure level as 7
`Bridge4(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge4(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge4(g8032-config-switch)#ring-id 1`	Configure ring-id as 1
`Bridge4(g8032-config-switch)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge4(g8032-config-switch)#ring-type sub-ring`	Configure ring-type as sub-ring
`Bridge4(g8032-config-switch)#physical-ring lagsubring`	Associate Physical ring lagsubring to erp2 instance
`Bridge4(g8032-config-switch)#rpl role non-owner`	Configure the node as neighbor node on east interface
`Bridge4(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge4(g8032-config-switch)#level 7`	Configure level as 7
`Bridge4(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge4(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge4(g8032-config-switch)#ring-id 2`	Configure ring-id as 2
`Bridge4(g8032-config-switch)# tcn-propogation enable`	Enable tcn propogation
`Bridge4(g8032-config-switch)# tcn-to-instance erp1`	Attach erp1 instance to erp2 instance to notify any changes in subring to major ring
`Bridge4(g8032-config-switch)#end`	Exit g8032 erp instance mode

Bridge 5

`Bridge5#config term`	Enter config mode
`Bridge5(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`Bridge5((config)#vlan database`	Configure VLAN database
`Bridge5(config-vlan)#vlan 200-205 bridge 1 state enable`	Create VLAN 200-205 on bridge 1
`Bridge5(config-vlan)#interface po5`	Configure lag interface po5
`Bridge5(config-if)#switchport`	Configure po5 as a layer 2 port
`Bridge5(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge5(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge5(config-if)#switchport mode trunk`	Configure port as trunk port

© 2021 IP Infusion Inc. Proprietary

`Bridge5(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po3 interface
`Bridge5(config-if)#interface po6`	Configure lag interface po3
`Bridge5(config-if)#switchport`	Configure po3 as a layer 2 port
`Bridge5(config-if)#bridge-group 1`	Configure interface in bridge group 1
`Bridge5(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree for bridge group 1 on that interface
`Bridge5(config-if)#switchport mode trunk`	Configure port as trunk port
`Bridge5(config-if)#switchport trunk allowed vlan add 200-205`	Allow vlan 200-205 on po3 interface
`Bridge5(config-if)#interface xe1`	Configure interface xe1
`Bridge5(config-if)#channel-group 6 mode active`	Configure xe1 as part of po6
`Bridge5(config-if)#interface xe2`	Configure interface xe2
`Bridge5(config-if)#channel-group 6 mode active`	Configure xe2 as part of po6
`Bridge5(config-if)#interface xe10`	Configure interface xe10
`Bridge5(config-if)#channel-group 5 mode active`	Configure xe10 as part of po5
`Bridge5(config-if)#interface xe11`	Configure interface xe11
`Bridge5(config-if)#channel-group 5 mode active`	Configure xe11 as part of po5
`Bridge5(config-if)#ethernet cfm domain-type character-string domain-name nod15 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod15 and set mip creation criteria to default with level 7 on bridge 1
`Bridge5(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 15 active true local-vid 200 po6`	Create down mep 15 with local vid 200 for po6 interface
`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 51`	Configure crosscheck to remote MEP with value 51
`Bridge5(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge5(config-ether-cfm)#ethernet cfm domain-type character-string domain-name nod45 level 7 mip-creation none bridge 1`	Create cfm domain with type as character string with name nod45 and set mip creation criteria to default with level 7 on bridge 1
`Bridge5(config-ether-cfm)#service ma-type string ma-name 43982 vlan 200 mip-creation none`	Create ma type as string with name 43982 and set mip creation criteria to default on vlan 200
`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 45 active true local-vid 200 po5`	Create down mep 45 with local vid 200 for po5 interface

`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast
`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 54`	Configure crosscheck to remote MEP with value 54
`Bridge5(config-ether-cfm-ma)#cc interval 3`	Enable cc interval with 3
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet ma mode
`Bridge5(config-ether-cfm)#g8032 physical-ring lagsubring bridge 1`	Create g8032 physical ring with name lagsubring on bridge 1
`Bridge5(g8032-ring-config)#east-interface po5`	Associate po5 interface as east-interface
`Bridge5(g8032-ring-config)#west-interface po6`	Associate po6 interface as west-interface
`Bridge5(g8032-ring-config)#g8032 profile profile1 bridge 1`	Create g8032 profile with profile name profile1 on bridge 1
`Bridge5(g8032-profile-config)#timer wait-to-restore 1`	Configure wait to restore time as 1 min
`Bridge5(g8032-profile-config)#timer hold-off 0`	Configure hold-off timer value as 0
`Bridge5(g8032-profile-config)#timer guard-timer 10`	Configure guard-timer value as 10ms
`Bridge5(g8032-profile-config)#switching-mode revertive`	Configure Switching mode as revertive Switching mode
`Bridge5(g8032-profile-config)#g8032 erp-instance erp2 bridge 1`	Create g8032 erp instance erp2 on bridge 1
`Bridge5(g8032-config-switch)#physical-ring lagsubring`	Associate Physical ring lagsubring to erp2 instance
`Bridge5(g8032-config-switch)#ring-type sub-ring`	Configure ring-type as subring
`Bridge5(g8032-config-switch)#rpl role owner west-interface`	Configure the node as owner node on west interface
`Bridge5(g8032-config-switch)#profile profile1`	Associate Profile profile1 to erp2 instance
`Bridge5(g8032-config-switch)#level 7`	Configure level as 7
`Bridge5(g8032-config-switch)#raps-channel-vlan 200`	Configure RAPS channel vlan as 200
`Bridge5(g8032-config-switch)#data-traffic-vlan 201-205`	Configure traffic vlan from 201-205
`Bridge5(g8032-config-switch)#ring-id 2`	Configure ring-id as 2
`Bridge5(g8032-config-switch)#end`	Exit g8032 erp instance mode

Validation

```
Bridge1#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
```


© 2021 IP Infusion Inc. Proprietary

```
State           : G8032_ST_IDLE
Phy Ring        : lagsubring
Ring Type       : SUB-RING (NON VIRTUAL)
Role            : NEIGHBOR (EAST)
Node ID         : 3c:2c:99:26:e6:7b
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  po6                 -
State           :  Blocked             -
Remote NodeId   :  6c:b9:c5:67:72:f6   -
Remote BPR      :  0                   -
Endpoint Info
-------------
Domain Name     :  nod15               -
MEP ID          :  51                  -
MA Name         :  43982               -
============================================================
TCN Propagation : Enabled
TCN Propagation List: erp1,

     Channel              |
 (LEVEL, VLAN, RING ID)   |
============================
 (7,    200,   2)         |
============================

Bridge1#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1ance erp2 bridge
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagring
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : 3c:2c:99:26:e6:80
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  po4                 po1
State           :  Unblocked           Unblocked
Remote NodeId   :  34:17:eb:e4:af:10   -
Remote BPR      :  1                   -
Endpoint Info
-------------
Domain Name     :  nod41               nod12
MEP ID          :  14                  12
MA Name         :  43982               43982
============================================================
----------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
============================
 (7,    200,   1)         |
============================

DataTraffic vlan: 201-205
```

```
Profile : profile1

Bridge2#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagring
Ring Type       : MAJOR-RING
Role            : NON-OWNER
Node ID         : d8:9e:f3:5e:f8:29
-------------------------------------------------------
                   East Link           West Link
=======================================================
Interface       :  po1                 po2
State           :  Unblocked           Unblocked
Remote NodeId   :  34:17:eb:e4:af:10   -
Remote BPR      :  1                   -
Endpoint Info
-------------
Domain Name     :  nod12               nod23
MEP ID          :  21                  23
MA Name         :  43982               43982
=======================================================
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge3#show  g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagring
Ring Type       : MAJOR-RING
Role            : NEIGHBOR (WEST)
Node ID         : 3c:2c:99:1a:da:7d
-------------------------------------------------------
                   East Link           West Link
=======================================================
Interface       :  po2                 po3
State           :  Unblocked           Blocked
Remote NodeId   :  34:17:eb:e4:af:10   34:17:eb:e4:af:10
Remote BPR      :  1                   1
Endpoint Info
-------------
Domain Name     :  nod23               nod34
MEP ID          :  32                  34
MA Name         :  43982               43982
=======================================================
--------------------------
```


© 2021 IP Infusion Inc. Proprietary

```
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge4#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagsubring
Ring Type       : SUB-RING (NON VIRTUAL)
Role            : NON-OWNER
Node ID         : 34:17:eb:e4:af:0b
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  po5                 -
State           :  Unblocked           -
Remote NodeId   :  6c:b9:c5:67:72:f6   -
Remote BPR      :  0                   -
Endpoint Info
-------------
Domain Name     :  nod45               -
MEP ID          :  54                  -
MA Name         :  43982               -
============================================================
TCN Propagation : Enabled
TCN Propagation List: erp1,

     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   2)         |
==========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge4#show g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagring
Ring Type       : MAJOR-RING
Role            : OWNER (EAST)
Node ID         : 34:17:eb:e4:af:10
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  po3                 po4
State           :  Blocked             Unblocked
```

```
Remote NodeId   :  -                    -
Remote BPR      :  -                    -
Endpoint Info
-------------
Domain Name     :  nod34                nod41
MEP ID          :  43                   41
MA Name         :  43982                43982
============================================================
---------------------------
     Channel               |
 (LEVEL, VLAN, RING ID)    |
===========================
 (7,    200,   1)          |
===========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge5#show g8032 erp-instance erp2 bridge 1

Inst Name       : erp2
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagsubring
Ring Type       : SUB-RING
Role            : OWNER (WEST)
Node ID         : 6c:b9:c5:67:72:f6
------------------------------------------------------------
                   East Link           West Link
============================================================
Interface       :  po5                  po6
State           :  Unblocked            Blocked
Remote NodeId   :  -                    -
Remote BPR      :  -                    -
Endpoint Info
-------------
Domain Name     :  nod45                nod15
MEP ID          :  45                   15
MA Name         :  43982                43982
============================================================
---------------------------
     Channel               |
 (LEVEL, VLAN, RING ID)    |
===========================
 (7,    200,   2)          |
===========================

DataTraffic vlan: 201-205
Profile : profile1

Bridge3#show  g8032 erp-instance erp1 bridge 1

Inst Name       : erp1
Description     :
State           : G8032_ST_IDLE
Phy Ring        : lagring
Ring Type       : MAJOR-RING
```


© 2021 IP Infusion Inc. Proprietary

```
Role            : NEIGHBOR (WEST)
Node ID         : 3c:2c:99:1a:da:7d
-------------------------------------------------------
                   East Link           West Link
=======================================================
Interface       :  po2                 po3
State           :  Unblocked           Blocked
Remote NodeId   :  34:17:eb:e4:af:10   34:17:eb:e4:af:10
Remote BPR      :  1                   1
Endpoint Info
-------------
Domain Name     :  nod23               nod34
MEP ID          :  32                  34
MA Name         :  43982               43982
=======================================================
--------------------------
     Channel              |
 (LEVEL, VLAN, RING ID)   |
==========================
 (7,    200,   1)         |
==========================

DataTraffic vlan: 201-205
Profile : profile1
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 Ethernet CFM Configurations

This chapter contains examples of Ethernet Operations and Management (OAM) configurations using the Connectivity Fault Management (CFM) protocol.

Connectivity Fault Management detects, verifies, isolates and notifies connectivity failures on a Virtual Bridged LAN (B-VLAN) based on the protocol standard specified in IEEE 802.1ag 2007. It provides discovery and verification of paths through 802.1 bridges and LANs and is part of the Operation, Administration and Management (OAM) module. CFM is transparent to customer data being transported by a network and is capable of providing maximum fault management.

Continuity Check Message(CCM)

Topology



Figure 3-23: CFM Topology

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW1(config)#vlan database`	Entering vlan database
`SW1(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.
`SW1(config-vlan)#exit`	Exit vlan database
`SW1(config)#int ce49`	Configure interface ce49.
`SW1(config-if)#switchport`	Configure the interface as switch port.
`SW1(config-if)#bridge-group 1 spanning-tree disable`	Configure interface in bridge group 1, with spanning tree disabled..
`SW1(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface ce49.
`SW1(config-if)#exit`	Exit config mode.
`SW1(config)#ethernet cfm domain-type character-string domain-name mdnam level 7 mip-creation default bridge 1`	Create cfm domain with type as character string and set mip creation criteria to default.
`SW1(config-ether-cfm)#service ma-type string ma-name testtm vlan 512 mip-creation default`	Create ma type as string and set mip creation criteria to default.

`SW1(config-ether-cfm-ma)#ethernet cfm mep down mpid 2 active true local-vid 512 ce49`	Create down mep for local-vid on ce49.
`SW1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable cc multicast.
`SW1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit ethernet cfm ma-mep mode.
`SW1(config-ether-cfm-ma)#mep crosscheck mpid 1`	Configure crosscheck to remote MEP in VLAN 512.
`SW1(config-ether-cfm-ma)#cc interval 3`	Enable cc interval for 100 millisecond.
`SW1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit ethernet ma mode.
`SW1(config-ether-cfm)#exit`	Exit ethernet CFM mode.

SW2

`SW2#configure terminal`	Enter configure mode.
`SW2(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW2(config)#vlan database`	Entering vlan database
`SW2(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.
`SW2(config-vlan)#exit`	Exit vlan database
`SW2(config)#int ce0`	Configure interface ce0.
`SW2(config-if)#switchport`	Configure the interface as switch port.
`SW2(config-if)#bridge-group 1 spanning-tree disable`	Configure interface in bridge group 1, with spanning tree disabled..
`SW2(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW2(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface ce0.
`SW2(config-if)#exit`	Exit config mode.
`SW2(config)#int xe0`	Configure interface xe0.
`SW2(config-if)#switchport`	Configure the interface as switch port.
`SW2(config-if)#bridge-group 1 spanning-tree disable`	Configure interface in bridge group 1, with spanning tree disabled..
`SW2(config-if)#switchport mode trunk`	Configure interface mode as trunk.
`SW2(config-if)#switchport trunk allowed vlan all`	Allow all VLANs on interface xe1.
`SW2(config-if)#exit`	Exit config mode.

SW3

`SW3#configure terminal`	Enter configure mode.
`SW3(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge 1 as an RSTP VLAN-aware bridge.
`SW3(config)#vlan database`	Entering vlan database
`SW3(config-vlan)#vlan 512 bridge 1 state enable`	Create VLAN 512 on bridge 1.

© 2021 IP Infusion Inc. Proprietary

SW3(config-vlan)#exit	Exit vlan database
SW3(config)#int xe17	Configure interface xe17
SW3(config-if)#switchport	Configure the interface as switch port.
SW3(config-if)#bridge-group 1 spanning-tree disable	Configure interface in bridge group 1, with spanning tree disabled..
SW3(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW3(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe17.
SW3(config-if)#exit	Exit config mode.
SW3(config)#int xe1	Configure interface xe1.
SW3(config-if)#switchport	Configure the interface as switch port.
SW3(config-if)#bridge-group 1 spanning-tree disable	Configure interface in bridge group 1, with spanning tree disabled..
SW3(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW3(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW3(config-if)#exit	Exit config mode.

SW4

SW4#configure terminal	Enter configure mode.
SW4(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW4(config)#vlan database	Entering vlan database
SW4(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW4(config-vlan)#exit	Exit vlan database
SW4(config)#int xe1	Configure interface xe1.
SW4(config-if)#switchport	Configure the interface as switch port.
SW4(config-if)#bridge-group 1 spanning-tree disable	Configure interface in bridge group 1, with spanning tree disabled..
SW4(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW4(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe1.
SW4(config-if)#exit	Exit config mode.
SW4(config)#int xe9	Configure interface xe9.
SW4(config-if)#switchport	Configure the interface as switch port.
SW4(config-if)#bridge-group 1 spanning-tree disable	Configure interface in bridge group 1, with spanning tree disabled..
SW4(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW4(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe9.
SW4(config-if)#exit	Exit config mode.

SW5

SW5#configure terminal	Enter configure mode.
SW5(config)#bridge 1 protocol rstp vlan-bridge	Create bridge 1 as an RSTP VLAN-aware bridge.
SW5(config)#vlan database	Entering vlan database
SW5(config-vlan)#vlan 512 bridge 1 state enable	Create VLAN 512 on bridge 1.
SW5(config-vlan)#exit	Exit vlan database
SW5(config)#int xe9	Configure interface xe9.
SW5(config-if)#switchport	Configure the interface as switch port.
SW5(config-if)#bridge-group 1 spanning-tree disable	Configure interface in bridge group 1, with spanning tree disabled..
SW5(config-if)#switchport mode trunk	Configure interface mode as trunk.
SW5(config-if)#switchport trunk allowed vlan all	Allow all VLANs on interface xe9.
SW5(config-if)#exit	Exit config mode.
SW5(config)#ethernet cfm domain-type character-string domain-name mdnam level 7 mip-creation default bridge 1	Create cfm domain with type as character string and set mip creation criteria to default.
SW5(config-ether-cfm)#service ma-type string ma-name testtm vlan 512 mip-creation default	Create ma type as string and set mip creation criteria to default.
SW5(config-ether-cfm-ma)#ethernet cfm mep down mpid 1 active true local-vid 512 xe9	Create down mep for local-vid on xe9.
SW5(config-ether-cfm-ma-mep)#cc multicast state enable	Enable cc multicast.
SW5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit ethernet ma-mep mode.
SW5(config-ether-cfm-ma)#mep crosscheck mpid 2	Configure crosscheck to remote MEP in VLAN 512.
SW5(config-ether-cfm-ma)#cc interval 3	Enable cc interval for 10 millisecond.
SW5(config-ether-cfm-ma)#exit-ether-ma-mode	Exit ethernet ma mode.
SW5(config-ether-cfm)#exit	Exit ethernet CFM mode.

Validation

```
SW1#ping ethernet mac 3c2c.9926.e683 unicast source 2 domain mdnam vlan 512 bridge 1
success rate is 100 (5/5)


SW1#traceroute ethernet 3c2c.9926.e683 mepid 2 domain mdnam vlan 512 bridge 1 MP Mac
HopsRelay-actionIngress/EgressIngress/Egressaction 3c2c.9926.e6831RlyHitIngressIngOK


SW1#show ethernet cfm maintenance-points local mep domain mdnam bridge 1
MPID Dir Lvl VLAN CC-Stat  CC-Intvl MAC-Address    Def Port  MD Name
------------------------------------------------------------------------------
1    Dn  7   512   Enable  100 ms    a82b.b5d4.e33e F   ce49 mdnam
SW1#
```


© 2021 IP Infusion Inc. Proprietary

```
SW1#show ethernet cfm errors domain mdnam bridge 1

Domain Name          Level     Vlan     MEPID     Defects
-------------------------------------------------------
mdnam                7         512       1         .....

1. defRDICCM    2. defMACstatus  3. defRemoteCCM
4. defErrorCCM  5. defXconCCM
SW1#
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 Provider Bridging Configuration

This chapter contains sample Provider Bridging configurations.

A Provider Bridged network is a virtual bridged LAN that comprises of Provider Bridges (SVLAN Bridges and Provider Edge Bridges), attached LANs, and is under the administrative control of a single service provider. Provider Bridges interconnect the separate MACs of the IEEE 802 LANs that compose a Provider Bridged network, relaying frames to provide connectivity between all the LANs to provide customer interfaces for each service instance. Provider Bridging allows a service provider to offer an equivalent of separate LAN segments, bridged or virtual bridged LANs, over the Provider Bridged network. This feature offers inter-operability and consistent management. It also requires minimum cooperation between the customers and service provider and does not require cooperation among the customers.

Provider Bridging with Customer Hosts

This sample shows configuring a Provider Bridged network with customer hosts.

Topology

Figure 4-24 displays a sample Provider Bridged topology.

Note: Customer Host machine will always send untagged traffic.

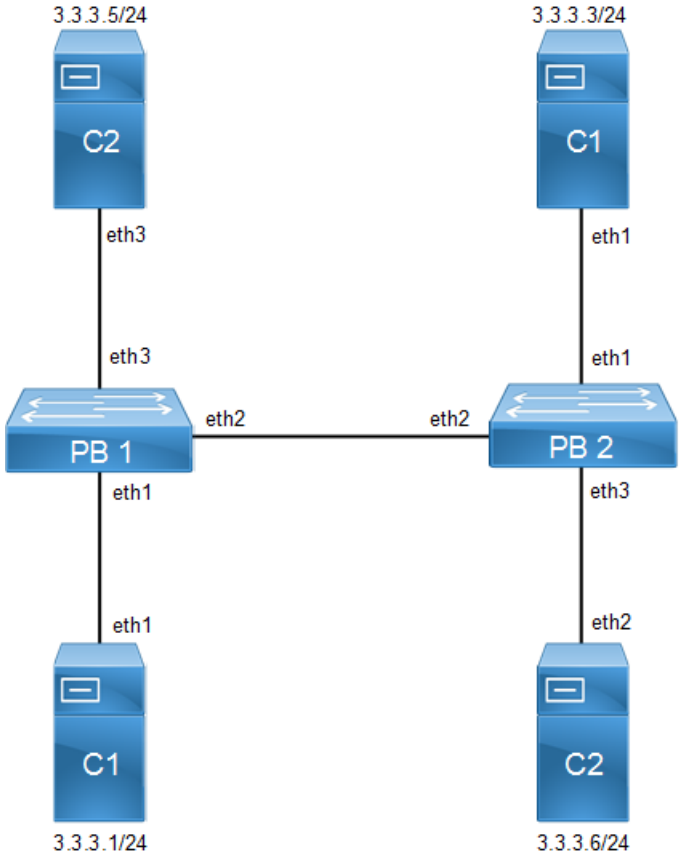


Figure 4-24: Provider Bridge Topology

Legend

The following table is the legend for Figure 4-24:

C1	Customer 1 host machines
C2	Customer 2 host machines
PB1, PB2	Provider bridges

PB1

`PB1#configure terminal`	Enter configure mode.
`PB1(config)#bridge 1 protocol provider-mstp edge`	Configure bridge 1 as a provider edge bridge.
`PB1(config)#vlan database`	Enter the VLAN Configure mode.
`PB1(config-vlan)#vlan 2 type customer bridge 1 state enable`	Configure VLAN 2 as a customer VLAN and associate it with bridge 1.
`PB1(config-vlan)#vlan 4 type customer bridge 1 state enable`	Configure VLAN 4 as a customer VLAN and associate it with bridge 1.
`PB1(config-vlan)#vlan 3 type customer bridge 1 state enable`	Configure VLAN 3 as a service VLAN and associate it with bridge 1.
`PB1(config-vlan)#vlan 6 type service point-point bridge 1 state enable`	Configure VLAN 6 as a service VLAN and associate it with bridge 1.
`PB1(config-vlan)#vlan 7 type service point-point bridge 1 state enable`	Configure VLAN 7 as a service VLAN and associate it with bridge 1.
`PB1(config-vlan)#exit`	Exit the VLAN Configure mode.
`PB1(config)#interface eth1`	Enter interface mode.
`PB1(config-if)#switchport`	Configure eth1 as a Layer-2 interface.
`PB1(config-if)#bridge-group 1`	Associate the eth1 interface with bridge 1.
`PB1(config-if)#switchport mode customer-edge access`	Configure the interface to access mode.
`PB1(config-if)#switchport customer-edge access vlan 2`	Associate the eth1 interface with VLAN 2.
`PB1(config-if)#exit`	Exit interface mode.
`PB1(config)#interface eth3`	Enter interface mode.
`PB1(config-if)#switchport`	Configure eth3 as a Layer-2 interface.
`PB1(config-if)#bridge-group 1`	Associate the eth3 interface with bridge 1.
`PB1(config-if)#switchport mode customer-edge access`	Configure the interface to access mode.
`PB1(config-if)#switchport customer-edge access vlan 4`	Associate the eth3 interface with VLAN 4.
`PB1(config-if)#exit`	Exit interface mode.
`PB1(config)#interface eth2`	Enter interface mode.
`PB1(config-if)#switchport`	Configure eth2 as a Layer-2 interface.
`PB1(config-if)#bridge-group 1`	Associate the eth2 interface with bridge 1.
`PB1(config-if)#switchport provider-network allowed vlan add 3,6`	Associate Service VLAN 3 and Service VLAN 6 with the provider network.

© 2021 IP Infusion Inc. Proprietary

`PB1(config-if)#exit`	Exit interface mode.
`PB1(config)#cvlan registration table customer1 bridge 1`	Create a CVLAN table customer1, and associate it with bridge 1.
`PB1(config-cvlan-registration)#cvlan 2 svlan 3`	Map CVLAN 2 with SVLAN 3.
`PB1(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.
`PB1(config)#cvlan registration table customer2 bridge 1`	Create a CVLAN table customer2, and associate it with bridge 1.
`PB1(config-cvlan-registration)#cvlan 4 svlan 6`	Map CVLAN 4 with SVLAN 6.
`PB1(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.
`PB1(config)#interface eth1`	Enter interface mode.
`PB1(config-if)#switchport customer-edge vlan registration customer1`	Associate the customer1 table with the interface.
`PB1(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.
`PB1(config)#interface eth3`	Enter interface mode.
`PB1(config-if)#switchport customer-edge vlan registration customer2`	Associate the customer2 table with the interface.
`PB1(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.

PB2

`PB2#configure terminal`	Enter configure mode.
`PB2(config)#bridge 1 protocol provider-mstp edge`	Configure bridge 1 as a provider edge bridge.
`PB2(config)#vlan database`	Enter the VLAN Configure mode.
`PB2(config-vlan)#vlan 2 type customer bridge 1 state enable`	Configure VLAN 2 as a customer VLAN and associate it with bridge 1.
`PB2(config-vlan)#vlan 3 type customer bridge 1 state enable`	Configure VLAN 3 as a customer VLAN and associate it with bridge 1.
`PB2(config-vlan)#vlan 4 type customer bridge 1 state enable`	Configure VLAN 4 as a customer VLAN and associate it with bridge 1.
`PB2(config-vlan)#vlan 6 type service point-point bridge 1 state enable`	Configure VLAN 6 as a service VLAN and associate it with bridge 1.
`PB2(config-vlan)#vlan 7 type service point-point bridge 1 state enable`	Configure VLAN 7 as a service VLAN and associate it with bridge 1.
`PB2(config-vlan)#exit`	Exit the VLAN Configure mode.
`PB2(config)#interface eth1`	Enter interface mode.
`PB2(config-if)#switchport`	Configure eth1 as a Layer-2 interface.
`PB2(config-if)#bridge-group 1`	Associate the eth1 interface with bridge 1.
`PB2(config-if)#switchport mode customer-edge access`	Configure the interface to access mode.
`PB2(config-if)#switchport customer-edge access vlan 2`	Associate the eth1 interface with VLAN 2.
`PB2(config-if)#exit`	Exit interface mode.

`PB2(config)#interface eth3`	Enter interface mode.
`PB2(config-if)#switchport`	Configure eth3 as a Layer-2 interface.
`PB2(config-if)#bridge-group 1`	Associate the eth3 interface with bridge 1.
`PB2(config-if)#switchport mode customer-edge access`	Configure the interface to access mode.
`PB2(config-if)#switchport customer-edge access vlan 4`	Associate the eth3 interface with VLAN 4.
`PB2(config-if)#exit`	Exit interface mode.
`PB2(config)#interface eth2`	Enter interface mode.
`PB2(config-if)#switchport`	Configure eth2 as a Layer-2 interface.
`PB2(config-if)#bridge-group 1`	Associate the eth2 interface with bridge 1.
`PB2(config-if)#switchport provider-network allowed vlan add 3,6`	Associate Service VLAN 3 and Service VLAN 6 with the provider network.
`PB2(config-if)#exit`	Exit interface mode.
`PB2(config)#cvlan registration table customer1 bridge 1`	Create a CVLAN table customer1, and associate it with bridge 1.
`PB2(config-cvlan-registration)#cvlan 2 svlan 3`	Map CVLAN 2 with SVLAN 3.
`PB2(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.
`PB2(config)#cvlan registration table customer2 bridge 1`	Create a CVLAN table customer2, and associate it with bridge 1.
`PB2(config-cvlan-registration)#cvlan 4 svlan 6`	Map CVLAN 4 with SVLAN 6.
`PB2(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.
`PB2(config)#interface eth1`	Enter interface mode.
`PB2(config-if)#switchport customer-edge vlan registration customer1`	Associate the customer1 table with the interface.
`PB2(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.
`PB2(config)#interface eth3`	Enter interface mode.
`PB2(config-if)#switchport customer-edge vlan registration customer2`	Associate the customer2 table with the interface.
`PB2(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.

Validation

```
#sh cvlan registration table
Bridge          Table Name       Port List
======          ==========       =========
1               customer1        eth1

CVLAN ID        T-CVLAN ID      SVLAN ID        CCOS  SCOS  CCFI  SCFI
========        ==========      ========        ====  ====  ====  ====
2           -     3

Bridge          Table Name       Port List
======          ==========       =========
1               customer2        eth3
```


© 2021 IP Infusion Inc. Proprietary

```
    CVLAN ID         T-CVLAN ID      SVLAN ID         CCOS  SCOS  CCFI  SCFI
    ========         ==========      ========         ====  ====  ====  ====
    4            -       6
```

Customer C1

Customer C1 (3.3.3.1) on VLAN2 should be able to ping customer C1's other site (3.3.3.3) on the same VLAN.

```
[root@C1 root]#ping 3.3.3.3
PING 3.3.3.3(3.3.3.3) 56(84) bytes of data.
64 bytes from 3.3.3.3: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 3.3.3.3: icmp_seq=2 ttl=64 time=0.394 ms
--- 3.3.3.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 0.394/0.730/1.067/0.337 ms
```

Customer C1 (3.3.3.1) on VLAN 2 should not be able to ping customer C2's site (3.3.3.6) on VLAN 4.

```
[root@C1 root]#ping 3.3.3.6
PING 3.3.3.6 (3.3.3.6) 56(84) bytes of data.
--- 3.3.3.6 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2010ms
```

Customer C2

Customer C2 (3.3.3.6) on VLAN 4 should be able to ping customer C2's other site (3.3.3.5) on the same VLAN.

```
[root@C2 root]#ping 3.3.3.5
PING 3.3.3.5 (3.3.3.5) 56(84) bytes of data.
64 bytes from 3.3.3.5: icmp_seq=1 ttl=64 time=0.647 ms
64 bytes from 3.3.3.5: icmp_seq=2 ttl=64 time=0.342 ms
64 bytes from 3.3.3.5: icmp_seq=3 ttl=64 time=0.358 ms
--- 3.3.3.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2011ms
rtt min/avg/max/mdev = 0.342/0.449/0.648/0.141 ms
```

Customer C2 (3.3.3.6) on VLAN 4 should not be able to ping customer C1's other site (3.3.3.1) on VLAN 2.

```
[root@C2 root]#ping 3.3.3.1
PING 3.3.3.1 (3.3.3.1) 56(84) bytes of data.
--- 3.3.3.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1018ms
```

Provider Bridging with Customer Equipment

This sample shows configuring a Provider Bridged network with customer equipment.

Topology

Figure 4-25 displays a sample Provider Bridged topology with customer equipment.

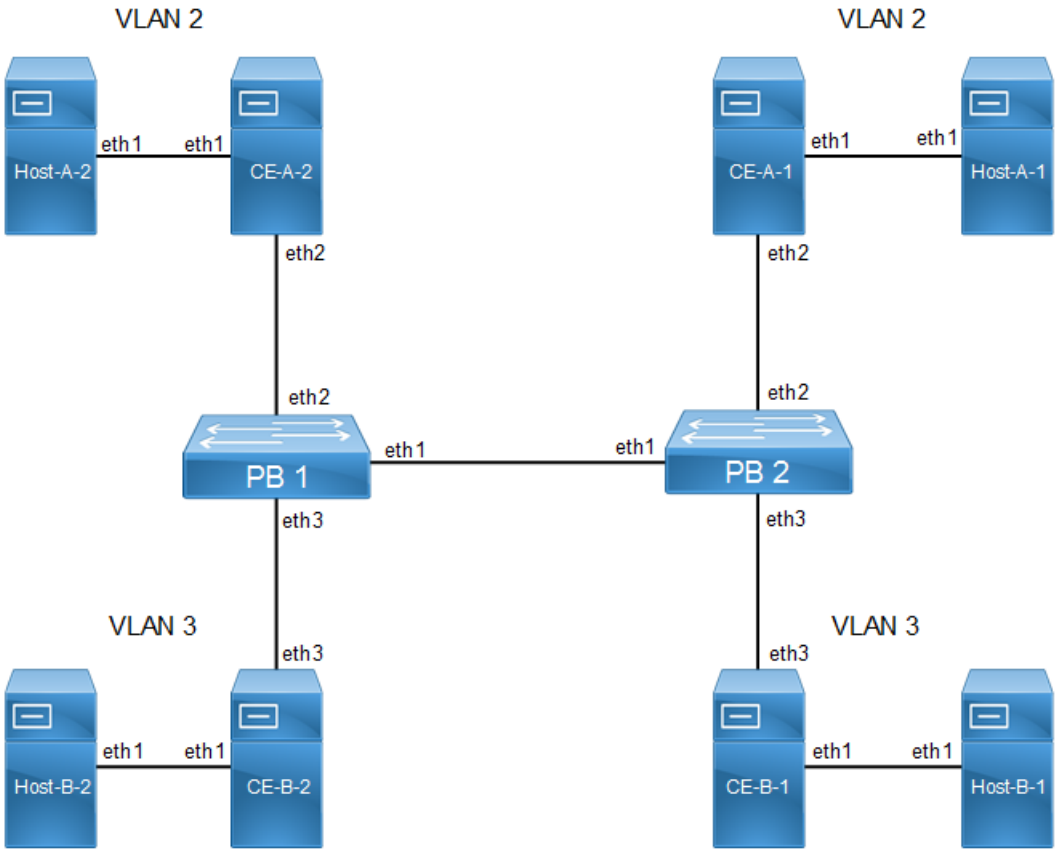


Figure 4-25: Provider Bridging with Customer Equipment Topology

Legend

The following table is the legend for Figure 4-25:

CE-A-1, CE-A-2, CE-B-1, CE-B-2	Customer equipment
Host A-1, Host A-2, Host B-1, Host B-2	Customer host machines
PB1, PB2	Provider edge bridges

PB1

`PB1#configure terminal`	Enter configure mode.
`PB1(config)#bridge 1 protocol provider-mstp edge`	Configure bridge 1 as a provider MSTP edge bridge.
`PB1(config)#vlan database`	Enter the VLAN Configure mode.
`PB1(config-vlan)#vlan 2 type customer bridge 1 state enable`	Configure VLAN 2 as a customer VLAN and associate it with bridge 1.
`PB1(config-vlan)#vlan 3 type customer bridge 1 state enable`	Configure VLAN 3 as a customer VLAN and associate it with bridge 1.
`PB1(config-vlan)#vlan 4 type service point-point bridge 1 state enable`	Configure VLAN 4 as a service VLAN and associate it with bridge 1.

© 2021 IP Infusion Inc. Proprietary

`PB1(config-vlan)#vlan 5 type service point-point bridge 1 state enable`	Configure VLAN 5 as a service VLAN and associate it with bridge 1.
`PB1(config-vlan)#exit`	Exit the VLAN Configure mode.
`PB1(config)#interface eth2`	Enter interface mode.
`PB1(config-if)#switchport`	Configure eth2 as a Layer-2 interface.
`PB1(config-if)#bridge-group 1`	Associate the eth2 interface with bridge 1.
`PB1(config-if)#switchport mode customer-edge hybrid`	Configure the eth2 interface to hybrid mode.
`PB1(config-if)#switchport customer-edge hybrid allowed vlan all`	Configure the eth2 interface to allow all VLANs.
`PB1(config-if)#exit`	Exit interface mode.
`PB1(config)#interface eth3`	Enter interface mode.
`PB1(config-if)#switchport`	Configure eth3 as a Layer-2 interface.
`PB1(config-if)#bridge-group 1`	Associate the eth3 interface with bridge 1.
`PB1(config-if)#switchport mode customer-edge hybrid`	Configure the eth3 interface to hybrid mode.
`PB1(config-if)#switchport customer-edge hybrid allowed vlan all`	Configure the eth3 interface to allow all VLANs.
`PB1(config-if)#exit`	Exit interface mode.
`PB1(config)#interface eth1`	Enter interface mode.
`PB1(config-if)#switchport`	Configure eth1 as a Layer-2 interface.
`PB1(config-if)#bridge-group 1`	Associate the eth1 interface with bridge 1.
`PB1(config-if)#switchport provider-network allowed vlan add 4,5`	Associate Service VLAN 4 and Service VLAN 5 with the provider network.
`PB1(config-if)#exit`	Exit interface mode.
`PB1(config)#cvlan registration table customer1 bridge 1`	Create a CVLAN table customer1, and associate it with bridge 1.
`PB1(config-cvlan-registration)#cvlan 1 svlan 4`	Map CVLAN 1 with SVLAN 4.
`PB1(config-cvlan-registration)#cvlan 2 svlan 4`	Map CVLAN 2 with SVLAN 4.
`PB1(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.
`PB1(config)#cvlan registration table customer2 bridge 1`	Create a CVLAN table customer2, and associate it with bridge 1.
`PB1(config-cvlan-registration)#cvlan 1 svlan 5`	Map CVLAN 1 with SVLAN 5.
`PB1(config-cvlan-registration)#cvlan 3 svlan 5`	Map CVLAN 3 with SVLAN 5.
`PB1(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.
`PB1(config)#interface eth2`	Enter interface mode.
`PB1(config-if)#switchport customer-edge vlan registration customer1`	Associate the customer1 table with the interface.
`PB1(config-if)#exit`	Exit interface mode.
`PB1(config)#interface eth3`	Enter interface mode.

`PB1(config-if)#switchport customer-edge vlan registration customer2`	Associate the customer2 table with the interface.
`PB1(config-if)#exit`	Exit interface mode.

PB2

`PB2#configure terminal`	Enter configure mode.
`PB2(config)#bridge 1 protocol provider-mstp edge`	Configure bridge 1 as a provider MSTP edge bridge.
`PB2(config)#vlan database`	Enter the VLAN Configure mode.
`PB2(config-vlan)#vlan 2 type customer bridge 1 state enable`	Configure VLAN 2 as a customer VLAN and associate it with bridge 1.
`PB2(config-vlan)#vlan 3 type customer bridge 1 state enable`	Configure VLAN 3 as a customer VLAN and associate it with bridge 1.
`PB2(config-vlan)#vlan 4 type service point-point bridge 1 state enable`	Configure VLAN 4 as a service VLAN and associate it with bridge 1.
`PB2(config-vlan)#vlan 5 type service point-point bridge 1 state enable`	Configure VLAN 5 as a service VLAN and associate it with bridge 1.
`PB2(config-vlan)#exit`	Exit the VLAN Configure mode.
`PB2(config)#interface eth2`	Enter interface mode.
`PB2(config-if)#switchport`	Configure eth2 as a Layer-2 interface.
`PB2(config-if)#bridge-group 1`	Associate the eth2 interface with bridge 1.
`PB2(config-if)#switchport mode customer-edge hybrid`	Configure the eth2 interface to hybrid mode.
`PB2(config-if)#switchport customer-edge hybrid allowed vlan all`	Configure the eth2 interface to allow all VLANs.
`PB2(config-if)#exit`	Exit interface mode.
`PB2(config)#interface eth3`	Enter interface mode.
`PB2(config-if)#switchport`	Configure eth3 as a Layer-2 interface.
`PB2(config-if)#bridge-group 1`	Associate the eth3 interface with bridge 1.
`PB2(config-if)#switchport mode customer-edge hybrid`	Configure the eth3 interface to hybrid mode.
`PB2(config-if)#switchport customer-edge hybrid allowed vlan all`	Configure the eth3 interface to allow all VLANs.
`PB2(config-if)#exit`	Exit interface mode.
`PB2(config)#interface eth1`	Enter interface mode.
`PB2(config-if)#switchport`	Configure eth1 as a Layer-2 interface.
`PB2(config-if)#bridge-group 1`	Associate the eth1 interface with bridge 1.
`PB2(config-if)#switchport provider-network allowed vlan add 4,5`	Associate Service VLAN 4 and Service VLAN 5 with the provider network.
`PB2(config-if)#exit`	Exit interface mode.
`PB2(config)#cvlan registration table customer1 bridge 1`	Create a CVLAN table customer1, and associate it with bridge 1.
`PB2(config-cvlan-registration)#cvlan 1 svlan 4`	Map CVLAN 1 with SVLAN 4.

© 2021 IP Infusion Inc. Proprietary

`PB2(config-cvlan-registration)#cvlan 2 svlan 4`	Map CVLAN 2 with SVLAN 4.
`PB2(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.
`PB2(config)#cvlan registration table customer2 bridge 1`	Create a CVLAN table customer2, and associate it with bridge 1.
`PB2(config-cvlan-registration)#cvlan 1 svlan 5`	Map CVLAN 1 with SVLAN 5.
`PB2(config-cvlan-registration)#cvlan 3 svlan 5`	Map CVLAN 3 with SVLAN 5.
`PB2(config-cvlan-registration)#exit`	Exit the CVLAN table configuration.
`PB2(config)#interface eth2`	Enter interface mode.
`PB2(config-if)#switchport customer-edge vlan registration customer1`	Associate the customer1 table with the interface.
`PB2(config-if)#exit`	Exit interface mode.
`PB2(config)#interface eth3`	Enter interface mode.
`PB2(config-if)#switchport customer-edge vlan registration customer2`	Associate the customer2 table with the interface.
`PB2(config-if)#exit`	Exit interface mode.

CE-A-1

`CE-A-1#configure terminal`	Enter configure mode.
`CE-A-1(config)#bridge 1 protocol mstp`	Create an MSTP bridge.
`CE-A-1(config)#vlan database`	Enter the VLAN Configure mode.
`CE-A-1(config-vlan)#vlan 2 bridge 1 state enable`	Create VLAN 2, and associate it with bridge 1.
`CE-A-1(config-vlan)#exit`	Exit the VLAN Configure mode.
`CE-A-1(config)#interface eth1`	Enter interface mode.
`CE-A-1(config-if)#switchport`	Configure eth1 as a Layer-2 interface.
`CE-A-1(config-if)#bridge-group 1`	Associate the eth1 interface with bridge 1.
`CE-A-1(config-if)#switchport mode hybrid`	Configure the eth1 interface to hybrid mode.
`CE-A-1(config-if)#switchport hybrid allowed vlan all`	Configure the eth1 interface to allow all VLANs.
`CE-A-1(config-if)#exit`	Exit interface mode.
`CE-A-1(config)#interface eth2`	Enter interface mode.
`CE-A-1(config-if)#switchport`	Configure eth2 as a Layer-2 interface.
`CE-A-1(config-if)#bridge-group 1`	Associate the eth2 interface with bridge 1.
`CE-A-1(config-if)#switchport mode hybrid`	Configure the eth2 interface to hybrid mode.
`CE-A-1(config-if)#switchport hybrid allowed vlan all`	Configure the eth2 interface to allow all VLANs.
`CE-A-1(config-if)#exit`	Exit interface mode.

CE-A-2

`CE-A-2#configure terminal`	Enter configure mode.
`CE-A-2(config)#bridge 1 protocol mstp`	Create an MSTP bridge.
`CE-A-2(config)#vlan database`	Enter the VLAN Configure mode.
`CE-A-2(config-vlan)#vlan 2 bridge 1 state enable`	Create VLAN 2, and associate it with bridge 1.
`CE-A-2(config-vlan)#exit`	Exit the VLAN Configure mode.
`CE-A-2(config)#interface eth1`	Enter interface mode.
`CE-A-2(config-if)#switchport`	Configure eth1 as a Layer-2 interface.
`CE-A-2(config-if)#bridge-group 1`	Associate the eth1 interface with bridge 1.
`CE-A-2(config-if)#switchport mode hybrid`	Configure the eth1 interface to hybrid mode.
`CE-A-2(config-if)#switchport hybrid allowed vlan all`	Configure the eth1 interface to allow all VLANs.
`CE-A-2(config-if)#exit`	Exit interface mode.
`CE-A-2(config)#interface eth2`	Enter interface mode.
`CE-A-2(config-if)#switchport`	Configure eth2 as a Layer-2 interface.
`CE-A-2(config-if)#bridge-group 1`	Associate the eth2 interface with bridge 1.
`CE-A-2(config-if)#switchport mode hybrid`	Configure the eth2 interface to hybrid mode.
`CE-A-2(config-if)#switchport hybrid allowed vlan all`	Configure the eth2 interface to allow all VLANs.
`CE-A-2(config-if)#exit`	Exit interface mode.

CE-B-1

`CE-B-1#configure terminal`	Enter configure mode.
`CE-B-1(config)#bridge 1 protocol mstp`	Create an MSTP bridge.
`CE-B-1(config)#vlan database`	Enter the VLAN Configure mode.
`CE-B-1(config-vlan)#vlan 3 bridge 1 state enable`	Create VLAN 3, and associate it with bridge 1.
`CE-B-1(config-vlan)#exit`	Exit the VLAN Configure mode.
`CE-B-1(config)#interface eth1`	Enter interface mode.
`CE-B-1(config-if)#switchport`	Configure eth1 as a Layer-2 interface.
`CE-B-1(config-if)#bridge-group 1`	Associate the eth1 interface with bridge 1.
`CE-B-1(config-if)#switchport mode hybrid`	Configure the eth1 interface to hybrid mode.
`CE-B-1(config-if)#switchport hybrid allowed vlan all`	Configure the eth1 interface to allow all VLANs.
`CE-B-1(config-if)#exit`	Exit interface mode.
`CE-B-1(config)#interface eth3`	Enter interface mode.
`CE-B-1(config-if)#switchport`	Configure eth3 as a Layer-2 interface.
`CE-B-1(config-if)#bridge-group 1`	Associate the eth3 interface with bridge 1.
`CE-B-1(config-if)#switchport mode hybrid`	Configure the eth3 interface to hybrid mode.

© 2021 IP Infusion Inc. Proprietary

`CE-B-1(config-if)#switchport hybrid allowed vlan all`	Configure the eth3 interface to allow all VLANs.
`CE-B-1(config-if)#exit`	Exit interface mode.

CE-B-2

`CE-B-2#configure terminal`	Enter configure mode.
`CE-B-2(config)#bridge 1 protocol mstp`	Create an MSTP bridge.
`CE-B-2(config)#vlan database`	Enter the VLAN Configure mode.
`CE-B-2(config-vlan)#vlan 3 bridge 1 state enable`	Create VLAN 3, and associate it with bridge 1.
`CE-B-2(config-vlan)#exit`	Exit the VLAN Configure mode.
`CE-B-2(config)#interface eth1`	Enter interface mode.
`CE-B-2(config-if)#switchport`	Configure eth1 as a Layer-2 interface.
`CE-B-2(config-if)#bridge-group 1`	Associate the eth1 interface with bridge 1.
`CE-B-2(config-if)#switchport mode hybrid`	Configure the eth1 interface to hybrid mode.
`CE-B-2(config-if)#switchport hybrid allowed vlan all`	Configure the eth1 interface to allow all VLANs.
`CE-B-2(config-if)#exit`	Exit interface mode.
`CE-B-2(config)#interface eth3`	Enter interface mode.
`CE-B-2(config-if)#switchport`	Configure eth3 as a Layer-2 interface.
`CE-B-2(config-if)#bridge-group 1`	Associate the eth3 interface with bridge 1.
`CE-B-2(config-if)#switchport mode hybrid`	Configure the eth3 interface to hybrid mode.
`CE-B-2(config-if)#switchport hybrid allowed vlan all`	Configure the eth3 interface to allow all VLANs.
`CE-B-2(config-if)#exit`	Exit interface mode.

Validation

```
PB1#show cvlan registration table bridge 1
Bridge          Table Name       Port List
======          ==========       =========
1               customer1       eth2
CVLAN ID        SVLAN ID
========        ========
1               4
2               4

Bridge          Table Name       Port List
======          ==========       =========
1               customer2        eth3

CVLAN ID        SVLAN ID
========        ========
1               5
3               5
```

```
PB2#show cvlan registration table bridge 1
Bridge          Table Name       Port List
======          ==========       =========
1               customer1        eth2

CVLAN ID        SVLAN ID
========        ========
1               4
2               4

Bridge          Table Name       Port List
======          ==========       =========
1               customer2        eth3

CVLAN ID        SVLAN ID
========        ========
1               5
3               5
```

Host A-1 and Host A-2

Host machine (Host-A-1 [8.8.8.5]) of customer A on VLAN2 should be able to ping host machine (Host-A-2 [8.8.8.3]) in customer A's other site on the same VLAN.

```
[root@Host-A-1 root]#ping 8.8.8.3
PING 8.8.8.3(8.8.8.3) 56(84) bytes of data.
64 bytes from 8.8.8.3: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 8.8.8.3: icmp_seq=2 ttl=64 time=0.015 ms
--- 8.8.8.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.015/0.023/0.032/0.009 ms
```

Host B-2 and Host B-1

Host machine (Host-B-2 [8.8.8.2]) of customer B on VLAN3 should be able to ping host machine (Host-B-1 [8.8.8.8]) in customer B's other site on the same VLAN.

```
[root@Host-B-2 root]#ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.2: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 8.8.8.2: icmp_seq=2 ttl=64 time=0.015 ms
--- 8.8.8.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.015/0.023/0.032/0.009 ms
```

Host A-2 and Host B-1

Host machine (Host-A-2 [8.8.8.3]) of customer A on VLAN2 should not be able to ping host machine (Host-B-1 [8.8.8.8] in customer B's site because it is in a different VLAN.

```
[root@Host-A-2 root]#ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5010ms
```


© 2021 IP Infusion Inc. Proprietary

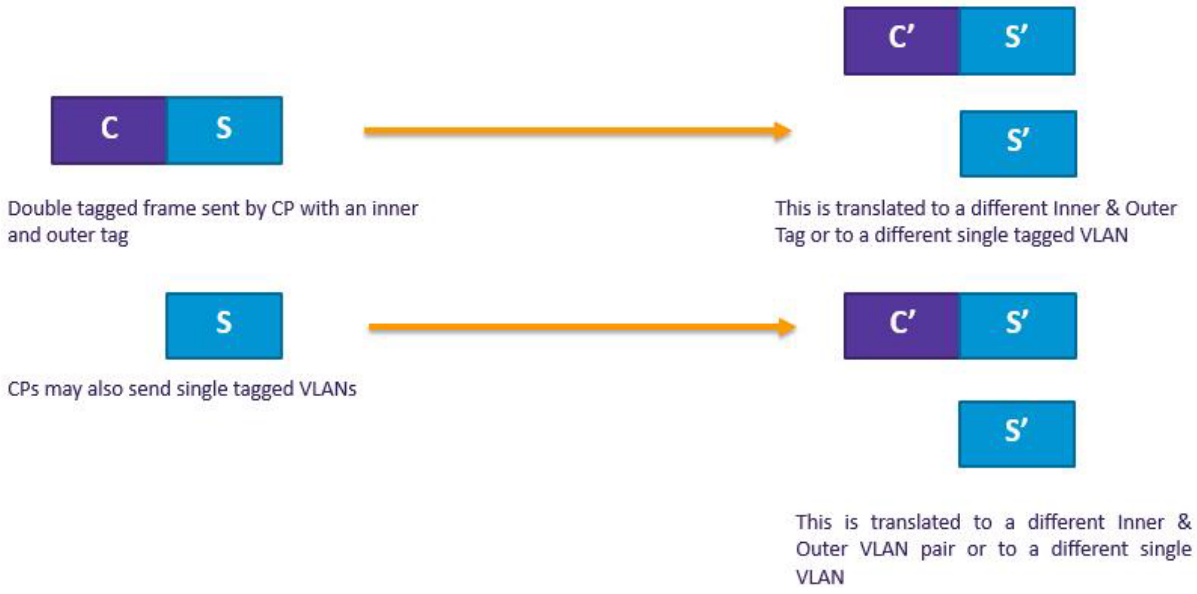
Host B-2 and Host A-1

Host machine (Host-B-2 [8.8.8.2]) of customer B on VLAN3 should not be able to ping host machine (Host-A-1 [8.8.8.5] in customer A's site because it is in a different VLAN.

```
[root@QA-33 root]#ping 8.8.8.5
PING 8.8.8.5 (8.8.8.5) 56(84) bytes of data.
--- 8.8.8.5 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1015ms
```

Provider Bridging with VLAN Translation

This is a sample configurations to verify functionality to support provider-bridging feature with extended SVLAN translation as below:



Topology

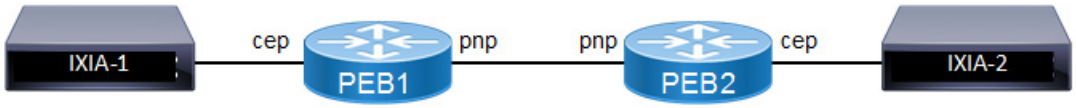


Figure 4-26: Provider Bridging with VLAN Traslation Topology

PEB1

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol provider-mstp edge`	Enter Configure bridge type as provider-MSTP edge bridge
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`(config-vlan)#vlan 2 type customer bridge 1 state enable`	Configure VLAN 2 as a customer VLAN and associate it with bridge 1
`(config-vlan)#vlan 3 type customer bridge 1 state enable`	Configure VLAN 3 as a customer VLAN and associate it with bridge 1
`(config-vlan)#vlan 6 type service point-point bridge 1 state enable`	Configure VLAN 6 as a service VLAN and associate it with bridge 1
`(config-vlan)#vlan 7 type service point-point bridge 1 state enable`	Configure VLAN 7 as a service VLAN and associate it with bridge 1
`(config-vlan)#end`	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`PEB1(config-cvlan-registration)#cvlan 2 svlan 6 untagged-pep`	Map CVLAN to SVLAN
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode customer-edge hybrid`	Configure port as customer-edge hybrid port
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Add all VLANs configured above to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#exit`	Exit interface and configure mode.

© 2021 IP Infusion Inc. Proprietary

PNP Port Configuration

`(config)#interface ge3`	Enter interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port
`(config-if)#exit`	Exit interface and configure mode.

PEB2

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol provider-mstp edge`	Enter configure bridge type as provider-MSTP edge bridge
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`vlan 2 type customer bridge 1 state enable`	Configure VLAN 2 as a customer VLAN and associate it with bridge 1
`vlan 3 type customer bridge 1 state enable`	Configure VLAN 3 as a customer VLAN and associate it with bridge 1
`vlan 6 type service point-point bridge 1 state enable`	Configure VLAN 6 as a service VLAN and associate it with bridge 1
`vlan 7 type service point-point bridge 1 state enable`	Configure VLAN 7 as a service VLAN and associate it with bridge 1
`(config-vlan)#end`	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode customer-edge hybrid`	Configure port as customer-edge hybrid port
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Add all VLANs configured above to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#exit`	Exit interface and configure mode.

PNP Port Configuration

`(config)#interface ge9`	Enter interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port
`(config-if)#exit`	Exit interface and configure mode.

Translation Cases

Case1 - (C S - C' S')

Configuration on PEB2

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter interface mode
`(config-if)#switchport provider-network vlan translation cvlan 2 svlan 6 cvlan 3 svlan 7`	Translate CVLAN and SVLAN to new CVLAN and new SVLAN on PNP port

Validation for Case1

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with both CTAG and STAG entering provider network and gets translated to new CVLAN and SVLAN as per Case1.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address      FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1                1             ge27         1402.ec1c.3144    1     300
 1                6             ge9          6400.6a1e.d9a5    1     300
 1                7             ge9          0000.0500.0400    1     300
 1                7             ge9          6400.6a1e.d9a5    1     300
```

New SVLAN 7 is observed on PEB2 after translation. Also, captured packets on CEP show new CVLAN 3.

© 2021 IP Infusion Inc. Proprietary

When tagged traffic for CVLAN 3 is sent from IXIA-2 to IXIA-1

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+------------------+-----+---------+
 1               1             ge9          74e6.e2af.598b    1     300
 1               6             ge3          0000.0500.0400    1     300
 1               6             ge9          0000.0500.0700    1     300
```

When traffic is reversed and traffic has both new CVLAN 3 and SVLAN 7 on provider network from IXIA-2, translation to old CVLAN 2 and SVLAN 6 happens. Also, captured packets have CVLAN as 2.

Case2 - (C S - S')

Configuration on PEB2

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7 untagged-pep`	Map CVLAN to SVLAN with untagged-pep
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter interface mode
`(config-if)#switchport customer-edge hybrid vlan 3`	Allow access VLAN 3 configured above to this CEP port
`(config-if)#switchport customer-edge hybrid allowed vlan add 2-3 egress-tagged disable`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#exit`	Exit interface and configure mode.

PNP Port Configuration

`(config)#interface ge9`	Enter interface mode
`(config-if)#no switchport provider-network vlan translation cvlan 2 svlan 6`	Unconfigure Translation Case1 from PNP port
`(config-if)#switchport provider-network vlan translation cvlan 2 svlan 6 svlan 7`	Configure Translation Case2 on PNP port
`(config-if)#exit`	Exit interface and configure mode.

Validation for Case2

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with both CTAG and STAG entering provider network and translated to new SVLAN as per Case2.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+------------------+-----+---------+
 1                 1             ge27         1402.ec1c.3144    1     300
 1                 7             ge9          0000.0500.0400    1     300
```

New SVLAN 7 is observed on PEB2 after translation. At CEP port connected to IXIA-2, untagged traffic should be received.

When tagged traffic for CVLAN 3 is sent from IXIA-2 to IXIA-1.

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+------------------+-----+---------+
 1                 1             ge9          74e6.e2af.598b    1     300
 1                 6             ge3          0000.0500.0400    1     300
 1                 6             ge9          0000.0500.0700    1     300
```

When traffic is reversed and traffic has both new CVLAN 3 and SVLAN 7 from IXIA-2, translatiom to old CVLAN 2 and SVLAN 6 happens. Also, captured packets have CVLAN as 2.

Case3 - (S - S')

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 2 svlan 6 untagged-pep`	Map CVLAN to SVLAN with untagged-pep
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter interface mode
`(config-if)#switchport customer-edge hybrid vlan 2`	Allow access VLAN 2 configured above to this CEP port
`(config-if)#switchport customer-edge hybrid allowed vlan add 2-3 egress-tagged disable`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#exit`	Exit interface and configure mode.

© 2021 IP Infusion Inc. Proprietary

Configuration on PEB2

CVLAN Registration Table Configuration

`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7 untagged-pep`	Map CVLAN to SVLAN with untagged-pep
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter interface mode
`(config-if)#switchport customer-edge hybrid vlan 3`	Allow access VLAN 3 configured above to this CEP port
`(config-if)#switchport customer-edge hybrid allowed vlan add 2-3 egress-tagged disable`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#exit`	Exit interface and configure mode.

PNP Port Configuration

`(config)#interface ge9`	Enter interface mode
`(config-if)#no switchport provider-network vlan translation cvlan 2 svlan 6`	Unconfigure Translation Case2 from PNP port
`(config-if)#switchport provider-network vlan translation svlan 6 svlan 7`	Configure Translation Case3 on PNP port
`(config-if)#exit`	Exit interface and configure mode.

Validation for Case3

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with only STAG entering provider network and translation happens to new SVLAN as per Case3.

```
PEB2#show bridge
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+-----------------+-----+---------+
 1               1             ge27        1402.ec1c.3144    1     300
 1               7             ge9         0000.0500.0400    1     300
 1               7             ge9         6400.6a1e.d9a5    1     300
```

New SVLAN 7 is observed on PEB2 after translation . At CEP port connected to IXIA-2, untagged traffic should be received.

When tagged traffic for CVLAN 3 is sent from IXIA-2 to IXIA-1:

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+-----------------+-----+---------+
 1               1             ge9         74e6.e2af.598b    1     300
```

```
1                6              ge3          0000.0500.0400    1      300
1                6              ge9          0000.0500.0700    1      300
```

When traffic is reversed and traffic has SVLAN 7 in provider network, translation to old CVLAN 2 and SVLAN 6 happens. Also, captured packets untagged traffic at other end.

Case4 - (S - C' S')

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 2 svlan 6 untagged-pep`	Map CVLAN to SVLAN with untagged-pep
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter interface mode
`(config-if)#switchport customer-edge hybrid vlan 2`	Allow access VLAN 2 configured above to this CEP port
`(config-if)#switchport customer-edge hybrid allowed vlan add 2-3 egress-tagged disable`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#exit`	Exit interface and configure mode.

Configuration on PEB2

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter interface mode
`(config-if)#switchport`	Configure switchport

© 2021 IP Infusion Inc. Proprietary

(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode customer-edge hybrid	Configure port as customer-edge hybrid port
(config-if)#switchport customer-edge hybrid allowed vlan all	Allow other VLANs configured to this CEP port
(config-if)#switchport customer-edge vlan registration map1	Attach the Map1 to CEP port
(config-if)#exit	Exit interface and configure mode.

PNP Port Configuration

(config)#interface ge9	Enter interface mode
(config-if)#no switchport provider-network vlan translation svlan 6 svlan 7	Unconfigure Translation Case2 from PNP port
(config-if)#switchport provider-network vlan translation svlan 6 cvlan 3 svlan 7	Configure Translation Case3 on PNP port
(config-if)#exit	Exit interface and configure mode.

Validation for Case4

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with only STAG entering provider network and translation happens to new CVLAN and new SVLAN as per Case4.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+------------------+-----+---------+
 1               1             ge27         1402.ec1c.3144     1     300
 1               7             ge9          0000.0500.0400     1     300
 1               7             ge9          6400.6a1e.d9a5     1     300
```

New SVLAN 7 is observed on PEB2 after translation. At CEP port connected to IXIA-2, traffic should be received with CVLAN 3.

When tagged traffic for CVLAN 3 is sent from IXIA-2 to IXIA-1:

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+------------------+-----+---------+
 1               6             ge3          0000.0500.0400     1     300
 1               6             ge9          0000.0500.0700     1     300
```

When traffic is reversed and traffic has SVLAN 7 in provider network, translation to old CVLAN 2 and SVLAN 6 happens. Also captured packets untagged traffic at other end.

Layer 2 Protocol Tunneling (L2PT/L2CP Tunneling)

L2CP tunneling provides support for tunneling Control plane frames between CE nodes.

When control frames received at CEP port of PE bridge, predefined multicast address (01-00-C2-CD-CD-D0) is used for tunneling the packets across service provider network. If control packets are customer vlan tagged or untagged, then PE bridge will append corresponding service vlan tag to the control packet as per registration table / vlan translation table mapped to the port and send it across the service provider as a data packet.

When tunneled control packet with multicast address (01-00-C2-CD-CD-D0) received on PNP port, the multicast address is replaced with corresponding control packet multicast address and cvlan/svlan removal or updating is done as per registration table / vlan translation table.

Topology

Figure 4-27 displays a sample Provider Bridged topology with customer equipment.

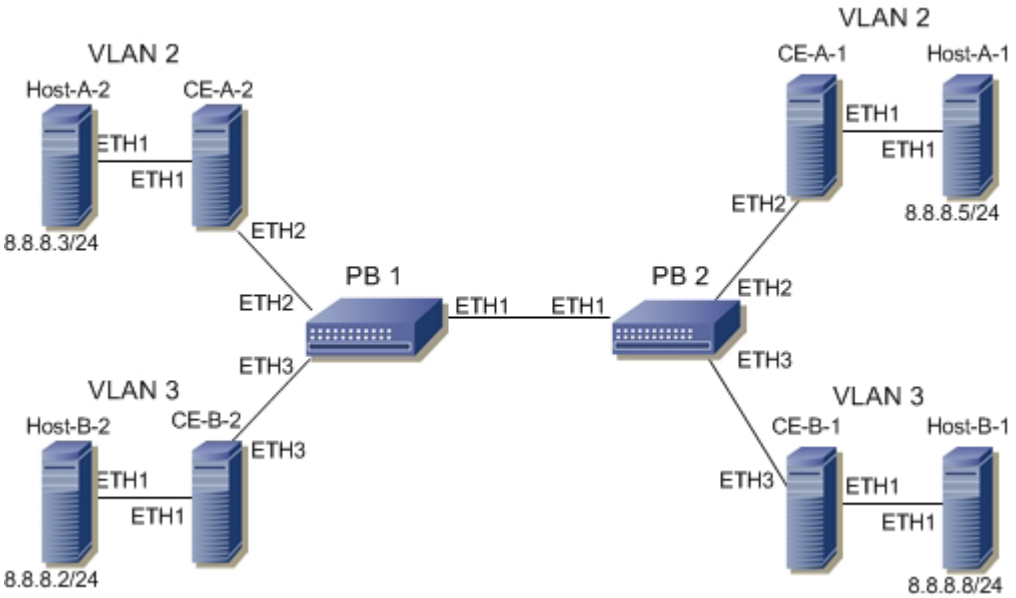


Figure 4-27: Provider Bridging with Customer Equipment Topology

Configuring the L2PT Protocol on the Interface

The following L2PT protocols are supported:

- EFM: Ethernet first mile (Link OAM)
- ELMI: Ethernet Local Management Interface
- LACP: Link Aggregation Control Protocol
- LLDP: Link Layer Discovery Protocol
- STP: Spanning Tree Protocols
- SyncE: Synchronous Ethernet

PB1

`PB1#configure terminal`	Enter Configure mode.
`PB1(config)#interface eth2`	Enter Interface mode
`PB1(config-if)#l2protocol stp peer`	Configure STP protocol as peer
`PB1(config-if)#l2protocol elmi tunnel`	Configure Elmi protocol as tunnel
`PB1(config-if)#l2protocol lldp tunnel`	Configure LLDP protocol as tunnel
`PB1(config-if)#l2protocol lacp discard`	Configure LACP protocol as discard

© 2021 IP Infusion Inc. Proprietary

PB1(config-if)#l2protocol efm discard	Configure EFM protocol as discard
PB1(config-if)#l2protocol synce discard	Configure Synce protocol as discard
PB1(config-if)#exit	Exit of the interface

Validation

```
PB1#show l2protocol processing interface eth2
Bridge    Interface Name                  Protocol       Processing Status
======    ==============                  ========       =================
1         eth2                           stp            Peer
1         eth2                           gmrp           Peer
1         eth2                           gvrp           Peer
1         eth2                           mmrp           Peer
1         eth2                           mvrp           Peer
1         eth2                           lacp           Discard
1         eth2                           lldp           Tunnel
1         eth2                           efm            Discard
1         eth2                           elmi           Tunnel
1         eth2                            ptp           Peer
1         eth2                          synce          Discard
```

© 2021 IP Infusion Inc. Proprietary

Carrier Ethernet Command Reference

Contents

This document contains these chapters and appendices:

- Chapter 1, *CFM Commands*
- Chapter 2, *G.8032 ERPS Version 2 Commands*
- Chapter 3, *Provider Bridging Commands*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 CFM Commands

This chapter describes the commands used to manage the Connectivity Fault Management (CFM). CFM refers to the service OAM of Ethernet used to manage individual Layer 2 Ethernet services. The CFM protocol can discover and verify the path through 802.1 bridges and LANs. OcNOS adheres to the IEEE 802.1ag 2007 standard.

- cc interval
- cc multicast
- clear ethernet cfm maintenance-point remote
- clear ethernet cfm traceroute-cache
- ethernet cfm domain-type
- ethernet cfm mep
- exit-ether-ma-mep-mode
- exit-ether-ma-mode
- mep crosscheck
- mep lowest-priority-defect
- ping ethernet mac
- service ma-type
- show ethernet cfm errors
- show ethernet cfm ma status
- show ethernet cfm maintenance-points local mep
- show ethernet cfm maintenance-points local mip
- show ethernet cfm maintenance-points remote
- show running-config cfm
- traceroute ethernet

© 2021 IP Infusion Inc. Proprietary

cc interval

Use this command to set the continuity checking (CC) message interval.

Command Syntax

```
cc interval (3|4|5)
```

Parameters

3	100 milliseconds
4	1 seconds
5	10 seconds

Command Mode

Ethernet CFM MA mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#cc interval 3
```


© 2021 IP Infusion Inc. Proprietary

cc multicast

Use this command to start or stop multicast continuity checking messages (CCMs) on a MEP.

Command Syntax

```
cc multicast state (enable|disable)
```

Parameters

`enable`	Start sending CCMs
`disable`	Stop sending CCMs

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10 xe2
(config-ether-cfm-ma-mep)#cc multicast state enable
```

clear ethernet cfm maintenance-point remote

Use this command to remove a dynamically learned RMEP.

The RMEP is relearned if service ma-type is enabled and a CCM (Continuity Checking Message) is received.

Command Syntax

```
clear ethernet cfm maintenance-points remote domain <DOMAIN_NAME> bridge <1-32>
```

Parameters

DOMAIN_NAME	MD name
<1-32>	Bridge identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#clear ethernet cfm maintenance-points remote domain abcde bridge 1
```


© 2021 IP Infusion Inc. Proprietary

clear ethernet cfm traceroute-cache

Use this command to clear the CFM traceroute cache entry.

Command Syntax

```
clear ethernet cfm traceroute-cache bridge <1-32>
```

Parameters

<1-32>	Bridge identifier

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#clear ethernet cfm traceroute-cache bridge 1
```

ethernet cfm domain-type

Use this command to create a CFM Maintenance Domain (MD) in a bridge and enter Ethernet CFM mode.

Use the `no` form of this command to remove a domain.

Note: You can create up to 15 MDs in a bridge.

Only one domain can be created without any domain name in a bridge.

A domain name of type `character-string` can only created only after the mep crosscheck command is executed.

Command Syntax

```
ethernet cfm domain-type (no-name|character-string) domain-name DOMAIN_NAME level
  <0-7> mip-creation (none|default|explicit) bridge <1-32>
```

```
no ethernet cfm domain-name DOMAIN_NAME level <0-7> mip-creation
  (none|default|explicit) bridge <1-32>
```

Parameters

`domain-type`	Domain type (must match service ma-type setting)
`no-name`	No MD name. The `ma-type` must be `integer` or `itu-t` carrier code (ICC) format defined by Y.1731.
`character-string`	Character string name. The `ma-type` must be string.
`DOMAIN_NAME`	Domain name (name must be a 5-character string)
`<0-7>`	MD level
`mip-creation`	Maintenance Intermediate Point (MIP) creation permission for this domain
`none`	No MIP can be created for this VLAN identifier
`default`	MIP can be created if no lower active level or MEP at next lower active level
`explicit`	Maintenance End Point (MEP) is needed at the next lower active level
`<1-32>`	Bridge identifier

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7
mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation
none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10
xe7
(config-ether-cfm-ma-mep)#
```


© 2021 IP Infusion Inc. Proprietary

ethernet cfm mep

Use this command to create a Maintenance End Point (MEP), make it active or inactive and enter Ethernet CFM MA MEP mode.

A MEP created with the `active false` option remains inactive and CFM functionality is suspended for such a MEP.

Use the `no` form of this command to delete a MEP.

Command Syntax

```
ethernet cfm mep down mpid MEPID active (false|true) (local-vid VID|) IFNAME
no ethernet cfm mep down mpid MEPID (local-vid VID|) IFNAME
```

Parameters

`down`	Down MEP
`MEPID`	Host MEP identifier <1-8191>
`active`	Administrative state of the MEP
`true`	Make the MEP active
`false`	Make the MEP inactive
`VID`	Local VLAN identifier for the MEP, a secondary VLAN for the MA
`IFNAME`	Interface name

Command Mode

Ethernet CFM MA mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7
mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation
none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10
xe2
(config-ether-cfm-ma-mep)#
```

exit-ether-ma-mep-mode

Use this command to exit Ethernet CFM MA MEP mode and go back to Ethernet CFM MA mode.

Command Syntax

```
exit-ether-ma-mep-mode
```

Parameters

None

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10 xe2
(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode
```


© 2021 IP Infusion Inc. Proprietary

exit-ether-ma-mode

Use this command to exit Ethernet CFM MA mode and go back to Ethernet CFM mode.

Command Syntax

```
exit-ether-ma-mode
```

Parameters

None

Command Mode

Ethernet CFM MA mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#exit-ether-ma-mode
```

mep crosscheck

Use this command to configure a remote MEP crosscheck.

Use the `no` form of this command to delete a crosscheck MEP.

Command Syntax

```
mep crosscheck mpid MEPID
no mep crosscheck mpid MEPID
```

Parameters

`MEPID`	Remote host MEP identifier <1-8191>

Command Mode

Ethernet CFM MA mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#mep crosscheck mpid 51
```


© 2021 IP Infusion Inc. Proprietary

mep lowest-priority-defect

Use this command to set the lowest-priority defect that can generate a fault alarm.

Use the `no` form of this command to set the lowest-priority defect to its default (`defMACstatus`).

Command Syntax

```
mep lowest-priority-defect
  (defRDICCM|defMACstatus|defRemoteCCM|defErrorCCM|defXconCCM)
no mep lowest-priority-defect
```

Parameters

`defRDICCM`	1 (lowest): At least one of the Remote MEP state machines is receiving valid CCMs from its remote MEP that has the Remote Defect Indication (RDI) bit set.
`defMACstatus`	2: One or more of the remote MEPs is reporting a failure in its Port Status Type-Length-Value (TLV) or Interface Status TLV: MEP Down.
`defRemoteCCM`	3: At least one of the remote MEP state machines is not receiving valid CCMs from its remote MEP.
`defErrorCCM`	4: One or more invalid CCMs has been received, and 3.5 times the CCMs' transmission interval has not yet expired.
`defXconCCM`	5: (highest): One or more cross-connect continuity check messages (CCMs) has been received, and 3.5 times at least one of those CCMs' transmission interval has not yet expired.

Default Value

defMACstatus

Command Mode

Ethernet CFM MA MEP mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10 xe7
(config-ether-cfm-ma-mep)#mep lowest-priority-defect defRemoteCCM
```

ping ethernet mac

Use this command to send a loopback message for a MAC address to a remote MEP for fault verification. Use either the `domain` or the `level` parameter with the `vlan` or `bridge` parameter to target a specific device.

Command Syntax

```
ping ethernet mac MACADDRESS unicast source MEPID (domain DOMAIN_NAME | level <0-
  7>) (vlan VLAN_ID | bridge <1-32> |)
```

Parameters

`MACADDRESS`	Destination MAC address in HHHH.HHHH.HHHH format
`MEPID`	Source host MEP ID <1-8191>
`DOMAIN_NAME`	Maintenance domain name of MEP
`<0-7>`	Level associated with the domain
`VLAN_ID`	Primary VLAN identifier <2-4094> of the MA
`<1-32>`	Bridge identifier

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#ping ethernet mac 0018.236e.5eb5 unicast source 201 domain 12345 vlan 10 bridge 1
success rate is  100 (5/5)
```


© 2021 IP Infusion Inc. Proprietary

service ma-type

Use this command to create a service Maintenance Association (MA), with or without a VLAN, and enter Ethernet CFM MA mode

This command allows creation of a maintenance association for link-level MEPs (level 0) which do not listen on a VLAN.

A VID can be associated with an MA only at the time of MA creation. If an MA is created without a VID, a VID cannot be added to it during runtime because an MA without a VID is a link-level MA.

Use the `no` form of this command to remove an MA.

Command Syntax

```
service ma-type (string|integer|itu-t) ma-name MA_NAME (vlan VLAN_ID mip-creation
  (none|default|explicit|defer)
```

```
no service ma-name MA_NAME (vlan VLAN_ID mip-creation (none|default|explicit|defer)
```

Parameters

`ma-type`	Type of MA name (must match ethernet cfm domain-type `md-type` setting)
`string`	Character MA name. The `md-type` must be `character-string`.
`integer`	Integer MA name. The `md-type` must be `no-name`.
`itu-t`	ITU-T carrier code (ICC) format name defined by Y.1731.The `md-type` must be `integer`.
`MA_NAME`	MA name
`VLAN_ID`	Primary VLAN identifier <2-4094>
`mip-creation`	Maintenance domain Intermediate Point (MIP) creation permission for this domain
`none`	No MIP can be created for this VLAN identifier
`default`	MIP can be created if no lower active level or MEP at next lower active level
`explicit`	MEP is needed at the next lower active level
`defer`	Use the MIP creation permissions of the MD to which this MA belongs

Command Mode

Ethernet CFM mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#ethernet cfm domain-type character-string domain-name 12345 level 7 mip-
creation none bridge 1
(config-ether-cfm)#service ma-type string ma-name 43982 vlan 10 mip-creation none
(config-ether-cfm-ma)#ethernet cfm mep down mpid 201 active true local-vid 10 xe7
(config-ether-cfm-ma-mep)#
```

show ethernet cfm errors

Use this command to verify the defects present in a MEP.

Command Syntax

```
show ethernet cfm errors domain DOMAIN_NAME bridge <1-32>
```

Parameters

DOMAIN_NAME	Maintenance domain name
<1-32>	Bridge identifier

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm errors domain 12345 bridge 1
Domain Name      Level     Vlan      MEPID      Defects
-----------------------------------------------------
12345             7        10        100        .....
```

Table 1-209 explains the output fields

Table 1-209: show ethernet cfm errors

Field	Description
Domain Name	Maintenance Domain name
Level	MD Level
Vlan	Vlan identifier
MEPID	Maintenance End Point identifier
Defects	Defects in current MEP

© 2021 IP Infusion Inc. Proprietary

show ethernet cfm ma status

Use this command to display the connectivity status of Maintenance Associations (MAs) in a domain.

Command Syntax

```
show ethernet cfm ma status domain DOMAIN_NAME (vlan <2-4094>|)
  (mep <1-8191>| mep all|) bridge <1-32>
```

Parameters

DOMAIN_NAME	Maintenance domain name
<2-4094>	VLAN identifier
mep	Host MEP
<1-8191>	Host MEP identifier
all	All host MEPs
<1-32>	Bridge identifier

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm ma status domain 12345 vlan 10 bridge 1
MA NAME        VLAN                  STATUS
-----------------------------------------
  43982          10                  Active
```

Table 1-210 explains the output fields.

Table 1-210: show ethernet cfm ma status

Field	Description
MA NAME	Maintenance Association name
VLAN	VLAN identifier
STATUS	Active: All connected MEPs in MA are receiving the CCM with no defect or alarm present Partially Active: One or more connected MEPs in MA is not receiving CCM or it is receiving CCM with defect or alarm present Not Active: None of the connected MEPS in MA are receiving CCM or it is receiving CCM with defect or alarm present

show ethernet cfm maintenance-points local mep

Use this command to display information about the Maintenance End Points (MEPs) on a local interface.

Command Syntax

```
show ethernet cfm maintenance-points local mep (interface IFNAME|domain
  DOMAIN_NAME|level <0-7>) bridge <1-32>
```

Parameters

IFNAME	Interface name. This token can be used only for Down MEPs on L2 bridge.
DOMAIN_NAME	Maintenance domain name
<0-7>	Maintenance level
<1-32>	Bridge identifier

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm maintenance-point local mep level 7 bridge 1
MPID  Dir Lvl  VLAN  CC-Stat  HW-Status  CC-Intvl  MAC-Address    Def  Port  MD Name
--------------------------------------------------------------------------------
100   Dn   7    10    Enable   Installed  100 ms   3c2c.99f0.b0c1  F    xe2   12345

#show ethernet cfm maintenance-points local mep domain 12345 bridge 1
MPID  Dir Lvl  VLAN  CC-Stat  HW-Status  CC-Intvl  MAC-Address    Def  Port  MD Name
--------------------------------------------------------------------------------
100   Dn   7    10    Enable   Installed  100 ms   3c2c.99f0.b0c1  F    xe2   12345
```

Table 1-211 explains the output fields.

Table 1-211: show ethernet cfm maintenance-points local mep

Field	Description
MPID	MEP identifier
Dir	Up MEP or Down MEP
Lvl	MD level
Vlan	VLAN identifier
CC-Stat	Whether continuity checking (CC) is enabled or disabled
HW-Status	Installed or pending to install in hardware
CC-Intvl	CCM Interval

© 2021 IP Infusion Inc. Proprietary

Table 1-211: show ethernet cfm maintenance-points local mep

Field	Description
MAC-Address	MAC address
Def	Defect present
Port	CFM interface
MD Name	MD name

show ethernet cfm maintenance-points local mip

Use this command to display information about the Maintenance Intermediate Points (MIPs) on a local interface.

Command Syntax

```
show ethernet cfm maintenance-points local mip (interface IFNAME|level <0-7>)
  (bridge <1-32>|)
```

Parameters

IFNAME	Interface name.
<0-7>	Maintenance level.
<1-32>	Bridge identifier.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm maintenance-points local mip level 7 bridge 1
Level  VID   Type  Port   MAC-Address
------------------------------------------------------
7      10    MIP   xe3    0018.23ea.da36
7      10    MIP   xe5    0018.23ea.da38
```

Table 1-212 explains the output fields.

Table 1-212: show ethernet cfm maintenance-points local mip

Field	Description
Level	MD level
VID	VLAN identifier
Type	MIP
Port	Interface name
MAC-Address	MAC address

© 2021 IP Infusion Inc. Proprietary

show ethernet cfm maintenance-points remote

Use this command to display information about a remote MEP.

Command Syntax

```
show ethernet cfm maintenance-points remote (mpid MEP_ID|) (domain
  DOMAIN_NAME|level LEVEL_ID) (vlan VLAN_ID|) bridge <1-32>
```

Parameters

MEP_ID	Remote MEP identifier <1-8191>
DOMAIN_NAME	Maintenance domain name
LEVEL_ID	Maintenance level <0-7>
VLAN_ID	VLAN identifier <2-4094>
<1-32>	Bridge identifier

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show ethernet cfm maintenance-points remote level 7 bridge 1
MEPID   RMEPID   LEVEL   VLAN    Rx CCM    RDI     PEER-MAC         TYPE
------------------------------------------------------------------------------
100     200        7      10       Yes    False   a82b.b579.fd2a   Configured

#show ethernet cfm maintenance-points remote domain 12345 bridge 1
MEPID   RMEPID   LEVEL   VLAN    Rx CCM    RDI     PEER-MAC         TYPE
------------------------------------------------------------------------------
100     200         7       10        Yes      False    a82b.b579.fd2a    Configured
```

Table 1-213 explains the output fields.

Table 1-213: show ethernet cfm maintenance-points remote

Field	Description
MEPID	MEP identifier
RMEPID	Remote MEP identifier
LEVEL	MD level
VLAN	VLAN identifier
Rx CCM	Yes if CCM receives, no if CCM doesn't receive.
RDI	Whether Remote Defect Indication (RDI) is on or off

Table 1-213: show ethernet cfm maintenance-points remote

Field	Description
PEER-MAC	Remote MEP mac address
TYPE	Configured or auto learned

© 2021 IP Infusion Inc. Proprietary

show running-config cfm

Use this command to display CFM running configuration alone.

Command Syntax

```
show running-config cfm
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#show running-config cfm
ethernet cfm domain-type character-string domain-name 12345 level 7 mip-
creation none bridge 1
 service ma-type string ma-name 43982 vlan 10 mip-creation none
   ethernet cfm mep down mpid 201 active true local-vid 10 xe2
     cc multicast state enable
     exit-ether-ma-mep-mode
   mep crosscheck mpid 18
   cc interval 3
   exit-ether-ma-mode
!
```

traceroute ethernet

Use this command to start traceroute messages on a remote MEP.

Command Syntax

```
traceroute ethernet MAC mepid MEPID (domain DOMAIN | level <0-7>) (vlan VLANID |
  bridge <1-32> | )
```

Parameters

MAC	MAC address of the remote MEP or MIP in HHHH.HHHH.HHHH format.
MEPID	Host MEP identifier <1-8191>.
DOMAIN	MD name of the destination MEP or MIP.
<0-7>	Maintenance level to which remote MEP or MIP belongs.
VLANID	Primary VLAN identifier to which the destination MEP or MIP is associated.<2-4096>.
<1-32>	Bridge identifier.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#traceroute ethernet 0018.236e.5eb8 mepid 201 domain 12345 vlan 10 bridge 1
MP Mac         Hops  Relay-action          Ingress/Egress  Ingress/Egress
action
0018.23ea.da36   1     RlyFDB                Ingress         IngOK
0018.23ea.da38   2     RlyFDB                Egress          EgrOK
0018.236e.5eb8   3     RlyHit                Ingress         IngOK
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 G.8032 ERPS Version 2 Commands

This chapter contains the G.8032 (2012) Ethernet Ring Protection Switching (ERPS) version 2 commands.

- g8032 physical-ring
- force-switch|manual-switch
- g8032 erp-instance
- g8032 profile
- level
- non-virtual-channel
- physical-ring
- profile name
- ring-id
- ring-type
- raps-channel-vlan
- data-traffic-vlan
- rpl role
- show g8032 erp-instance
- show g8032 physical-ring
- show g8032 profile
- switching-mode
- tcn-propogation
- tcn-propagation-instance
- timer
- virtual-channel

© 2021 IP Infusion Inc. Proprietary

g8032 physical-ring

Use this command to create a physical ring and associate east and west interfaces with it. All ERP instances on this ring have the same east and west interfaces,

Use the `no` form of this command to delete a physical ring.

Command Syntax

```
g8032 physical-ring RINGNAME bridge <1-32>
no g8032 physical-ring RINGNAME bridge <1-32>
```

Parameters

`bridge`	Bridge.
`<1-32>`	Bridge identifier.
`physical-ring`	Physical ring.
`RINGNAME`	Physical ring name (maximum 37 characters).
`IFNAME`	East interface name.
`IFNAME`	West interface name.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#g8032 physical-ring ERPS123 bridge 1
(config)#no g8032 physical-ring ERPS123 bridge 1
```


© 2021 IP Infusion Inc. Proprietary

force-switch|manual-switch

Use this command to configure administrative commands.

Command Syntax

```
(((force-switch|manual-switch)(east-interface|west-interface))|clear)
```

Parameters

`force-switch`	Forcefully block a ring port.
`manual-switch`	Manually block a ring port.
`east-interface`	Apply command to east interface.
`west-interface`	Apply command to west interface.
`clear`	Cancel a command.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#force-switch east-interface
```

g8032 erp-instance

Use this command to create an ERP instance and change to G.8032 configure switch mode.

Use the `no` form of this command to delete an ERP instance.

Command Syntax

```
g8032 erp-instance INSTANCENAME bridge (<1-32>)
no g8032 erp-instance INSTANCENAME bridge (<1-32>)
```

Parameters

`INSTANCENAME`	Instance name (maximum 32 characters).
`bridge`	Bridge.
`<1-32>`	Bridge identifier.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#g8032 erp-instance instance1 bridge 1
(g8032-config-switch)#
```


© 2021 IP Infusion Inc. Proprietary

g8032 profile

Use this command to create a profile on a bridge and switch to G.8032 profile configure mode.

Use the `no` form of this command delete a profile on a bridge.

Command Syntax

```
g8032 profile PROFILENAME bridge (<1-32>)
no g8032 profile PROFILENAME bridge (<1-32>)
```

Parameters

`PROFILENAME`	Profile name (maximum 32 characters).
`bridge`	Bridge.
`<1-32>`	Bridge identifier.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#g8032 profile profile123 bridge 1
(g8032-profile-config)#
```

level

Use this command to set the maintenance entity group (MEG) level (MEL) to carry in R-APS messages.

Command Syntax

```
level <0-7>
```

Parameters

<0-7>	Level.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#level 2
```


© 2021 IP Infusion Inc. Proprietary

non-virtual-channel

Use this command to make a sub-ring function without a virtual channel.

Use the `no` form of this command to delete a non-virtual channel.

Command Syntax

```
non-virtual-channel
no non-virtual-channel
```

Parameters

None

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#non-virtual-channel
```

physical-ring

Use this command to associate the ERP instance to a physical ring.

Command Syntax

```
physical-ring RINGNAME
```

Parameters

RINGNAME	Physical ring name.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#physical-ring ring1
```


© 2021 IP Infusion Inc. Proprietary

profile name

Use this command to associate the ERP instance to a profile.

Command Syntax

```
profile name PROFILENAME
```

Parameters

PROFILENAME	Profile name.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#profile prof_1
```

ring-id

Use this command to set the ring identifier.

Command Syntax

```
ring-id <1-239>
```

Parameters

<1-239>	Ring identifier.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#ring-id 1
```


© 2021 IP Infusion Inc. Proprietary

ring-type

Use this command to specify the type of the ethernet ring for this ERP instance.

Command Syntax

```
ring-type <major-ring/sub-ring>
```

Parameters

`<major-ring/sub-ring>` type of erps ring

Command Mode

G.8032 configure switch mode

Example

```
(g8032-config-switch)#ring-type major-ring
```

raps-channel-vlan

Use this command to configure APS channel VLAN-ID for this ERP instance

Command Syntax

```
raps-channel-vlan <2-4094>
no raps-channel-vlan
```

Parameters

<2-4094>	VLANID

Command Mode

G.8032 configure switch mode.

Examples

```
(g8032-config-switch)#raps-channel-vlan 10
```


© 2021 IP Infusion Inc. Proprietary

data-traffic-vlan

Use this command to configure VLANs as data channels.

Use the no forms of this command to remove the same.

Command Syntax

```
data-traffic-vlan VLAN_RANGE
no data-traffic-vlan VLAN_RANGE
```

Parameters

VLAN_RANGE	Enter VLAN ID 2-4094 or list of VLAN ID's separated by commas. Eg 2 or 2,4,5 or 50,51,52 etc...

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#data-traffic-vlan 201,202,203
```

rpl role

Use this command to set the RPL (Ring Protection Link) role of the ring node.

Command Syntax

```
rpl role ((owner | neighbor | next-neighbor)(east-interface | west-interface) |
  non-owner )
```

Parameters

`owner`	Ring node is the RPL owner.
`neighbor`	Ring node is neighbor to the RPL owner.
`next-neighbor`	Ring node is neighbor to the neighbor of the RPL owner.
`east-interface`	Role assigned to east interface.
`west-interface`	Role assigned to west interface.
`non-owner`	Ring node does not own the RPL.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#rpl role owner east-interface
```


© 2021 IP Infusion Inc. Proprietary

show g8032 erp-instance

Use this command to display details about an ERP instance.

Command Syntax

```
show g8032 erp-instance INSTANCENAME bridge (<1-32>)
```

Parameters

INSTANCENAME	Instance name.
bridge	Bridge.
<1-32>	Bridge identifier.

Command Mode

Configure mode

Example

```
(config)#show g8032 erp-instance instance1 bridge 1
Inst Name  : instance1
State      : G8032_ST_INIT
Phy Ring   : -
Role       : -
East Link  : -
West Link  : -
Attached   : -
Attached To: -
Virt Chan  : -
-------------------------------------------------------------

     Channel        |    Interface           |  Profile
 (LEVL, VID, RID)   | (east,ver), (west,ver) |
=========================================================
 (7, 4065, 135)     | (eth11,1),  (eth2,2)   | PROF1
=========================================================
Data Traffic: 1,2,3,10,12...
```

show g8032 physical-ring

Use this command to display details about a physical ring.

Command Syntax

```
show g8032 physical-ring RINGNAME bridge (<1-32>)
```

Parameters

RINGNAME	Ring name
bridge	Bridge
<1-32>	Bridge identifier

Command Mode

Configure mode

Examples

```
(config)#show g8032 physical-ring ring1 bridge1
Ring     : ring1
==========
Bridge   : 1
East     : eth1
West     : eth2
ERP Inst : inst1, inst2, inst3
```


© 2021 IP Infusion Inc. Proprietary

show g8032 profile

Use this command to display details about a profile.

Command Syntax

```
show g8032 profile PROFILENAME bridge (<1-32>)
```

Parameters

PROFILENAME	Profile name.
bridge	Bridge.
<1-32>	Bridge identifier.

Command Mode

Configure mode

Examples

```
(config)#show g8032 profile profile1 bridge 1
Profile : profile1
=========
 Wait-To-Restore : 5 mins
 Hold Off Timer  : 0 secs
 Guard Timer     : 500 ms
 Wait-To-Block   : 5500 ms
 Protection Type : Revertive
```

switching-mode

Use this command to set the revertive behavior of the ring node.

Command Syntax

```
switching-mode <non-revertive/revertive>
```

Parameters

`revertive`	revertive mode operation of a G.8032 ethernet ring
`non-revertive`	represents non-revertive mode operation of a G.8032 ethernet ring revertive

Command Mode

G.8032 profile configure mode

Examples

```
(g8032-profile-config)# switching-mode revertive
```


© 2021 IP Infusion Inc. Proprietary

tcn-propogation

Use this command to enable or disable TCN (topology change notification) propagation for an interconnected ring.

Command Syntax

```
tcn-propogation (enable|disable)
```

Parameters

`enable`	Enable TCN propagation.
`disable`	Disable TCN propagation.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#tcn-propogation enable
```

tcn-propagation-instance

Use this command to associate TCN instance (topology change notification) propagation for an interconnected ring when configured in non-virtual mode.

Command Syntax

```
tcn-to-instance <instance name>
```

Parameters

`<instance name>` Instance name.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#tcn-to-instance erp1
```


© 2021 IP Infusion Inc. Proprietary

timer

Use this command to set timers.

Command Syntax

```
timer (wait-to-restore (<1-12>|default) | hold-off (<0-10000>|default) | guard-
  timer (<10-2000>|default))
```

Parameters

`wait-to-restore`	Wait-to-restore timer used to verify that a signal failure is not intermittent.
`<1-12>`	Timer value in minutes.
`default`	Default value of timer <5>.
`hold-off`	Hold-off timer used to filter intermittent link faults.
`<0-10000>`	Timer value in a multiple of 100 milliseconds.
`default`	Default value of timer <0>.
`guard-timer`	Guard timer that blocks latent outdated messages from causing unnecessary state changes.
`<1-20000>`	Timer value in a multiple of 10 milliseconds.
`default`	Default value of timer <500> milliseconds.

Command Mode

G.8032 profile configure mode

Examples

```
(g8032-profile-config)#timer wait-to-restore 7
(g8032-profile-config)#timer hold-off 50
(g8032-profile-config)#timer guard-timer 30
```

virtual-channel

Use this command on a sub-ring to attach it to a major instance.

Use the `no` form of this command to delete a virtual channel.

Command Syntax

```
virtual-channel (<2-4094>|) attached-to-instance INSTANCENAME
no virtual-channel
```

Parameters

`<2-4094>`	VLAN identifier.
`INSTANCENAME`	Major instance name.

Command Mode

G.8032 configure switch mode

Examples

```
(g8032-config-switch)#virtual-channel 3 attached-to-instance inst1
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 Provider Bridging Commands

This chapter describes the Provider Bridging (PB) commands.

IEEE 802.1ad standardizes the architecture and bridged protocols to allow Ethernet frames with multiple VLAN tags. Packets through a provider network are doubly tagged with both an:

- Inner (C-VLAN) tag which is the customer network VLAN identifier
- Outer (S-VLAN) tag which is the service provider network VLAN identifier

- bridge protocol provider-mstp
- bridge protocol provider-rstp
- cvlan registration table
- cvlan svlan
- show cvlan registration table
- switchport customer-edge
- switchport customer-edge default-svlan
- switchport customer-edge hybrid
- switchport customer-edge trunk
- switchport customer-network vlan
- switchport customer-network vlan translation
- switchport ethertype
- switchport mode
- switchport mode ingress-filter
- switchport mode customer-edge
- switchport mode customer-edge hybrid acceptable-frame-type
- switchport provider-edge
- switchport provider-network vlan translation
- vlan type customer
- vlan type service
- vlan type

© 2021 IP Infusion Inc. Proprietary

bridge protocol provider-mstp

Use this command to create a provider multiple spanning-tree protocol (MSTP) bridge. MSTP bridges can have different spanning-tree topologies for different VLANs inside a region of similar MSTP bridges.

Using this command creates an instance of the spanning tree, and associates the VLANs specified with that instance. A bridge created by this command forms its own separate region.

The multiple spanning tree protocol, like the rapid spanning tree protocol, provides rapid reconfiguration features, while providing load-balancing capability.

Command Syntax

```
bridge <1-32> protocol provider-mstp (edge|)
```

Parameters

`<1-32>`	Bridge identifier.
`edge`	Configure as an edge bridge.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 2 protocol provider-mstp edge
```


© 2021 IP Infusion Inc. Proprietary

bridge protocol provider-rstp

Use this command to add an IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in interface mode.

Command Syntax

```
bridge <1-32> protocol provider-rstp (edge|)
```

Parameters

`<1-32>`	Bridge identifier.
`edge`	Configure as an edge bridge.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 2 protocol provider-rstp edge
```

cvlan registration table

Use this command to create a customer VLAN (CVLAN) registration table that maps between CVLANs and service provider VLANs (SVLANs).

Use the `no` parameter with this command to delete the CVLAN registration table.

Command Syntax

```
cvlan registration table WORD bridge <1-32>
no cvlan registration table WORD bridge <1-32>
```

Parameters

`WORD`	Name of the CVLAN registration table.
`<1-32>`	Specify a bridge ID.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#cvlan registration table customer1
(config-cvlan-registration)#
```


© 2021 IP Infusion Inc. Proprietary

cvlan svlan

Use this command to map one or more customer VLANs (C-VLANs) to a service provider VLAN (S-VLAN).

Use the `no` forms of this command to delete a mapping.

Command Syntax

```
cvlan VLAN_RANGE (cvlan VLAN_ID) svlan VLAN_ID ({untagged-pep|untagged-cep}|)({scos
  <0-7> | scfi <0-1> | ccos <0-7> | ccfi <0-1>}|)
no cvlan VLAN_RANGE
no svlan VLAN_ID
```

Parameters

`cvlan`	Configure C-VLAN Registration table entry
`VLAN_RANGE`	VLAN identifier <2-4094> or range such as 2-5,10 or 2-5,7-19
`VLAN_ID`	Translated CVID
`svlan`	Service Provider VLAN corresponding to the C-VLAN
`VLAN_ID`	VLAN identifier <2-4094> “Translated CVID”
`untagged-pep`	Provider edge port is untagged for this CVLAN
`untagged-cep`	Customer edge port is untagged for this CVLAN
`scos`	Class of Service in the Priority Code Point (PCP) field of the Service Provider Tag (STAG)
`<0-7>`	Class-of-service value
`scfi`	Canonical Format Indicator in the Drop Eligible Indicator (DEI) field of the STAG
`<0-1>`	Canonical Format Indicator value
`ccos`	Class of Service in the PCP field of the customer tag (CTAG)
`<0-7>`	Class-of-service value
`ccfi`	Canonical Format Indicator in the DEI field of the CTAG
`<0-1>`	Canonical Format Indicator value

Command Mode

CVLAN Registration mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.3.

Example

```
#configure terminal
(config-cvlan-registration)#cvlan 10 svlan 20 scos 1 scfi 1 ccos 0 ccfi 0
(config-cvlan-registration)#cvlan 11 svlan 21 untagged-pep untagged-cep scos 1
scfi 1 ccos 0 ccfi 0
(config-cvlan-registration)#cvlan 13 svlan 23 untagged-pep untagged-cep scfi 0
ccfi 1
(config-cvlan-registration)#cvlan 14 svlan 24 scos 0 ccos 1
(config-cvlan-registration)#no cvlan 10 svlan 20
```

```
(config-cvlan-registration)#cvlan 30 cvlan 32 svlan 40 scos 0 scfi 1 ccos 1
ccfi 0
(config-cvlan-registration)#cvlan 41 cvlan 43 svlan 41 scfi 1 ccfi 0
(config-cvlan-registration)#no cvlan 30 svlan 40
```


© 2021 IP Infusion Inc. Proprietary

show cvlan registration table

Use this command to display the CVLAN registration table.

Command Syntax

```
show cvlan registration table (WORD|bridge <1-32>|WORD bridge <1-32>|)
```

Parameters

WORD	CVLAN registration table name.
<1-32>	Bridge identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show cvlan registration table map1 bridge 1
Bridge    Table Name     Port List
====== ========== =========
1              map1           xe4, po2
CVLAN ID  T-CVLAN ID SVLAN ID CCOS SCOS  CCFI   SCFI
======== ========== ========  ====  ==== ===== ====
10        11         100       1    2     1      1
20         -         200
```

Table 3-214 explains the output fields.

Table 3-214: show cvlan registration table output

Entry	Description
Bridge	ID number of the bridge associated with the Customer VLAN (CVLAN).
Table Name	ID of the CVLAN registration table.
Port List	List of ports used by this CVLAN (including Link aggregaters).
CVLAN ID	ID number of the CVLAN.
SVLAN ID	ID number of the Service VLAN (SVLAN) associated with the CVLAN.
CCFI	Canonical Format Indicator in the DEI field of the CTAG.
SCFI	Canonical Format Indicator in the Drop Eligible Indicator (DEI) field of the STAG.

switchport customer-edge

Use this command to set the switching characteristics of the layer 2 interface and the default customer VLAN.

Use the `no` form of this command to remove a customer VLAN.

Command Syntax

```
switchport customer-edge (access|hybrid) vlan <2-4094>
no switchport customer-edge (access|hybrid) vlan
```

Parameters

`access`	Set the layer 2 interface as access.
`hybrid`	Set the layer 2 interface as hybrid.
`<2-4094>`	Set the default VID for the interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport customer-edge access vlan 3

(config)#interface eth0
(config-if)#no switchport customer-edge access vlan
```


© 2021 IP Infusion Inc. Proprietary

switchport customer-edge default-svlan

Use this command to set the switching characteristics of the layer 2 interface and the default service VLAN.

Use the `no` form of this command to remove the default service VLAN.

Command Syntax

```
switchport customer-edge (hybrid|trunk) default-svlan DEFAULT_SVLAN
no switchport customer-edge (hybrid|trunk) default-svlan
```

Parameters

`hybrid`	Set the layer 2 interface as hybrid.
`trunk`	Set the layer 2 interface as trunk.
`DEFAULT_SVLAN`	Set the default service VLAN identifier <2-4094>.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport customer-edge hybrid default-svlan 3

(config)#interface eth0
(config-if)#no switchport customer-edge hybrid default-svlan
```

switchport customer-edge hybrid

Use this command to set the switching characteristics of the Layer 2 customer-facing interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.

Command Syntax

```
switchport customer-edge hybrid allowed vlan add VLAN_ID egress-tagged
  (enable|disable)
switchport customer-edge hybrid allowed vlan remove VLAN_ID
switchport customer-edge hybrid allowed vlan all
switchport customer-edge hybrid allowed vlan none
```

Parameters

`add`	Add a VLAN to transmit and receive through the Layer 2 interface.
`VLAN_ID`	ID of the VLAN <2-4094>.
`egress-tagged`	Set the egress tagging for the outgoing frames.
`enable`	Enable egress tagging for outgoing frames.
`disable`	Disable egress tagging for outgoing frames.
`remove`	Remove a VLAN from the member set.
`VLAN_ID`	ID of the VLAN <2-4094>.
`all`	Allow all VLANs to transmit and receive through the Layer 2 interface.
`none`	Allow no VLANs to transmit and receive through the Layer 2 interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#switchport customer-edge hybrid allowed vlan add 2 egress-tagged
enable
```


© 2021 IP Infusion Inc. Proprietary

switchport customer-edge trunk

Use this command to set the Layer2 interface as trunk.

Command Syntax

```
switchport customer-edge trunk allowed vlan add VLAN_ID
switchport customer-edge trunk allowed vlan remove VLAN_ID
switchport customer-edge trunk allowed vlan all
switchport customer-edge trunk allowed vlan none
```

Parameters

`add`	Add a VLAN to the member set.
`VLAN_ID`	Specify a VLAN ID <2-4094>
`remove`	Remove a VLAN from the member set.
`all`	Allow all VLANs to transmit and receive through the Layer 2 interface.
`none`	Allow no VLANs to transmit and receive through the Layer 2 interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#switchport customer-edge trunk allowed vlan add 12
```

switchport customer-edge vlan registration

Use this command to configure the VLAN registration parameters.

Use the `no` parameter with this command to delete the mapping from the interface.

Command Syntax

```
switchport customer-edge vlan registration WORD
no switchport customer-edge vlan registration
```

Parameters

`WORD`	Name of the CVLAN registration table.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#switchport customer-edge vlan registration customer1
```


© 2021 IP Infusion Inc. Proprietary

switchport customer-network vlan

Use this command to set the Layer2 interface as a Customer Network which behaves as specified by the 802.1 AD standard.

Command Syntax

```
switchport customer-network vlan <2-4094>
no switchport customer-network vlan
```

Parameters

<2-4094>	Set the default VLAN ID for the interface.

Default

The default action is to tunnel.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport customer-network vlan 2
```

switchport customer-network vlan translation

Use this command to add a translation table entry for CVLAN and SVLAN on a customer network port.

Use the `no` option with this command to delete a translation table entry for CVLAN and SVLAN on a customer network port.

Command Syntax

```
switchport customer-network vlan translation (cvlan <2-4094>| ) svlan <2-4094>
  (cvlan <2-4094> | ) svlan <2-4094> ({scos <0-7> | scfi <0-1> | ccos <0-7> | ccfi
  <0-1>}|)
no switchport customer-network vlan translation (cvlan <2-4094>|) svlan <2-4094>
```

Parameters

`cvlan`	CVLAN to translate
`<2-4094>`	CVLAN identifier to translate
`svlan`	SVLAN to translate
`<2-4094>`	SVLAN identifier to translate
`cvlan`	Translated CVLAN
`<2-4094>`	Translated CVLAN identifier
`svlan`	Translated SVLAN
`<2-4094>`	Translated SVLAN identifier
`scos`	Class of Service in the Priority Code Point (PCP) field of the service provider tag (STAG)
`<0-7>`	Class-of-service value
`scfi`	Canonical Format Indicator in the Drop Eligible Indicator (DEI) field of the STAG
`<0-1>`	Canonical Format Indicator value
`ccos`	Class of Service in the PCP field of the customer tag (CTAG)
`<0-7>`	Class-of-service value
`ccfi`	Canonical Format Indicator in the DEI field of the CTAG
`<0-1>`	Canonical Format Indicator value

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode provider-network
(config-if)#switchport provider-network allowed vlan all
```


© 2021 IP Infusion Inc. Proprietary

```
(config-if)#switchport customer-network vlan translation cvlan 2 svlan 3 cvlan
4 svlan 5
```

switchport ethertype

Use this command to change the TPID for a port.

Use the `no` option with this command to unset the TPID to default value.

Command Syntax

```
switchport (customer-network|provider-network|dot1q) ethertype ETHERTYPE
no switchport (customer-network|provider-network|dot1q) ethertype
```

Parameters

`customer-network`	Set the switching characteristics of the Layer2 interface to Customer-network port.
`provider-network`	Set the switching characteristics of the Layer2 interface to Provider-network port>.
`ETHERTYPE`	Ethertype value (in 0xhhhh hexadecimal notation) for the outer SVLAN tag (0x8100, 0x88a8, 0x9100, or 0x9200).
`dot1q`	Set the switching characteristics of the Layer2 interface to dot1q.

Defaut

Default TPID value is 88a8.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not supported on Qumran platforms.

Example

```
#configure terminal
(config)#interface xe54/1
(config-if)#switchport provider-network ethertype 0x8100

(config-if)#no switchport provider-network ethertype
```


© 2021 IP Infusion Inc. Proprietary

switchport mode

Use this command to set the switching characteristics of the Layer 2 interface.

Command Syntax

```
switchport mode (provider-network|customer-edge|customer-network)
```

Parameters

`provider-network`
: Provider network.

`customer-network`
: Customer network.

`customer-edge`
: Customer edge.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode provider-network
```

switchport mode ingress-filter

Use this command to specify only tagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode (access|hybrid|trunk|provider-network|customer-network)
  ingress-filter (enable|disable)
```

Parameters

`access`	Access.
`hybrid`	Hybrid.
`trunk`	Trunk.
`provider-network`	Provider network.
`customer-network`	Customer network.
`ingress-filter`	Set the ingress filtering for the received frames.
`enable`	Enable ingress filtering
`disable`	Disable ingress filtering

Default

If you do not give this command, ingress filtering is off and all frame types are classified and accepted. Giving this command without the `ingress-filter` parameter causes this command to use the default values.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode provider-network ingress-filter enable
```


© 2021 IP Infusion Inc. Proprietary

switchport mode customer-edge

Use this command to set the switching characteristics of the Layer 2 customer facing interface and classify only untagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode customer-edge (access|hybrid|trunk)
switchport mode customer-edge (access|hybrid|trunk) ingress-filter (enable|disable)
```

Parameters

`access`	Set the layer 2 interface as access.
`hybrid`	Set the layer 2 interface as hybrid.
`trunk`	Set the layer 2 interface as trunk.
`ingress-filter`	Set the ingress filtering for the received frames.
`enable`	Enable ingress filtering
`disable`	Disable ingress filtering

Default

The result of not using this command is that ingress filtering is off, and that all frame types are classified and accepted. Using this command without the `ingress-filter` parameter causes this command to use the default values.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode customer-edge access ingress-filter enable
```

switchport mode customer-edge hybrid acceptable-frame-type

Use this command to set the layer 2 interface acceptable frames types. This processing occurs after VLAN classification.

Command Syntax

```
switchport mode customer-edge hybrid acceptable-frame-type (all|vlan-tagged)
```

Parameters

`all`	Set all frames can be received.
`vlan-tagged`	Set only VLAN-tagged frames can be received.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode customer-edge hybrid acceptable-frame-type vlan-
tagged
```


© 2021 IP Infusion Inc. Proprietary

switchport provider-edge

Use this command to set the switching characteristics of the Layer 2 logical provider edge port. By default, egress tagging is enabled for all VLANs on the provider edge ports.

Command Syntax

```
switchport provider-edge vlan VLANID untagged-vlan VLANID
switchport provider-edge vlan VLANID default-vlan VLANID
```

Parameters

`vlan`	VLAN ID Of the provider edge port <1-4094>.
`untagged-vlan`	VLAN ID that will be untagged on the provider side <1-4094>.
`default-vlan`	VLAN ID to which untagged packets will be classified <1-4094>.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport provider-edge vlan 122 default-vlan 12
```

switchport provider-network vlan translation

Use this command to add a translation table entry for CVLAN and SVLAN on a provider network port.

Use the `no` form of this command to delete a translation table entry for CVLAN and SVLAN on a provider network port.

Command Syntax

```
switchport provider-network vlan translation (cvlan <2-4094>| ) svlan <2-4094>
  (cvlan <2-4094> | ) svlan <2-4094> ({scos <0-7> | scfi <0-1> | ccos <0-7> | ccfi
  <0-1>}|)
no switchport (provider-network) vlan translation svlan VLAN_ID svlan VLAN_ID
no switchport (provider-network) vlan translation cvlan <1-4095> svlan <1-4095>
```

Parameters

`cvlan`	CVLAN to translate
`<2-4094>`	CVLAN identifier to translate
`svlan`	SVLAN to translate
`<2-4094>`	SVLAN identifier to translate
`cvlan`	Translated CVLAN
`<2-4094>`	Translated CVLAN identifier
`svlan`	Translated SVLAN
`<2-4094>`	Translated SVLAN identifier
`scos`	Class of Service in the Priority Code Point (PCP) field of the service provider tag (STAG)
`<0-7>`	Class-of-service value
`scfi`	Canonical Format Indicator in the Drop Eligible Indicator (DEI) field of the STAG
`<0-1>`	Canonical Format Indicator value
`ccos`	Class of Service in the PCP field of the customer tag (CTAG)
`<0-7>`	Class-of-service value
`ccfi`	Canonical Format Indicator in the DEI field of the CTAG
`<0-1>`	Canonical Format Indicator value

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
interface xe10
switchport
bridge-group 1
switchport mode provider-network
switchport provider-network allowed vlan all
```


© 2021 IP Infusion Inc. Proprietary

```
switchport provider-network vlan translation svlan 20 svlan 21
switchport provider-network vlan translation svlan 22 svlan 24
switchport provider-network vlan translation cvlan 10 svlan 21 cvlan 13 svlan
28
switchport provider-network vlan translation cvlan 11 svlan 22 svlan 27

interface xe11
switchport
bridge-group 1
switchport mode provider-network
switchport provider-network allowed vlan all
switchport provider-network vlan translation svlan 20 svlan 21 scfi 0  ccos 3

interface xe12
switchport
bridge-group 1
switchport mode provider-network
switchport provider-network allowed vlan all
switchport provider-network vlan translation svlan 20 cvlan 3 svlan 21 scos 6
scfi 0

interface xe13
switchport
bridge-group 1
switchport mode provider-network
switchport provider-network allowed vlan all
switchport provider-network vlan translation cvlan 2 svlan 20 cvlan 3 svlan 21
scfi 1  ccfi 0

interface xe14
switchport
bridge-group 1
switchport mode provider-network
switchport provider-network allowed vlan all
switchport provider-network vlan translation cvlan 2 svlan 20 svlan 21 scos 5
scfi 1  ccos 7  ccfi 0
```

vlan type customer

Use this command to configure VLANs of type customer, to enable or disable the state of the VLANs, and to configure the name for VLANs.

Use the `no` form of this command to remove the VLAN type.

Command Syntax

```
vlan <2-4094> type customer bridge <1-32>
vlan <2-4094> type customer bridge <1-32> state (enable|disable)
vlan <2-4094> type customer bridge <1-32> name WORD
no vlan <2-4094> type customer bridge <1-32>
```

Parameters

`<2-4094>`	The VID of the VLAN that will be enabled or disabled on the bridge <2-4094>.
`type`	Identifies the VLAN as a customer, service, or VLAN.
`customer`	Identifies the Customer VLAN
`bridge`	Indicates a Service VLAN <1-32>.
`name`	The ASCII name of the VLAN. Maximum length allowed is 16 characters.
`state`	Indicates the operational state of the VLAN.
`enable`	Sets VLAN into an enable state.
`disable`	Sets VLAN into a disable state.
`WORD`	ASCII name of the VLAN.

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#vlan database
(config-vlan)#vlan 12 type customer bridge 1 name new state enable
```


© 2021 IP Infusion Inc. Proprietary

vlan type service

Use this command to configure VLANs of type service, to enable or disable the state of the VLANs, and to configure the name for VLANs.

Use the `no` form of this command to remove the VLAN type.

Command Syntax

```
vlan <2-4094> type service (point-point|multipoint-multipoint|rooted-multipoint)
  bridge <1-32> state (enable|disable)
vlan <2-4094> type service (point-point|multipoint-multipoint|rooted-multipoint)
  bridge <1-32> name WORD (state (enable|disable)|)
vlan <2-4094> type service (point-point|multipoint-multipoint|rooted-multipoint)
  bridge <1-32>
no vlan <2-4094> type service bridge <1-32>
```

Parameters

`point-point`	Sets the VLAN connectivity mode to point-to-point
`multipoint-multipoint`	Sets the VLAN connectivity mode to multipoint-multipoint
`rooted-multipoint`	Sets the VLAN connectivity mode to rooted-multipoint
`state`	Indicates the operational state of the VLAN.
`enable`	Sets VLAN into an enable state.
`disable`	Sets VLAN into a disable state.
`bridge`	Indicates a Service VLAN <1-32>.
`WORD`	ASCII name of the VLAN.

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#vlan database
(config-vlan)#vlan 12 type service multipoint-multipoint bridge 23 state
enable
```

vlan type

This command allows you to create a single/range of VLAN's on provide/edge bridge.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE type customer bridge <1-32>
vlan VLAN_RANGE type customer bridge <1-32> name WORD
vlan VLAN_RANGE type customer bridge <1-32> state (enable | disable)
vlan VLAN_RANGE type service (point-point | multipoint-multipoint
  |rootedmultipoint) bridge <1-32>
vlan VLAN_RANGE type service (point-point | multipoint-multipoint
  |rootedmultipoint) bridge <1-32> name WORD
vlan VLAN_RANGE type service (point-point | multipoint-multipoint
  |rootedmultipoint) bridge <1-32> state (enable | disable)


no vlan VLAN_RANGE type customer bridge <1-32>
no vlan VLAN_RANGE type service bridge <1-32>
```

Parameters

`VLAN_RANGE`	VLAN identifier <2-4094> or range such as 2-5,10 or 2-5,7-19
`customer`	Identifies the Customer VLAN
`bridge`	Specify the bridge group ID in the range <1-32>.
`name`	The ASCII name of the VLAN. Maximum length allowed is 16 characters.
`point-point`	Sets the VLAN connectivity mode to point-to-point
`multipoint-multipoint`	Sets the VLAN connectivity mode to multipoint-multipoint
`rooted-multipoint`	Sets the VLAN connectivity mode to rooted-multipoint
`WORD`	ASCII name of the VLAN.
`state`	Indicates the operational state of the VLAN.
`enable`	Sets VLAN into an enable state.
`disable`	Sets VLAN into a disable state.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

© 2021 IP Infusion Inc. Proprietary

Examples

```
(config)vlan 2,4,5-6 customer bridge 2
(config)vlan 10-12 service type point-point bridge 3
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Link Layer Discovery Protocol v2 Commands

The commands in this chapter support:

- Link Layer Discovery Protocol (LLDP) version 2 as described in IEEE 802.1AB 2009
- LLDP-MED protocol extension as per ANSI/TIA-1057 April 2006.

Note: To enable LLDPv2, LLDP (previous version) should be disabled or vice versa.

- clear lldp counters
- lldp-agent
- debug lldp
- lldp run
- lldp tlv basic-mgmt
- lldp tlv med
- lldp tlv ieee-8021-org-specific
- lldp tlv ieee-8023-org-specific
- lldp tlv-select basic-mgmt
- lldp tlv-select ieee-8021-org-specific
- lldp tlv-select ieee-8023-org-specific
- set lldp agt-circuit-id
- set lldp chassis-id-tlv
- set lldp chassis locally-assigned
- set lldp disable
- set lldp enable
- set lldp locally-assigned
- set lldp management-address-tlv
- set lldp med-devtype
- set lldp msg-tx-hold
- set lldp port-id-tlv
- set lldp timer
- set lldp too-many-neighbors
- set lldp tx-fast-init
- set lldp tx-max-credit
- show debugging lldp
- show lldp neighbors
- show lldp interface
- snmp restart lldp

© 2021 IP Infusion Inc. Proprietary

clear lldp counters

Use this command to clear the LLDP statistics on all the interfaces.

Command Syntax

```
clear lldp counters
```

Parameters

`counters`	Reset the LLDP traffic counters to zero.

Command Mode

Exec Mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear lldp counters
```


© 2021 IP Infusion Inc. Proprietary

lldp-agent

Use this command to create an LLDP agent mode.

Note: This command is not supported in SVLAN, VLAN, and loopback interfaces.

Use the `no` parameter to remove configured lldp agent mode.

Command Syntax

```
lldp-agent (non-tpmr-bridge |customer-bridge| )
no lldp-agent (non-tpmr-bridge |customer-bridge| )
```

Parameters

`non-tpmr-bridge`

non-tpmr-bridge

`customer-bridge`

customer-bridge

Default

By default LLDP agent is disabled.

Command Mode

Interface Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent customer-bridge
(if-lldp-agent)#

(if-lldp-agent)#no lldp-agent customer-bridge
(if-lldp-agent)#exit
(config-if)#
```

debug lldp

Use this command to set the debugging functions for LLDP.

Use the no form of this command to turn off LLDP debugging functions

Command Syntax

```
debug lldp (event|ha|rx|tx|message)
no debug lldp (event|ha|rx|tx|message)
```

Parameters

`event`	Enable or disable event debugging
`ha`	Enable or disable high availability debugging
`rx`	Enable or disable RX debugging
`tx`	Enable or disable TX debugging
`message`	Enable or disable NSM message debugging

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug lldp event
#debug lldp message
```


© 2021 IP Infusion Inc. Proprietary

lldp run

Use this command to start the Link Layer Discovery Protocol (LLDP)

Use the no form of this command to stop LLDP

Command Syntax

```
lldp run
```

```
no lldp run
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#lldp run

(config)#no lldp run
```

lldp tlv basic-mgmt

Use this command to select and unselect basic management TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

Use the `no` parameter to remove the basic management TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name) (select|unselect)
no lldp tlv basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name)
```

Parameters

`management-address`	Management address TLV
`port-description`	Port description TLV
`system-capabilities`	System capabilities TLV
`system-description`	System Description TLV
`system-name`	System name TLV
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv basic-mgmt system-name select
(if-lldp-agent)#exit
```


© 2021 IP Infusion Inc. Proprietary

lldp tlv med

Use this command to select and unselect Media Endpoint Devices (MED) TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

LLDP MED TLVs determine the capabilities the connected device supports and the capabilities the device has enabled.

Use the `no` parameter to remove the MED TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv med (network-policy|location|inventory|media-capabilities|extended-power-via-mdi) (select|unselect)
```

```
no lldp tlv med (network-policy|location|inventory|media-capabilities|extended-power-via-mdi)
```

Parameters

`network-policy`	Network-policy TLV
`location`	Location TLV
`inventory`	Inventory TLV
`media-capabilities`	Media-capabilities TLV
`extended-power-via-mdi`	Extended-power-via-mdi TLV (when PoE is available)
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv med network-policy select
(if-lldp-agent)#exit
```

lldp tlv ieee-8021-org-specific

Use this command to select and unselect ieee-8021-org-specific TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

Use the `no` parameter to remove the ieee-8021-org-specific TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv ieee-8021-org-specific (link-agg|mgmt-vid|port-ptcl-vlanid|port-
  vlanid|ptcl-identity|vid-digest|vlan-name) (select|unselect)
no lldp tlv ieee-8021-org-specific {port-vlanid| port-ptcl-vlanid| vlan-name|ptcl-
  identity|vid-digest|mgmt-vid|link-agg}
```

Parameters

`link-agg`	Link-aggregation TLV
`mgmt-vid`	Management VLAN identifier TLV
`port-ptcl-vlanid`	Port protocol VLAN identifier TLV
`port-vlanid`	Port VLAN identifier TLV
`ptcl-identity`	Protocol-identifier TLV
`vid-digest`	VLAN identifier digest TLV
`vlan-name`	VLAN name TLV
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select
(if-lldp-agent)#exit
```


© 2021 IP Infusion Inc. Proprietary

lldp tlv ieee-8023-org-specific

Use this command to select and unselect ieee-8023-org-specific TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

Use the `no` parameter to remove the ieee-8023-org-specific TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
  (select|unselect)
no lldp tlv ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
```

Parameters

`mac-phy`	Provider edge port VLAN ID TLV
`power-via-mdi`	Power-via-MDI TLV (when PoE is available)
`max-mtu-size`	Maximum MTU size TLV
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select
(if-lldp-agent)#exit
```

lldp tlv-select basic-mgmt

Use this command to select basic management TLVs to be include in the LLDP frames.

Use the `no` parameter to disable basic management TLVs.

Command Syntax

```
lldp tlv-select basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name)
no lldp tlv-select basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name)
```

Parameters

`management-address`
: Management address specific TLV

`port-description`
: Port description specific TLV

`system-capabilities`
: System capabilities specific TLV

`system-description`
: System Description specific TLV

`system-name`
: System name specific TLV

Default Value

None

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select basic-mgmt system-name
```


© 2021 IP Infusion Inc. Proprietary

lldp tlv-select ieee-8021-org-specific

Use this command to select ieee-8021-org-specific TLVs to include in the LLDP frames.

Use the `no` parameter to disable ieee-8021-org-specific TLVs.

Command Syntax

```
lldp tlv-select ieee-8021-org-specific (link-agg|mgmt-vid|port-ptcl-vlanid|port-
  vlanid|ptcl-identity|vid-digest|vlan-name)
no lldp tlv-select ieee-8021-org-specific {port-vlanid| port-ptcl-vlanid| vlan-
  name|ptcl-identity| vid-digest|mgmt-vid|link-agg}
```

Parameters

`link-agg`	Link-aggregation TLV
`mgmt-vid`	Management VLAN identifier TLV
`port-ptcl-vlanid`	Port protocol VLAN identifier TLV
`port-vlanid`	Port VLAN identifier TLV
`ptcl-identity`	Protocol-identifier TLV
`vid-digest`	VLAN identifier digest TLV
`vlan-name`	VLAN name TLV

Default Value

None

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select ieee-8021-org-specific port-vlanid
```

lldp tlv-select ieee-8023-org-specific

Use this command to select ieee-8023-org-specific TLVs to be include in LLDP frames.

Use the `no` parameter to disable ieee-8023-org-specific TLVs.

Command Syntax

```
lldp tlv-select ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
no lldp tlv-select ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
```

Parameters

`mac-phy`	VLAN ID Of the provider edge port <2-4094>.
`power-via-mdi`	Power-via-MDI (only when PoE feature is available)
`max-mtu-size`	Maximum MTU size TLV

Default Value

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select ieee-8023-org-specific mac-phy
```


© 2021 IP Infusion Inc. Proprietary

set lldp agt-circuit-id

Use this command to configure LLDP agt-circuit-id.

Command Syntax

```
set lldp agt-circuit-id  VALUE
```

Parameters

VALUE	Specify LLDP global agt-circuit ID.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#set lldp agt-circuit-id sample
```

set lldp chassis-id-tlv

Use this command to set the chassis ID subtype for the LLDP agent on a port.

Use no form of this command to unset the chassis ID subtype.

Command Syntax

```
set lldp chassis-id-tlv (if-alias | ip-address | mac-address | if-name | locally-
  assigned)
no set lldp chassis-id-tlv
```

Parameters

`mac-address`	Use the MAC address as the chassis ID
`ip-address`	Use the management IP address as the chassis ID
`if-alias`	Use the IP address as the chassis ID
`if-name`	Use the interface name as the chassis ID
`locally-assigned`	Use the locally assigned value as the chassis ID

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp chassis-id-tlv ip-address
(if-lldp-agent)#no set lldp chassis-id-tlv
```


© 2021 IP Infusion Inc. Proprietary

set lldp chassis locally-assigned

Use this command to set the locally assigned chassis name for the LLDP interface.

Command Syntax

```
set lldp chassis locally-assigned NAME
```

Parameters

NAME	Name assigned to the chassis.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#set lldp chassis locally-assigned box1
```

set lldp disable

Use this command to disable the admin status of a LLDP agent on a port.

Command Syntax

```
set lldp disable
```

Parameters

None

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp disable
(if-lldp-agent)#exit
```


© 2021 IP Infusion Inc. Proprietary

set lldp enable

Use this command to set the admin status of a LLDP agent on a port.

Command Syntax

```
set lldp enable (txonly|txrx|rxonly)
```

Parameters

`rxonly`	Receive-only
`txonly`	Transmit-only
`txrx`	Transmit and receive

Default

By default, no LLDP agent is enabled for a port.

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp enable txrx
(if-lldp-agent)#exit
```

set lldp locally-assigned

Use this command to set the locally assigned name for LLDP interface.

Use no form of this command to remove the locally assigned name for LLDP interface.

Command Syntax

```
set lldp locally-assigned NAME
no set lldp locally-assigned NAME
```

Parameters

NAME	Name assigned to the port.

Command Mode

Interface Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp locally-assigned port1
(config-if)#no set lldp locally-assigned
```


© 2021 IP Infusion Inc. Proprietary

set lldp management-address-tlv

Use this command to set the sub type of the Management Address TLV.

Use `no` form of this command to unset the sub type of the Management Address TLV.

Command Syntax

```
set lldp management-address-tlv (mac-address | ip-address)
no set lldp management-address-tlv
```

Parameters

`mac-address`	Use the MAC address as the Management Address.
`ip-address`	Use the management IP address as the Management Address.

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp management-address-tlv ip-address
(if-lldp-agent)#no set lldp management-address-tlv
```

set lldp med-devtype

Use this command to configure the LLDP device type as Network-Connectivity/ End-Point Class1/ End-Point Class2/ End-Point Class3 device.

Use the `no` parameter to un set the configured LLDP device type.

Command Syntax

```
set lldp med-devtype (net-connect| ep-class1| ep-class2| ep-class3)
no lldp med-devtype (net-connect| ep-class1| ep-class2| ep-class3)
```

Parameters

`net-connect`	Set device type as Network-Connectivity
`ep-class1`	Set device type as End-Point Class1
`ep-class2`	Set device type as End-Point Class2
`ep-class3`	Set device type as End-Point Class3

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp med-devtype ep-class1
(config-if)#exit

#configure terminal
(config)#interface eth0
(config-if)#no set lldp med-devtype
(config-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

set lldp msg-tx-hold

Use this command to set the `msg-tx-hold` parameter that determines the Time To Live (TTL) value for LLDPDUs to be transmitted by the port. The value set with this command is multiplied by the `lldp timer msg-tx-interval` value, which determines the final TTL value.

Use `no` form of this command to set the default value of message transmit hold.

Command Syntax

```
set lldp msg-tx-hold <1-100>
no set lldp msg-tx-hold
```

Parameters

`<1-100>`	Time in seconds to set message transmit hold.

Default

The default value of message transmit hold is 4 seconds.

Command Mode

LLDP agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp msg-tx-hold 3
(if-lldp-agent)#no set lldp msg-tx-hold
```

set lldp port-id-tlv

Use this command to set the sub type of the Port ID.

Use `no` form of this command to unset the sub type of the Port ID.

Command Syntax

```
set lldp port-id-tlv (if-alias | ip-address | mac-address | if-name | agt-circuit-
  id | locally-assigned)
no set lldp port-id-tlv
```

Parameters

`mac-address`	Use the MAC address as the port-id-tlv.
`ip-address`	Use the management IP address as the port-id-tlv
`if-alias`	Use the IP alias as the port-id-tlv
`if-name`	Use the interface name as the port-id-tlv
`agt-circuit-id`	Use the agt-circuit-id name as the port-id-tlv
`locally-assigned`	Use the locally assigned value as the port-id-tlv

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp port-id-tlv ip-address
(if-lldp-agent)#no set lldp port-id-tlv
```


© 2021 IP Infusion Inc. Proprietary

set lldp timer

Use this command to set the interval at which LLDP frames are transmitted.

Use `no` form of this command to set the default value for timer.

Command Syntax

```
set lldp timer msg-fast-tx <1-3600>
set lldp timer msg-tx-interval <5-3600>
set lldp timer reinit-delay <1-10>
no set lldp timer msg-fast-tx
no set lldp timer msg-tx-interval
no set lldp timer reinit-Delay
```

Parameters

`msg-fast-tx`	Set the value in range <1-3600>
`msg-tx-interval`	Set the value in range <5-3600>
`reinit-delay`	Set the value in range <1-10>

Default Values

The default value for `msg-fast-tx` is 1 second.

The default value for `msg-tx-interval` is 30 seconds.

The default value for `reinit-delay` is 2 seconds.

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp timer msg-fast-tx 40
(if-lldp-agent)#no set lldp timer msg-fast-tx
(if-lldp-agent)#exit

#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp timer msg-tx-interval 40
(if-lldp-agent)#no set lldp timer msg-tx-interval
(if-lldp-agent)#exit
```

© 2021 IP Infusion Inc. Proprietary

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp timer reinitDelay 3
(if-lldp-agent)#no set lldp timer reinitDelay
(if-lldp-agent)#exit
```


© 2021 IP Infusion Inc. Proprietary

set lldp too-many-neighbors

Use this command to set the action to take when the remote table is full.

Use no form of this command to unset too many neighbors parameters.

Command Syntax

```
set lldp too-many-neighbors limit <1-65535> discard received-info timer <1-65535>
set lldp too-many-neighbors limit <1-65535> discard existing-info MAC timer <1-
  65535>
no set lldp too-many-neighbors limit
```

Parameters

`limit`	The limit on the number of LLDP neighbors.
`<1-65535>`	Upper limit for the number of Remote LLDP Information.
`received-info`	The information received for this neighbor.
`timer`	The period after which received information is discarded.
`<1-65535>`	The period in seconds after which received information is discarded.
`existing-info`	The information for this neighbor.
`MAC`	Identifies the remote LLDP Agent for which information is discarded.
`timer`	The period in seconds after which existing information is discarded.
`<1-65535>`	The period in seconds after which existing information is discarded.

Default Value

No upper limit is enforced for the number of remote LLDP agents.

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#lldp-agent
(if-lldp-agent)#set lldp too-many-neighbors limit 20 disc existing-info
1001.1001.1001 timer 1

(config)#interface eth1
(config-if)#lldp-agent
(if-lldp-agent)#set lldp too-many-neighbors limit 1 discard received-info
timer 1
```

set lldp tx-fast-init

Use this command to determine the maximum value of LLDP frames that are transmitted during a fast transmission period.

Use `no` form of this command to set fast transmission period to default value.

Command Syntax

```
set lldp tx-fast-init <1-8>
no set lldp tx-fast-init
```

Parameters

`tx-fast-init`	Set the message transmit interval value <1-8>.

Default Value

Default value is 4.

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp tx-fast-init 4
(if-lldp-agent)#no set lldp tx-fast-init
(if-lldp-agent)#exit
```


© 2021 IP Infusion Inc. Proprietary

set lldp tx-max-credit

Use this command to set the maximum value of transmission credit, which signifies the number of consecutive LLDP frames transmitted.

Use `no` form of this command to set the maximum value of transmission credit to default value.

Command Syntax

```
set lldp tx-max-credit <1-10>
no set lldp tx-max-credit
```

Parameters

`tx-max-credit`	The maximum value of transmission credit.

Default Value

Default value is 5

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#set lldp tx-max-credit <1-10>
(if-lldp-agent)#no set lldp tx-max-credit
(if-lldp-agent)#exit
```

show debugging lldp

Use this command to display LLDP debugging information.

Command Syntax

```
show debugging lldp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following sample output displays information about an LLDP debugging.

```
#show debugging lldp
LLDP debugging status:
 LLDP message debugging is on
```


© 2021 IP Infusion Inc. Proprietary

show lldp neighbors

Use this command to display LLDP neighbors information.

Command Syntax

```
show lldp (nearest-bridge| non-tpmr-bridge| customer-bridge|) neighbors
  (brief|details)
```

Parameters

`nearest-bridge`	Display LLDP nearest bridge information
`non-tpmr-bridge`	Display LLDP non-TPMR-bridge information
`customer-bridge`	Display LLDP customer-bridge information
`neighbor`	Neighbor
`brief`	Brief
`details`	Details

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.1.

Example

The following sample output displays information about an LLDP neighbors

```
#sh lldp nearest-bridgr neighbors brief
Loc PortID  Rem Host Name   Rem Chassis Id  Rem Port Id   Agent Mode

-------------------------------------------------------------------------------
xe3/1        OcNOS       ecf4.bbfe.2864  ecf4.bbb2.4c65 Nearest bridge


#show lldp neighbors detail

-------------------------------------------------------------------------------
Nearest bridge Neighbors
 Interface Name : xe11
 Mandatory TLVs
 Chassis id type : MAC address [8cea.1b67.236c]
 Port id type : MAC address [8cea.1b28.4f6d]
 Time to live : 121
 Basic Management TLVs
 System Name : OcNOS
 System Description : Hardware Model:EC_AS5912-54X, Software version: OcNOS,1.3.1.122
 Port Description : xe11
 Remote System Capabilities : Bridge Router
 Capabilities Enabled : Router
```

```
Management Address : MAC Address [8cea.1b67.236c]
Interface Number subtype : ifindex
Interface Number : 10011
OID Number : 0
802.1 Org specific TLVs
Port vlan id : 0
Port & Protocol vlan id : 0
Remote Configured VLANs : None
Remote Protocols Advertised: None
Remote VID Usage Digest : 0
Remote Management Vlan : 0
Link Aggregation Capability: capable of being aggregated
Link Aggregation Status : not currently in aggregation
Link Aggregation Port ID :
802.3 Org specific TLVs
AutoNego Support : Supported
AutoNego Status : Disabled
AutoNego Capability : 16
Operational MAU Type : 54 [Four-pair Category 6A or better, full duplex mode only]
Max Frame Size : 1518
```

Table 1-216 Shows the output details.

Table 1-215: show lldp neighbor output details

Entry	Description
Loc Port ID	Local interface SNMP index (appears when the interface option is used).
Rem Host Name	Name of the remote host.
Rem Chassis Id	Remote chassis identifier of the chassis type listed.
Rem Port Id	Remote port identifier of the port type listed.
Agent Mode	Agent mode enabled to the nearest bridge.
Time to live	Number of seconds for which this information is valid.
Interface Name	Name of the interface.
Chassis id type	Chassis identifier of the chassis type listed.
Port id type	Type of port identifier supplied, such as Locally assigned.
System Name	Name supplied by the system on the interface.
System Description	Description supplied by the system on the interface.
Port Description	The port description field uses the configured port description, the port name or the SNMP if Index (appears when the interface option is used).
Remote System Capabilities	Remote system capabilities (such as Bridge, Bridge Router, and Bridge Telephone) that are supported.

© 2021 IP Infusion Inc. Proprietary

Table 1-215: show lldp neighbor output details

Entry	Description
Capabilities Enabled	Enabled by the system on the interface (appears when the interface option is used).
Management Address	Details of management address (such as 10.204.35.34).
Interface Number subtype	Interfaces subtype for which neighbor information is available.
Interface Number	Interfaces for which neighbor information is available.
OID Number	Number of identifier.
Port VLAN ID	Details of the port VLAN identifier.
Protocol VLAN ID	Details of the protocol VLAN identifier.
Remote Configured VLANs	Details of the remote configured VLAN.
Remote Protocols Advertised	Details of the remote protocols.
Remote VID usage Digest	Details of the VID usage.
Remote Management VLAN	Details of the management VLAN.
Link Aggregation Capability	Capabilities that supported by the link aggregation on the interface.
Link Aggregation Status	Status of the link aggregation.
Link Aggregation Port ID	Details of the link aggregation port identifier.
Auto Nego Support	Support of the auto nego on the interface.
Auto Nego Status	Status of the auto nego.
Auto Nego Capability	Capabilities that supported by the auto nego on the interface.
Operational MAU Type	Type of operational MAU on the interface.
Max Frame Size	Maximum frame size on the transit.

© 2021 IP Infusion Inc. Proprietary

show lldp interface

Use this command to display LLDP interface information.

Command Syntax

```
show lldp interface IFNAME (nearest-bridge| non-tpmr-bridge| customer-bridge | )
  (neighbor| )
```

Parameters

`IFNAME`

Display LLDP interface information for all agent

`nearest-bridge`

Display LLDP nearest bridge information

`non-TPMR-bridge`

Display LLDP non-TPMR-bridge information

`customer-bridge`

Display LLDP customer-bridge information

`neighbor`

Display LLDP neighbor details.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lldp interface eth0
Agent Mode : Customer-bridge
Enable (tx/rx): N/N
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 0
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0

Agent Mode : Non-TPMR-bridge
Enable (tx/rx): N/N
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 0
```

 © 2021 IP Infusion Inc. Proprietary

```
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0

Agent Mode : Nearest bridge
Enable (tx/rx): Y/Y
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 2495
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0
```

Table 1-216 Shows the output details.

Table 1-216: show lldp interface output details

Entry	Description
Agent Mode	Agent mode enabled to the customer-bridge, Non-TPMR-bridge, and nearest bridge.
Enable (tx/rx)	Enables the transmit and receive on the interface.
Device Type	Type of device in the networks.
LLDP Agent traffic statistics	Statistics on exchanged LLDP frames between a device and neighbors.
Total frames transmitted	Number of frames transmitted in network.
Total entries aged	Number of aged entries in a networks.
Total frames received	Number of frames received from the neighbor network.
Total frames received in error	Number of frames not received from the neighbor network.
Total discarded TLVs	Number of TLVs discarded in transit.
Total unrecognised TLVs	Number of unrecognised TLVs in transit.

snmp restart lldp

Use this command to restart SNMP in Link Layer Discovery Protocol (LLDP)

Command Syntax

```
snmp restart lldp
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#snmp restart lldp
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Link Layer Discovery Protocol Commands

This chapter describes the Link Layer Discovery Protocol (LLDP) commands.

- lldp debug
- lldp disable default-agent
- lldp ip
- lldp tlv
- set lldp chassis-id-tlv
- set lldp disable
- set lldp enable
- set lldp locally-assigned
- set lldp management-address-tlv
- set lldp msg-tx-hold
- set lldp system-description
- set lldp system-name
- set lldp timer
- set lldp too-many-neighbors
- show lldp
- snmp restart lldp

© 2021 IP Infusion Inc. Proprietary

lldp debug

Use this command to set the debugging functions for LLDP.

Use the no form of this command to turn off LLDP debugging functions

Command Syntax

```
lldp debug (event|rx|tx|message)
no lldp debug (event|rx|tx|message)
```

Parameters

`event`	Enable or disable event debugging
`message`	Enable or disable NSM message debugging
`rx`	Enable or disable RX debugging
`tx`	Enable or disable TX debugging

Command Mode

Exec mode and Privileged Exec mode

Examples

```
#lldp debug event
#lldp debug messages
```


© 2021 IP Infusion Inc. Proprietary

lldp disable default-agent

Use this command to exclude interface when LLDP enabled globally

Command Syntax

```
lldp (disable|enable) default-agent
```

Parameters

`disable`	Disables default LLDP agent
`enable`	Enables default LLDP agent

Command Mode

Interface mode

Applicability

This command is introduced from OcNOS version 5.0

Example

```
#configure terminal
(config)#interface xe1
(config-if)#lldp disable default-agent
(config-if)#lldp enable default-agent
```

lldp ip

Use this command to set the Link Layer Discovery Protocol with an IP address to be used as a chassis and management ID.

Use the `no` form of this command to remove this value.

Command Syntax

```
lldp ip address A.B.C.D
no lldp ip address
```

Parameters

`A.B.C.D`	Enter the IP address value

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#lldp ip address 1.1.1.1
(config)#no lldp ip address
```


© 2021 IP Infusion Inc. Proprietary

lldp tlv

Use this command to set the TLVs enabled for transmission on a port. Make sure that the complete set of Type Length Values (TLVs) is specified when giving this command, because TLVs not specified are disabled.

Command Syntax

```
lldp tlv {chassis-id|port-id|ttl|port-description|system-name|system-
  description|system-capabilities|management-address|ieee-8021-org-specific|ieee-
  8023-org-specific}
```

Parameters

`chassis-id`	Chassis ID type length values (TLV)
`port-id`	Port ID TLV
`ttl`	Time to live TLV
`port-description`	Port description TLV
`system-name`	System name TLV
`system-description`	System Description
`system-capabilities`	System capabilities TLV
`management-address`	Management address TLV
`ieee-8021-org-specific`	IEEE 802.1 organizationally-specific TLV
`ieee-8023-org-specific`	IEEE 802.3 organizationally-specific TLV

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#lldp tlv chassis-id ieee-8021-org-specific ieee-8023-org-specific
management-address port-description port-id system-capabilities system-
description system-name ttl
```

set lldp chassis-id-tlv

Use this command to set the chassis ID subtype for the LLDP agent on a port.

Command Syntax

```
set lldp chassis-id-tlv (mac-address | ip-address)
```

Parameters

`mac-address`	Use the MAC address as the chassis ID
`ip-address`	Use the management IP address as the chassis ID

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp chassis-id-tlv ip-address
```


© 2021 IP Infusion Inc. Proprietary

set lldp disable

Use this command to disable the LLDP agent on a port.

Command Syntax

```
set lldp disable
```

Parameters

None

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp disable
```

set lldp enable

Use this command to enables an LLDP agent on a port and specifies its type.

Command Syntax

```
set lldp enable (txonly|txrx|rxonly)
```

Parameters

`rxonly`	Receive-only
`txonly`	Transmit-only
`txrx`	Transmit and receive

Default

By default, no LLDP agent is enabled for a port.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp enable txrx
```


© 2021 IP Infusion Inc. Proprietary

set lldp locally-assigned

Use this command to locally assign the LLDP Port ID and the Chassis ID TLV parameters.

Command Syntax

```
set lldp locally-assigned NAME
```

Parameters

NAME	Name assigned to the port.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp locally-assigned port1
```

set lldp management-address-tlv

Use this command to set the management address subtype for the LLDP agent on a port.

Command Syntax

```
set lldp management-address-tlv (mac-address | ip-address)
```

Parameters

`mac-address`	Use the MAC address as the chassis ID
`ip-address`	Use the management IP address as the chassis ID

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp management-address-tlv ip-address
```


© 2021 IP Infusion Inc. Proprietary

set lldp msg-tx-hold

Use this command to set the `msg-tx-hold` parameter that determines the Time To Live (TTL) value for LLDPDUs to be transmitted by the port. The value set with this command is multiplied by the `lldp timer msg-tx-interval` value, which determines the final TTL value.

Command Syntax

```
set lldp msg-tx-hold VALUE
```

Parameters

`VALUE`	Time in seconds of LLDP msg-tx-hold

Default

The default value of the `lldp msg-tx-hold` parameter is 4 seconds.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config)#set lldp msg-tx-hold 3
```

set lldp system-description

Use this command to identify the string that describes the LLDP system.

Command Syntax

```
set lldp system-description LINE
```

Parameters

LINE	Set the description of the LLDP system.

Default

The default status of Ethernet OAM is disabled.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#set lldp system-description LLDP agent on B1
```


© 2021 IP Infusion Inc. Proprietary

set lldp system-name

Use this command to identify the system name of the LLDP function.

Command Syntax

```
set lldp system-name NAME
```

Parameters

NAME	Name of the LLDP system.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#set lldp system-name LLDP1
```

set lldp timer

Use this command to set the interval at which LLDP frames are transmitted.

Command Syntax

```
set lldp timer msg-tx-interval <5-32768>
set lldp timer reinitDelay VALUE
set lldp timer tx-delay <1-8192>
```

Parameters

`msg-tx-interval`	
	Set the message transmit interval value
`<5-32768>`	Set the message transmit interval value
`reinitDelay`	Set the reinit delay value
`VALUE`	Set the reinit delay value
`tx-delay`	Set the transmit delay value
`<1-8192>`	Set the transmit delay value in range of:
	(1 <= `tx-delay` <= ((0.25)* `msg-tx-interval`)

Default Values

The default value for `msg-tx-interval` is 30 seconds.

The default value for `reinitDelay` is 2 seconds.

The default value of the `tx-delay` is 2 seconds.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp timer msg-tx-interval 40

#configure terminal
(config)#interface eth0
(config-if)#set lldp timer reinitDelay 3

#configure terminal
(config)#interface eth0
(config-if)#set lldp timer tx-delay 3
```


© 2021 IP Infusion Inc. Proprietary

set lldp too-many-neighbors

Use this command to set the action to take when the remote table is full.

Command Syntax

```
set lldp too-many-neighbors limit <1-65535> discard received-info timer <1-65535>
set lldp too-many-neighbors limit <1-65535> discard existing-info MAC
  timer <1-65535>
```

Parameters

`limit`	The limit on the number of LLDP neighbors.
`<1-65535>`	The limit on the number of LLDP neighbors.
`received-info`	The information received for this neighbor.
`timer`	The period after which received information is discarded.
`<1-65535>`	The period in seconds after which received information is discarded.
`existing-info`	The information for this neighbor.
`MAC`	Identifies the remote LLDP Agent for which information is discarded.
`timer`	The period in seconds after which existing information is discarded.
`<1-65535>`	The period in seconds after which existing information is discarded.

Default Value

No upper limit is enforced for the number of remote LLDP agents.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#set lldp too-many-neighbors limit 20 disc existing-info 1.1.1.1.1
timer 1

(config)#interface eth1
(config-if)#set lldp too-many-neighbors limit 1 discard received-info timer 1
```

show lldp

Use this command to display LLDP port information.

Command Syntax

```
show lldp port IFNAME
show lldp port IFNAME statistics
```

Parameters

IFNAME	The name of the interface
statistics	Display LLDP port statistics

Command Mode

Exec mode and Privileged Exec mode

Example

The following sample output from this command displays detailed information about an LLDP-enabled port.

```
#show lldp port eth0
Remote LLDP
MAC Address: 01:06:29:CF:79:A1
TTL: 60
Network Address: 192.168.1.0
Interface Name: eth1
Interface Locally Assigned String: Port-a
Interface Description: bridge
Interface Number: 2
Port Vlan ID: 1
Protocol ID: 274242030202
AutoNego Support: Supported
AutoNego Capability: 1
Operational MAU Type: 3
Link Aggregation Status: Capable
Link Aggregation Port ID: 0
Max Frame Size: 128
System name:
System Description: bridge
System Capabilities: 4
System Capabilities Enabled: 4
```

The following sample output from this command displays all LLDP statistics for a selected port.

```
#show lldp port eth0 statistics
LLDP Port statistics for eth0
Frames transmitted: 22
Frames Aged out: 0
Frames Discarded: 0
Frames with Error: 0
Frames Received: 5
TLVs discarded: 0
TLVs unrecognized 0
```


© 2021 IP Infusion Inc. Proprietary

snmp restart lldp

Use this command to restart SNMP in Link Layer Discovery Protocol (LLDP)

Command Syntax

```
snmp restart lldp
```

Parameters

None

Command Mode

Configure mode

Examples

```
#snmp restart lldp
```

© 2021 IP Infusion Inc. Proprietary

SECTION 9

Data Center Bridging

Data Center Bridging Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *Enhanced Transmission Selection Configuration*
- Chapter 2, *Priority-based Flow Control Configuration*
- Chapter 3, *Quantized Congestion Notification Configuration*
- Chapter 4, *DCBx Configuration*

Note: Trident-2 and Trident-2+ platforms support all DCB features (PFC, QCN, ETS, DCBx for ETS and PFC parameter exchange).

Trident-3 platforms support only the following DCB features: PFC and DCBx only for PFC parameter exchange.

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Enhanced Transmission Selection Configuration

This chapter shows how to:

- Enable ETS on a bridge and interface
- Configure priorities and bandwidth for ETS

Topology



Figure 1-28: ETS-Enabled Bridge

Configuring a Bridge and Interface for ETS

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enables DCB on the bridge
`(config)#enhanced-transmission-selection enable bridge 1`	Enables ETS on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-org-specific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#enhanced-transmission-selection mode on`	Start sending DCBX TLVs in LLDP messages

Configuring Priorities and Bandwidth for ETS

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge

(config)#data-center-bridging enable bridge 1	Enables DCB on the bridge
(config)#enhanced-transmission-selection enable bridge 1	Enables ETS on the bridge
(config)#interface eth1	Configure interface eth1
(config-if)#switchport	Configure eth1 as a layer 2 port
(config-if)#bridge-group 1	Configure eth1 in bridge group 1
(config-if)#lldp-agent	Enter into LLDP agent mode.
(lldp-agent)#set lldp enable txrx	Configure LLDP for transmit and receive mode on eth1
(lldp-agent)#lldp tlv-select ieee-8021-org-specific	Configure LLDP to send an IEEE 802.1 organizationally specific TLV
(lldp-agent)#exit	Exit from LLDP mode.
(config-if)#enhanced-transmission-selection mode on	Configure the advertise flag and start sending DCBX TLVs in LLDP messages
(config-if)#traffic-class-group 1 add priority 0 1 2	Configure TCG 1 and add priorities 0, 1, and 2
(config-if)#traffic-class-group 0 add priority 3 4 5	Configure TCG 0 and add priorities 3, 4, and 5
(config-if)#bandwidth-percentage 0 40 1 60	Configure bandwidth percentages for TCG 1 and 1

Validation

Verify the ETS parameters configuration on the port specified.

```
#show enhanced-transmission-selection interface eth1
Interface : eth1
Enhanced Transmission Selection : on

Admin Configuration

Mode  Advertise Willing   Max-TCG  TCG-ID  BW%   Priorities
================================================================================
On    On        Off       0        0       40     3 4 5
On    On        Off       0        1       60     0 1 2
On    On        Off       0        15      NA     6 7

Operational Configuration
Oper  Max_TCG TCG-ID  BW%   Priorities
State
================================================================================
On    0       0       40     3 4 5
On    0       1       60     0 1 2
On    0       15      NA     6 7
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Priority-based Flow Control Configuration

This chapter shows how to:

- Enable PFC on a bridge and interface
- Configure priorities and link delay allowance for PFC
- Configuring application priority for PFC

Topology



Figure 2-29: PFC Enabled Bridge

Configuring a Bridge and Interface for PFC

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enables DCB on the bridge
`(config)#priority-flow-control enable bridge 1`	Enables PFC on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-org-specific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#priority-flow-control mode on`	Configure the advertise flag and start sending DCBX TLVs in LLDP messages

Configuring Priorities and Link Delay Allowance for PFC

`#configure terminal`	Enter Configure Mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge

`(config)#data-center-bridging enable bridge 1`	Enables DCB on the bridge
`(config)#priority-flow-control enable bridge 1`	Enables PFC on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-org-specific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#priority-flow-control mode on`	Configure the advertise flag and start sending DCBX TLVs in LLDP messages
`(config-if)#priority-flow-control cap 4`	Configure the maximum number of PFC priorities
`(config-if)#priority-flow-control enable priority 2 4 5`	Enable PFC on priorities 2, 4, and 5
`(config-if)#priority-flow-control link-delay-allowance 34567`	Configure the link delay allowance

Validation

1. Verify the default data set.

```
#sh priority-flow-control statistics bridge 1
bridge : 1
interface pri pause sent     pause received
=========================================
eth1     0  00              00
eth1     1  00              00
eth1     2  00              00
eth1     3  00              00
eth1     4  00              00
eth1     5  00              00
eth1     6  00              00
eth1     7  00              00

#sh priority-flow-control details bridge 1

Admin Configuration
interface mode advertise willing  cap   link delay     priorities allowance
=============================================================================

eth1       on    on       off      4      34567             2 4 5

Operational Configuration
-------------------------
interface state cap   link delay  priorities allowance
=============================================
eth1     on    4       34567          2 4 5
```


© 2021 IP Infusion Inc. Proprietary

Configuring Application Priority for PFC

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge.
`(config)#data-center-bridging enable bridge 1`	Enables DCB on the bridge
`(config)#application-priority enable bridge 1`	Enables application priority on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-org-specific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#application-priority enable`	Configure the advertise flag and start sending DCBX TLVs in LLDP messages
`(config-if)#tcp port-no 23 priority 6`	Enable priority for protocol using port number
`(config-if)#tcp service-name telnet priority 6`	Enable priority for protocol using TCP service-name

Validation

1. Verify the default data set.

```
#show application-priority interface eth1
bridge : 1
Application Priority : On

Admin Configuration
intf  Admin Config    Protocol    ProtoId   Priorities
      Mode  Advertise
================================================================================
eth1 On    On        tcp         telnet     6
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 Quantized Congestion Notification Configuration

This chapter shows how to:

- Enable QCN on a bridge and interface
- Enable a Congestion Notification Priority Value (CNPV) and create a Congestion Point (CP)

Topology



Figure 3-30: PFC-Enabled Bridge

Configuring a Bridge and Interface for QCN

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enable DCB on the bridge
`(config)#qcn enable bridge 1`	Enable QCN on the bridge
`(config-qcn)#exit`	Exit QCN mode
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-org-specific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV
`(lldp-agent)#exit`	Exit from LLDP mode.

Validation

```
#show qcn configuration bridge 1

 QCN:   Enable
 CNM Transmit Priority: 6
 Discarded Frames: 0
 Errored Port List: NONE
 Priority       CNPV
 ========       ====
```

```
0               No
1               No
2               No
3               No
4               No
5               No
6               No
7               No

CNPV details:

CNPV  DefModeChoice  AltPriority  DefenseMode
====  =============  ===========  ==============

CNPV details per interface:
Interface       CNPV  DefModeChoice  AltPriority  DefenseMode     XmitReady
==============  ====  =============  ===========  ==============  =========

Congestion Point Details:
Interface       CpId      W     SampleBase  MinHdrOctet  Qsp
==============  ========  ====  ==========  ===========  ===
```

Enable a CNPV and Create a CP

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an ieee vlan enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enables DCB on the bridge
`(config)#qcn enable bridge 1`	Enables QCN on the bridge
`(config-qcn)#cnpv 5`	Set the CNPV value on the QCN enabled bridge
`(config-qcn)#exit`	Exit QCN mode
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 asa layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-org-specific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#cp enable cnpv 5 sample-base 10000 weight 2`	Configure the congestion point

Validation

1. Verify the QCN configuration on the bridge.

   ```
   #show qcn configuration bridge 1
   ```


© 2021 IP Infusion Inc. Proprietary

```
QCN:   Enable
CNM Transmit Priority: 6
Discarded Frames: 0
Errored Port List: NONE

Priority       CNPV
========       ====
0              No
1              No
2              No
3              No
4              No
5              Yes
6              No
7              No

CNPV details:

CNPV  DefModeChoice  AltPriority  DefenseMode
====  =============  ===========  ==============
5     AUTO           0            EDGE

CNPV details per interface:
Interface       CNPV  DefModeChoice  AltPriority  DefenseMode     XmitReady
==============  ====  =============  ===========  ==============  =========
eth1            5     COMP           0            EDGE            FALSE
Congestion Point Details:
Interface            CpId        W     SampleBase  MinHdrOctet  Qsp
==============     ========     ====  ==========  ===========  =====
eth1          00ecf4bb530b0005   2      10000           0        31200
```

2. Verify the CNPV value on the QCN enabled bridge.

```
#show qcn cnpv bridge 1

Priority       CNPV
========       ====
0              No
1              No
2              No
3              No
4              No
5              Yes
6              No
7              No

CNPV details:

CNPV  DefModeChoice  AltPriority  DefenseMode
====  =============  ===========  ==============
5     AUTO           0            EDGE

CNPV details per interface:
Interface       CNPV  DefModeChoice  AltPriority  DefenseMode     XmitReady
==============  ====  =============  ===========  ==============  =========
eth1            5     COMP           0            EDGE            FALSE
```

3. Verify the CP on the QCN bridge.

```
# sh qcn cp interface eth1

Congestion Point Details:
 Interface       CpId              W     SampleBase  MinHdrOctet  Qsp
 ==============  ================  ====  ==========  ===========  ======
eth1             00ecf4bb530b0005  2     10000       0            31200
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 DCBx Configuration

This chapter show how to:

- Configure ETS parameter exchange
- Configure PFC parameter exchange

Topology



Figure 4-31: DCBx Configuration

Configuring ETS Parameter Exchange

SW1

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge.
`(config)#data-center-bridging enable bridge 1`	Enable DCB on the bridge
`(config)#enhanced-transmission-selection enable bridge 1`	Enable ETS on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-org-specific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#enhanced-transmission-selection mode on`	Configure the advertise flag and start sending DCBx TLVs in LLDP messages
`(config-if)#traffic-class-group 0 add priority 0 1 2`	Configure TCG 0 and add priorities 0, 1, and 2
`(config-if)#traffic-class-group 1 add priority 3 4 5`	Configure TCG 1 and add priorities 3, 4, and 5
`(config-if)#bandwidth-percentage 0 40 1 60`	Configure the bandwidth percentage for TCG 0and 1

© 2021 IP Infusion Inc. Proprietary

SW2

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge.
`(config)#data-center-bridging enable bridge 1`	Enable DCB on the bridge
`(config)#enhanced-transmission-selection enable bridge 1`	Enable ETS on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-org-specific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#enhanced-transmission-selection mode on`	Configure the advertise flag and start sending DCBx TLVs in LLDP messages
`(config-if)#traffic-class-group 0 add priority 0 1 2`	Configure TCG 0 and add priorities 0, 1 and 2
`(config-if)# traffic-class-group 1 add priority 3 4 5`	Configure TCG 1 and add priorities 3, 4, and 5
`(config-if)# bandwidth-percentage 0 40 1 60`	Configure the bandwidth percentage for TCG 0 and 1

Validation

SW1

Verify the data set on SW1

```
#show enhanced-transmission-selection interface eth1
Interface : eth1
Enhanced Transmission Selection : on

Admin Configuration

Mode  Advertise Willing   Max-TCG  TCG-ID  BW%   Priorities
================================================================================
On    On        Off       0        0       40     0 1 2
On    On        Off       0        1       60     3 4 5
On    On        Off       0        15      NA     6 7

Operational Configuration
Oper  Max_TCG TCG-ID  BW%   Priorities
State
================================================================================
On    0       0       40     0 1 2
On    0       1       60     3 4 5
On    0       15      NA     6 7
```


© 2021 IP Infusion Inc. Proprietary

SW2

Verify the data set on SW2

```
#show enhanced-transmission-selection interface eth1
Interface : eth1
Enhanced Transmission Selection : on

Admin Configuration

Mode  Advertise Willing   Max-TCG  TCG-ID  BW%   Priorities
================================================================================
On    On        Off       0        0       40     0 1 2
On    On        Off       0        1       60     3 4 5
On    On        Off       0        15      NA     6 7

Operational Configuration
Oper  Max_TCG TCG-ID  BW%   Priorities
State
================================================================================
On    0       0       40     0 1 2
On    0       1       60     3 4 5
On    0       15      NA     6 7
```

Configuring PFC Parameter Exchange

SW2

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enable DCB on the bridge
`(config)#priority-flow-control enable bridge 1`	Enable PFC on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-org-specific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#priority-flow-control mode on`	Configure the advertise flag and start sending DCBx TLVs in LLDP messages
`(config-if)#priority-flow-control cap 4`	Configure the maximum number of PFC priorities
`(config-if)#priority-flow-control enable priority 2 4 5`	Enables PFC on priorities 2,4, and 5
`(config-if)#priority-flow-control link-delay-allowance 34567`	Configure the link delay allowance

SW1

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enable DCB on the bridge
`(config)#priority-flow-control enable bridge 1`	Enable PFC on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-org-specific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#priority-flow-control mode on`	Configure the advertise flag and start sending DCBx TLVs in LLDP messages
`(config-if)#priority-flow-control cap 4`	Configure the maximum number of PFC priorities
`(config-if)#priority-flow-control enable priority 2 4 5`	Enables PFC on priorities 2,4, and 5
`(config-if)#priority-flow-control link-delay-allowance 34567`	Configure the link delay allowance

Validation

SW1

Verify the data set.

```
#show priority-flow-control details interface eth1
bridge : 1
priority flow control : on
interface : eth1

Admin Configuration
mode  advertise willing   cap   link        priorities
                                delay
                                allowance
================================================================================
on    on        off       4     34567       2 4 5

Operational Configuration
state cap   link        priorities
            delay
            allowance
================================================================================
on    4     34567       2 4 5
```


© 2021 IP Infusion Inc. Proprietary

SW2

Verify the data set.

```
#show priority-flow-control details interface eth1
bridge : 1
priority flow control : on
interface : eth1

Admin Configuration
mode  advertise willing   cap   link        priorities
                                delay
                                allowance
================================================================================
==
on    on        off       4     34567       2 4 5

Operational Configuration
state cap   link        priorities
            delay
            allowance
================================================================================
==
on    4     34567       2 4 5
```

© 2021 IP Infusion Inc. Proprietary

Data Center Bridging Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Enhanced Transmission Selection Commands*
- Chapter 2, *Quantized Congestion Notification Commands*
- Chapter 3, *Priority-based Flow Control Commands*

Note: Trident-2 and Trident-2+ platforms support all DCB features (PFC, QCN, ETS, DCBx for ETS and PFC parameter exchange).

Trident-3 platforms support only the following DCB features: PFC and DCBx only for PFC parameter exchange.

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Enhanced Transmission Selection Commands

This section list and describe the commands that can be used to configure Enhanced Transmission Selection (ETS) in a Data Center Bridging (DCB) environment. It includes the following commands:

- application-priority advertise-local-config
- application-priority enable (interface)
- application-priority enable (switch)
- bandwidth-percentage
- data-center-bridging
- dcbx enable
- enhanced-transmission-selection accept-peer-config
- enhanced-transmission-selection advertise-local-config
- enhanced-transmission-selection (switch)
- enhanced-transmission-selection (interface)
- ethertype
- max-traffic-class-group
- show application-priority bridge
- show application-priority interface
- show data-center-bridging
- show enhanced-transmission-selection bridge
- show enhanced-transmission-selection interface
- tcp
- traffic-class-group
- udp

© 2021 IP Infusion Inc. Proprietary

application-priority advertise-local-config

Use this command to enable advertising mode for ETS feature on the interface.

Use the no form of this command to disable advertising mode for the interface.

Command Syntax

```
application-priority advertise-local-config
no application-priority advertise-local-config
```

Parameters

None

Default

By default, advertising mode for ETS feature on the interface is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#application-priority advertise-local-config
```


© 2021 IP Infusion Inc. Proprietary

application-priority enable (interface)

Use this command to enable the application priority feature of DCB on an interface.

Use the no form of this command to disable application priority on an interface.

Command Syntax

```
application-priority enable
no application-priority
```

Parameters

None

Default

By default, application priority feature of DCB on an interface is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#application-priority enable
```

application-priority enable (switch)

Use this command to enable the application priority feature of DCB on a switch (bridge).

Use the no form of this command to disable application priority on a switch.

Command Syntax

```
application-priority enable bridge <1-32>
no application-priority bridge <1-32>
```

Parameters

<1-32>	Specify the Bridge ID.

Default

By default, application priority feature of DCB on a switch is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#application-priority enable bridge 2
```


© 2021 IP Infusion Inc. Proprietary

bandwidth-percentage

Use this command to assign a percentage of bandwidth to a traffic class group. The total percentage bandwidth should be equal to 100 percent.

Command Syntax

```
bandwidth-percentage (<0-1> <0-100> | <0-1> <0-100> <0-1> <0-100>)
```

Parameters

`<0-1>`	Specify the traffic class group ID. You can set a bandwidth percentage for up to two IDs.
`<0-100>`	Specify the bandwidth percentage for the traffic class group.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth1
(config-if)#bandwidth-percentage 0 40 0 60
```

data-center-bridging

Use this command to enable DCB (Data Center Bridging) on a switch (bridge).

Use the `no` form of this command to disable DCB.

Command Syntax

```
data-center-bridging enable bridge <1-32>
no data-center-bridging enable bridge <1-32>
```

Parameters

`bridge`	Bridge ID.

Default

By default, DCB on a switch is disabled.

Command Mode

Configure mode

Default

DCB is enabled.

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#data-center-bridging enable bridge 1


#configure terminal
(config)#no data-center-bridging enable bridge 1
```


© 2021 IP Infusion Inc. Proprietary

dcbx enable

Use this command to enables DCBX (Data Center Bridging Exchange) on the interface in lldp-agent mode.

Use the `no` form of this command to disable DCBX.

Command Syntax

```
dcbx enable
no dcbx enable
```

Parameters

None

Default

By default, DCBX is disabled.

Command Mode

LLDP Agent mode

Default

DCB is enabled.

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#lldp-agent
(lldp-agent)#dcbx enable
```

enhanced-transmission-selection accept-peer-config

Use this command to enable willing mode for ETS on the interface.

Use the `no` form of this command to disable willing mode.

Command Syntax

```
enhanced-transmission-selection accept-peer-config
no enhanced-transmission-selection accept-peer-config
```

Parameters

None

Default

By default, willing mode is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#enhanced-transmission-selection accept-peer-config
```


© 2021 IP Infusion Inc. Proprietary

enhanced-transmission-selection advertise-local-config

Use this command to enable advertising mode for ETS on the interface.

Use the `no` form of this command to disable advertising mode.

Command Syntax

```
enhanced-transmission-selection advertise-local-config
no enhanced-transmission-selection advertise-local-config
```

Parameters

None

Default

By default, advertising mode for ETS on the interface is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#enhanced-transmission-selection advertise-local-config
```

enhanced-transmission-selection (switch)

Use this command to enable the ETS feature of DCB on a switch (bridge).

Use the `no` form of this command to disable ETS.

Command Syntax

```
enhanced-transmission-selection enable bridge <1-32>
no enhanced-transmission-selection bridge <1-32>
```

Parameters

`<1-32>`	Bridge ID.

Default

By default, ETS feature is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#enhanced-transmission-selection enable bridge 1


#configure terminal
(config)#no enhanced-transmission-selection bridge 1
```


© 2021 IP Infusion Inc. Proprietary

enhanced-transmission-selection (interface)

Use this command to enable the ETS feature of DCB on an interface.

Use the `no` from of this command to disable the ETS at an interface.

Command Syntax

```
enhanced-transmission-selection mode (on|auto)
no enhanced-transmission-selection
```

Parameters

`auto`	Select auto to negotiate ETS capabilities.
`on`	Select on to force enable ETS.

Default

Default is Auto.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth1
(config-if)#enhanced-transmission-selection mode on

(config)#interface eth1
(config-if)#no enhanced-transmission-selection
```

ethertype

Use this command to set the application priority based on the Ethertype.

Use the `no` parameter along with this command to unset the application priority based on the Ethertype.

Command Syntax

```
ethertype (value ETHERTYPE | name ETHERNAME) priority <0-7>
no ethertype (value ETHERTYPE | name ETHERNAME) priority <0-7>
```

Parameters

`value ETHERTYPE`

Ethertype value in hexadecimal notation (such as “0xhhhh”).

`name ETHERNAME`

Enter a well-known Ethertype string. Ethertype supports the following protocol names:

ip (IPv4), ipv6 (IPv6), ipx (IPX), x25 (CCITT X.25), arp (Address Resolution), rarp (Reverse Address Resolution), atalkddp (Appletalk DDP), atalkaarp (Appletalk AARP), atmmulti (MultiProtocol over ATM), atmtransport (Frame-based ATM Transport), pppdiscovery (PPPoE discovery), pppsession (PPPoE Session), xeroxpup (Xerox PUP), xeroxaddrtrans (Xerox PUP Address Translation), g8bpqx25 (G8BPQ AX.25), ieeepup (Xerox IEEE802.3 PUP), ieeeaddrtrans (Xerox IEEE802.3 PUP Address Translation), dec (DEC Assigned), decdnadumpload (DEC DNA Dump/Load), decdnaremoteconsole (DEC DNA Remote Console), decdnarouting (DEC DNA Routing), declat (DEC LAT), decdiagnostics (DEC Diagnostics), deccustom (DEC Customer Use), decsyscomm (DEC Systems Comms Arch)

`priority` User priority value <0-7>.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ethertype value 0x0800 priority 6

(config)#interface eth1
(config-if)#ethertype name arp priority 6

(config)#interface eth1
(config-if)#no ethertype value 0x0800 priority 6

(config)#interface eth1
```

 © 2021 IP Infusion Inc. Proprietary

```
(config-if)#no ethertype name arp priority 6
```

max-traffic-class-group

Use this command to configure the maximum number of traffic classes that you can enable on ETS.

Use the `no` form of this command to set the maximum number of traffic classes to 0 which is the default.

If the value is 0, you can add priorities for all 8 traffic classes with the traffic-class-group command. When the number of traffic classes is not 0, you can add priorities with the traffic-class-group command until the maximum is reached.

Command Syntax

```
max-traffic-class-group <0-2>
no max-traffic-class-group
```

Parameters

`<0-2>`	The maximum number of traffic class groups.

Default

Default maximum number of traffic classes is 0.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#max-traffic-class-group 2
(config-if)#
```


© 2021 IP Infusion Inc. Proprietary

show application-priority bridge

Use this command to display application priority table for a bridge (switch).

Command Syntax

```
show application-priority bridge <1-32>
```

Parameter

<1-32>	Bridge ID.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example 1

```
#show application-priority bridge 2
bridge : 2

Admin Configuration
intf  Admin Config    Protocol    ProtoId   Priorities
      Mode  Advertise
=============================================================================
eth1  On    On        Ethertype   ip         6
eth1  On    On        Ethertype   arp        6
eth1  On    On        udp         telnet     6
eth1  On    On        tcp         telnet     6
```

Table 1-217 Explains the show command output fields

Table 1-217: Show application-priority output fields

Field	Description
intf	Number of maximum intf admin session.
Admin mode	Allows the user to configure and monitor security data.
Config Advertise	Allows the user to configure and advertise security data.
Protocol	Used to interconnect network devices on the internet.
Proto Id	Used to identify the network devices on the internet.
Priorities	Used to provide the priorities for the data.

show application-priority interface

Use this command to display application priority table for an interface.

Command Syntax

```
show application-priority interface IFNAME
```

Parameter

IFNAME	Name of the interface.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example 1

```
#show application-priority interface eth1
bridge : 2
Application Priority : On

Admin Configuration
intf  Admin Config    Protocol    ProtoId   Priorities
      Mode  Advertise
================================================================================
eth1  On    On        Off         -           -         -
```

Table 1-218 Explains the show command output fields

Table 1-218: Show application-priority interface output fields

Field	Description
intf	Number of maximum intf admin session.
Admin mode	Allows the user to configure and monitor security data.
Config Advertise	Allows the user to configure and advertise security data.
Protocol	Used to interconnect network devices on the internet.
Proto Id	Used to identify the network devices on the internet.
Priorities	Used to provide the priorities for the data.

© 2021 IP Infusion Inc. Proprietary

show data-center-bridging

Use this command to display administrative, operational, and remote parameters for DCBX.

Command Syntax

```
show data-center-bridging (admin-details | operational-details | remote-details)
  interface IFNAME
```

Parameter

admin-details	Administrative details.
operational-details	Operational details.
remote-details	Remote details.
interface	Interface.
IFNAME	Name of the interface.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example 1

```
#show data-center-bridging operational-details interface eth1
PFC Operational details
interface : eth1
state cap    syncd priorities
================================================================================
Off   0      Off


ETS Operational details
interface : eth1
State MAX_TCGs  TCG-ID    BW%  priorities
================================================================================
On    0         0         0
On    0         1         0     1 2 3 4 5 6 7
On    0         2         0
On    0         3         0
On    0         4         0
On    0         5         0
On    0         6         0
On    0         7         0
```

```
On     0          15         NA     0


Application priority operational details
interface : eth1
State Adv   Will  Proto ProtoID   priorities    app
================================================================================
```

Table 1-219 Explains the show command output fields

Table 1-219: show data-center-bridging output fields

Field	Description
State	State of the session.
Cap	Allows the user to configure and monitor security data.
MAX TCGs	Maximum trusted computing group in the interface.
TCG-ID	Trusted computing group identification.
BW	Bandwidth of network.
Will	Used to send and receive the data.
app	Network application.
Protocol	Used to interconnect network devices on the internet.
Proto Id	Used to identify the network devices on the internet.
Priorities	Used to provide the priorities for the data.

© 2021 IP Infusion Inc. Proprietary

show enhanced-transmission-selection bridge

Use this command to display all traffic class groups for a bridge (switch).

Command Syntax

```
show enhanced-transmission-selection bridge <1-32>
```

Parameter

<1-32>	Bridge ID.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example 1

```
#show enhanced-transmission-selection bridge 2
bridge : 2
Admin Configuration
intf  Admin Config    Willing   Max-TCG  TCGID BW% Priorities
      Mode  Advertise
================================================================================
eth1  On    On        On        0        15    NA   0 1 2 3 4 5 6 7

Operational Configuration
intf  Oper  Max-Tcg  TCGID BW% Priorities
      State
================================================================================
eth1  On    15    NA   0 1 2 3 4 5 6 7
```

Table 1-220 Explains the show command output fields

Table 1-220: show enhanced-transmission-selection bridge output fields

Field	Description
intf	Number of maximum intf admin session.
Admin mode	Allows the user to configure and monitor security data.
Config Advertise	Allows the user to configure and advertise security data.
State	State of the session.
MAX TCGs	Maximum trusted computing group in the interface.

Field	Description
TCG-ID	Trusted computing group identification.
BW	Bandwidth of network.
Willing	Used to send and receive the data.
Protocol	Used to interconnect network devices on the internet.
Proto Id	Used to identify the network devices on the internet.
Priorities	Used to provide the priorities for the data.

© 2021 IP Infusion Inc. Proprietary

show enhanced-transmission-selection interface

Use this command to display all traffic class groups for an interface.

Command Syntax

```
show enhanced-transmission-selection interface IFNAME
```

Parameter

IFNAME	Name of the interface.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example 1

```
#show enhanced-transmission-selection interface eth1
Interface : eth1
Enhanced Transmission Selection : on

Admin Configuration

Mode  Advertise Willing   Max-TCG  TCG-ID  BW%   Priorities
================================================================================
On    On        On        0        15      NA     0 1 2 3 4 5 6 7

Operational Configuration
Oper  Max_TCG TCG-ID  BW%   Priorities
State
================================================================================
On    0       15      NA     0 1 2 3 4 5 6 7
```

Table 1-221 Explains the show command output fields

Table 1-221: show enhanced-transmission-selection interface output fields

Field	Description
Admin mode	Allows the user to configure and monitor security data.
Config Advertise	Allows the user to configure and advertise security data.
State	State of the session.
MAX TCGs	Maximum trusted computing group in the interface.
TCG-ID	Trusted computing group identification.

Field	Description
BW	Bandwidth of network.
Willing	Used to send and receive the data.
Protocol	Used to interconnect network devices on the internet.
Proto Id	Used to identify the network devices on the internet.
Priorities	Used to provide the priorities for the data.

© 2021 IP Infusion Inc. Proprietary

tcp

Use this to set the application priority based on TCP. The protocol ID is the protocol number in decimal value or protocol service name.

Use the `no` parameter along with this command to unset the application priority based on the selection type.

Command Syntax

```
tcp (port-no <1-1023>) priority <0-7>
no tcp (port-no <1-1023>) priority <0-7>
tcp (service-name [PROTOSERV]) priority <0-7>
no tcp (service-name [PROTOSERV]) priority <0-7>
```

Parameters

`port-no`	Enter a well-known protocol number in decimal <1-1023>.
`service-name[PROTOSERV]`	Protocol service name. Enter a well-known service name, such as telnet.
`priority`	Default priority for CFM frames to be relayed <0-7>.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#tcp port-no 23 priority 6

(config)#interface eth1
(config-if)#tcp service-name telnet priority 6

(config)#interface eth1
(config-if)#no tcp port-no 23 priority 6

(config)#interface eth1
(config-if)#no tcp service-name telnet priority 6
```

traffic-class-group

Use this command to add or remove priorities for a traffic class group.

Use the `no` form of this command to remove all traffic-class-groups.

Command Syntax

```
traffic-class-group <0-1> add priority <0-7> (<0-7>(<0-7>(<0-7>(<0-7>(<0-7>(<0-
  7>(<0-7>|)|)|)|)|)|)|)
traffic-class-group <0-1> remove priority <0-7> (<0-7>(<0-7>(<0-7>(<0-7>(<0-7>(<0-
  7>(<0-7>|)|)|)|)|)|)|)
no traffic-class-groups
```

Parameters

`<0-1>`	Specify traffic-class-group ID.
`add priority`	Specify to add a traffic class group
`<0-7>`	Traffic-priority value. Up to seven priorities can be added.
`remove priority`	Specify to remove a traffic class group
`<0-7>`	Traffic-priority value. Up to seven priorities can be removed.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#traffic-class-group 1 add priority 1 2 3 4 5 6 7

(config)#interface eth1
(config-if)#traffic-class-group 1 remove priority 3 6

(config)#interface eth1
(config-if)#no traffic-class-group
```


© 2021 IP Infusion Inc. Proprietary

udp

Use this to set the application priority based on UDP. The protocol ID is the protocol number in decimal value or protocol service name.

Use the `no` parameter along with this command to unset the application priority.

Command Syntax

```
udp (port-no <1-1023>) priority <0-7>
no udp (port-no <1-1023>) priority <0-7>
udp (service-name [PROTOSERV]) priority <0-7>
no udp (service-name [PROTOSERV]) priority <0-7>
```

Parameters

`port-no`	Enter a well-known protocol number in decimal <1-1023>.
`service-name [PROTOSERV]`	Protocol service name. Enter a well-known service name, such as telnet.
`priority`	Default priority for CFM frames to be relayed <0-7>.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#udp port-no 23 priority 6

(config)#interface eth1
(config-if)#udp service-name telnet priority 6

(config)#interface eth1
(config-if)#no udp port-no 23 priority 6

(config)#interface eth1
(config-if)#no udp service-name telnet priority 6
```

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Quantized Congestion Notification Commands

This section describes the commands that you use to configure Quantized Congestion Notification (QCN) in a Data Center Bridging (DCB) environment. QCN is a IEEE 802.1Qau mechanism that manages network congestion. When a queue reaches a configured threshold, QCN throttles traffic at the source of the congestion by transmitting messages that propagate back to the source and temporarily stop the source from transmitting. When the queue crosses the threshold that indicates the congestion has dissipated, QCN sends a message to allow the source to resume transmitting frames. QCN includes the following commands:

- cnpv
- cp enable
- defense-mode cnpv
- qcn enable
- show qcn configuration
- show qcn cnpv
- show qcn cp

cnpv

Use this command to enable Congestion Notification Priority Values (CNPV). A CNPV corresponds to a class of applications or a single application, such as interprocess communications or disk storage, that have different requirements for network resources as such as latency or bandwidth. There are total of eight CNPVs with one reserved for “best-effort” traffic, meaning you can assign up to seven CNPVs.

Use the `no` form of this command to disable CNPVs.

Command Syntax

```
cnpv <0-7> (<0-7>(<0-7>(<0-7>(<0-7>(<0-7>|)|)|)|)|)|)
no cnpv <0-7> (<0-7>(<0-7>(<0-7>(<0-7>(<0-7>(<0-7>|)|)|)|)|)|)
```

Parameters

`<0-7>`	Congestion notification priority values (up to seven).

Default

By default, CNPV is disabled.

Command Mode

QCN mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#qcn enable bridge 1
(config-qcn)#cnpv 4 6
```


© 2021 IP Infusion Inc. Proprietary

cp enable

Use this command to create a Congestion Point (CP) for a Congestion Notification Priority Value (CNPV).

Use the `no` form of this command to disable a CP.

Command Syntax

```
cp enable ((cnpv <0-7>|) (sample-base <10000-4294967295>|) (weight WEIGHT|)
no cp (cnpv <0-7>|)
```

Parameters

`cnpv`	Congestion notification priority.
`<0-7>`	Congestion notification priority value.
`sample-base`	Sample base.
`<10000-4294967295>`	The minimum number of octets to enqueue in the Congestion Point's queue between transmissions of Congestion Notification Messages (CNMs). The default is 150,000.
`weight`	Weight in offset calculation.
`WEIGHT`	The weight change in queue length used to calculate whether the queue length is moving toward or away from the target number of octets for the CP's queue <-10 - 10>. The default is one (1).

Default

Default sample base value is 150,000 and WEIGHT value is 1.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>ena
#con term
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#interface eth0
(config-if)#cp enable sample-base 100000 weight 2
```

defense-mode cnpv

Use this command to set the defense mode for a Congestion Notification Priority Value (CNPV).

In QCN mode, you can:

- Specify an `admin` type to explicitly set the defense mode and the alternate priority.
- Specify `auto` to derive the defense mode from LLDP Congestion Notification TLVs.

In addition, in interface mode, you can specify `component` to set the defense mode the same as the bridge-level defense mode.

Command Syntax

QCN mode:

```
defense-mode cnpv <0-7> (admin (disabled|edge|interior|interior-ready) alternate-
  priority <0-7> | auto)
```

Interface mode:

```
defense-mode cnpv <0-7> (admin (disabled|edge|interior|interior-ready) alternate-
  priority <0-7> |auto |component)
```

Parameters

`cnpv`	CNPV.
`<0-7>`	CNPV.
`admin`	Explicitly set the defense mode:
`disabled`	Congestion notification is disabled for this CNPV and interface.
`edge`	On this interface and for this CNPV, the priority parameters of input frames are remapped to an alternate value. Congestion notification tags are not output.
`interior`	On this interface and for this CNPV, the priority parameters of input frames are not remapped to another value. Congestion notification tags are not output.
`interior-ready`	On this interface and for this CNPV, the priority parameters of input frames are not remapped to another value. Congestion notification tags can be output.
`alternate-priority`	Explicitly set the alternate priority.
`<0-7>`	Alternate priority value.
`auto`	Set the defense mode according to LLDP Congestion Notification TLVs and set the alternate priority to the cncpAutoAltPri variable as defined in the 802.1Qau standard.
`component`	Set the defense mode the same as the bridge-level defense mode and set the alternate priority to the cncpAutoAltPri variable as defined in the 802.1Qau standard.

Default

None

Command Mode

QCN mode and interface mode

© 2021 IP Infusion Inc. Proprietary

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#qcn enable bridge 1
(config-qcn)#defense-mode cnpv 4 admin edge alternate-priority 6

#configure terminal
 config)#interface eth1
(config-if)#defense-mode cnpv 4 component
```

qcn enable

Use this command to enable QCN at the switch (bridge) level. This command initializes the QCN module with default values.

Use the `no` form of this command to disable QCN.

Command Syntax

```
qcn enable bridge <1-32> (cnm-transmit-priority <0-7> | )
no qcn bridge <1-32>
```

Parameters

`<1-32>`	Bridge ID.
`<0-7>`	Priority to use when transmitting Congestion Notification Messages (CNMs).

Default

By default, QCN is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#qcn enable bridge 1 cnm-transmit-priority 4
```


© 2021 IP Infusion Inc. Proprietary

show qcn configuration

Use this command to show the configuration of the QCN module.

Command Syntax

```
show qcn configuration bridge <1-32>
```

Parameters

<1-32>	Bridge ID.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show qcn configuration bridge 2

 QCN:   Enable
 CNM Transmit Priority: 6
 Discarded Frames: 0
 Errored Port List: NONE

 Priority       CNPV
 ========       ====
 0              No
 1              No
 2              Yes
 3              Yes
 4              No
 5              No
 6              No
 7              No

 CNPV details:

 CNPV  DefModeChoice  AltPriority  DefenseMode
 ====  =============  ===========  ==============
 2     AUTO           0            EDGE
 3     AUTO           0            EDGE

 CNPV details per interface:
 Interface       CNPV  DefModeChoice  AltPriority  DefenseMode     XmitReady
 ==============  ====  =============  ===========  ==============  =========
 eth1            2     ADMIN          1            INTERIOR        TRUE
 eth1            3     ADMIN          6            EDGE            FALSE
```

```
Congestion Point Details:
Interface        CpId       W     SampleBase  MinHdrOctet  Qsp
==============   ========   ====  ==========  ===========  ===
eth1             ********   2.00  0           0            0
```

Table 2-222 Explains the show command output fields.

Table 2-222: show qcn configuration output fields

Field	Description
QCN	Enable the QCN on the bridge and interface.
CNM Transmit Priority	Details of the CNM transmit priority on the interface.
Discarded Frames	Discarded frames detail from the interface.
Errored Port List	List of the port error.
Priority	QCN priority on the interface.
CNPV details	Details of the CNPV on the bridge and interface.
CNPV details per interface	Details of the CNPV per interface.
Congestion Point Details	Details of the configured congestion point value.

© 2021 IP Infusion Inc. Proprietary

show qcn cnpv

Use this command to display application priority table per interface.

Command Syntax

```
show qcn cnpv ((bridge BRIDGE_ID) | (interface PORT_ID ))
```

Parameter

bridge	Bridge.
<1-32>	Bridge ID.
interface	Interface.
PORT_ID	Interface name.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example 1

```
#show qcn cnpv bridge 2

 Priority       CNPV
 ========       ====
 0              No
 1              No
 2              Yes
 3              Yes
 4              No
 5              No
 6              No
 7              No

 CNPV details:

 CNPV  DefModeChoice  AltPriority  DefenseMode
 ====  =============  ===========  ==============
 2     AUTO           0            EDGE
 3     AUTO           0            EDGE

 CNPV details per interface:
 Interface       CNPV  DefModeChoice  AltPriority  DefenseMode     XmitReady
 ==============  ====  =============  ===========  ==============  =========
 eth1            2     ADMIN          1            INTERIOR        TRUE
 eth1            3     ADMIN          6            EDGE            FALSE

#show qcn cnpv interface eth1
```

```
CNPV details per interface:
Interface       CNPV  DefModeChoice  AltPriority  DefenseMode     XmitReady
==============  ====  =============  ===========  ==============  =========
eth1            2     ADMIN          1            INTERIOR        TRUE
eth1            3     ADMIN          6            EDGE            FALSE
```

Table 2-223 Explains the show command output fields.

Table 2-223: show qcn cnpv output fields

Field	Description
Priority	QCN priority on the interface.
CNPV	Status of the CNPV on the bridge and interface.
CNPV details	Details of the CNPV on the bridge and interface.
CNPV details per interface	Details of the CNPV per interface.
Congestion Point Details	Details of the configured congestion point value.

© 2021 IP Infusion Inc. Proprietary

show qcn cp

Use this command to show the configuration of all congestion points on the interface.

Command Syntax

```
show qcn cp ((bridge <1-32> )|(interface PORT_ID))
```

Parameters

`bridge`	Bridge.
`<1-32>`	Bridge ID.
`interface`	Interface.
`PORT_ID`	Interface name.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show qcn cp bridge 2

 Congestion Point Details:
 Interface       CpId      W     SampleBase  MinHdrOctet  Qsp
 ==============  ========  ====  ==========  ===========  ===
 eth1            ********  2.00  0           0            0

#show qcn cp interface eth1

Congestion Point Details:
 Interface       CpId      W     SampleBase  MinHdrOctet  Qsp
 ==============  ========  ====  ==========  ===========  ===
 eth1            ********  2.00  0           0            0
```

Table 2-224 Explains the show command output fields.

Table 2-224: show qcn cp output fields

Field	Description
Congestion Point Details	Details of the configured congestion point value.

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 Priority-based Flow Control Commands

This section lists and describes the commands that can be used to configure Priority-based Flow Control (PFC) in a Data Center Bridging (DCB) environment.It includes the following commands:

- priority-flow-control accept-peer-config
- priority-flow-control advertise-local-config
- priority-flow-control enable
- priority-flow-control cap
- priority-flow-control enable priority
- priority-flow-control link-delay-allowance
- priority-flow-control mode
- show priority-flow-control details
- show priority-flow-control statistics

© 2021 IP Infusion Inc. Proprietary

priority-flow-control accept-peer-config

Use this command to enable willing mode for PFC on the interface.

If willing is enabled, then by default advertise mode is also enabled.

Use the `no` form of this command to disable willing mode.

Command Syntax

```
priority-flow-control accept-peer-config
no priority-flow-control accept-peer-config
```

Parameters

None

Default

By default, willing mode for PFC on the interface is disabled. If willing is enabled, then by default advertise mode is also enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#priority-flow-control accept-peer-config
```


© 2021 IP Infusion Inc. Proprietary

priority-flow-control advertise-local-config

Use this command to enable advertising mode for PFC on the interface.

Use the `no` form of this command to disable advertising mode.

Command Syntax

```
priority-flow-control advertise-local-config
no priority-flow-control advertise-local-config
```

Parameters

None

Default

By default, advertising mode for PFC on the interface is disabled. If willing is enabled, then by default advertise mode is also enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#priority-flow-control advertise-local-config
```

priority-flow-control enable

Use this command to enable Priority-based Flow Control (PFC) on a switch (bridge).

Use the `no` form of this command to disable PFC.

Command Syntax

```
priority-flow-control enable bridge <1-32>
no priority-flow-control bridge <1-32>
```

Parameters

`<1-32>`	Bridge ID.

Default

By default, PFC is disabled.

Command Mode

Configure mode

Default

PFC is disabled by default.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#priority-flow-control enable bridge 32

#configure terminal
(config)#no priority-flow-control bridge 32
```


© 2021 IP Infusion Inc. Proprietary

priority-flow-control cap

Use this command to configure a priority-flow-control cap for the number of priorities allowed on an interface.

Use the `no` parameter along with this command to return the value to its default level.

Command Syntax

```
priority-flow-control cap <0-8>
no priority-flow-control cap
```

Parameters

`<0-8>`	Select a cap value. Zero indicates that there is no limitations.

Default

By default, priority-flow-control cap value is 8.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth2
(config-if)#priority-flow-control cap 7
```

priority-flow-control enable priority

Use this command to enable the PFC at the interface level for a specific priority.

Use the `no` parameter along with this command to disable PFC for a priority.

Command Syntax

```
priority-flow-control enable priority <0-7> (<0-7>(<0-7>(<0-7> (<0-7>(<0-7>(<0-
  7>(<0-7>|)|)|)|)|)|)|)
no priority-flow-control enable priority <0-7> (<0-7>(<0-7>(<0-7>(<0-7>(<0-7>(<0-
  7>(<0-7>|)|)|)|)|)|)|)
```

Parameter

`<0-7>`	Traffic-priority value. You can specify up to seven priorities.

Default

None

Command Mode

Interface mode

Default

PFC is disabled by default.

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth1
(config-if)#priority-flow-control enable priority 1 2 3 4 5 6 7

(config)#interface eth1
(config-if)#no priority-flow-control enable priority 2 3 4
```


© 2021 IP Infusion Inc. Proprietary

priority-flow-control link-delay-allowance

Use this command to set PFC link delay allowance on an interface. This command provides allowance for round-trip propagation delay of the link in bits; moreover, it is one of the factors that determines when to trigger PAUSE.

Use the `no` parameter along with this command to unset PFC link delay allowance on an interface.

Command Syntax

```
priority-flow-control link-delay-allowance <0-4294967296>
no priority-flow-control link-delay-allowance
```

Parameter

`<0-4294967296>` Link characteristics that affect the link delay (for example, link length).

Command Mode

Interface mode

Default

Default value is zero.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#priority-flow-control link-delay-allowance 5

(config)#interface eth1
(config-if)#no priority-flow-control link-delay-allowance
```

priority-flow-control mode

Use this command to enable Priority-based Flow Control (PFC) on an interface.

Ues the `no` form of this command to disable PFC on an interface.

Command Syntax

```
priority-flow-control mode (on | auto)
no priority-flow-control
```

Parameters

`auto`	Negotiate PFC capabilities.
`on`	Force-enable PFC, overriding negotiation.

Default

By default, PFC is disabled.

Command Mode

Interface mode

Default

PFC is disabled by default.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#priority-flow-control mode auto
```


© 2021 IP Infusion Inc. Proprietary

show priority-flow-control details

Use this command to display the PFC details for a specified interface or bridge.

Command Syntax

```
show priority-flow-control details ((interface IFNAME)|(bridge <1-32>))
```

Parameters

IFNAME	Name of the input or output interface.
<1-32>	Specify a bridge ID.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show priority-flow-control details interface eth1
bridge : 2
priority flow control : on
interface : eth1

Admin Configuration
mode  advertise willing   cap   link        priorities
                                delay
                                allowance
================================================================================
on    on        off       5     128         2 3 4 5

Operational Configuration
state cap   link        priorities
            delay
            allowance
================================================================================
on    5     128         2 3 4 5
```

Table 3-225: Show priority-flow control details output

Entry	Description
bridge	The bridge number to which this interface is associated (1-32).
priority flow control	Show whether priority flow control is either on or off.

Table 3-225: Show priority-flow control details output (Continued)

Entry	Description
interface	The interface name.
Admin Configuration	The configuration as entered on this device.
mode	The priority flow control operating mode – `on`, `off`, or `auto`.
advertise	Status of advertisement of the configuration to the peer device.
willing	The willingness of the local interface to learn the PFC configuration from the peer. Values are either `on` or `off`.
cap	Cap is a limit set that specifies the maximum number of PFC priorities.
link delay allowance	The allowance made for round-trip propagation delay of the link in bits.
Priorities	Shows the PFCs that have been to be used on the priorities.
Operational Configuration	The actual configuration that exists between this device and its PFC peer.
state	Shows whether PFC is functioning. Values are `on`, `off`, or `auto`.
cap	Cap is the limit that specifies the maximum number of PFC priorities.
link delay allowance	The allowance being used for round-trip propagation delay of the link in bits.
priorities	The PFCs actually being used by this device and its peer.

© 2021 IP Infusion Inc. Proprietary

show priority-flow-control statistics

Use this command to display statistics about the number of PFC Pause frames sent and received for a specified interface or bridge. If you do not specify a bridge or interface, this commands shows statistics for the bridge.

Command Syntax

```
show priority-flow-control statistics ((interface IFNAME)| (bridge <1-32>))
```

Parameters

`<1-32>`	Specify bridge ID.
`IFNAME`	Name of the input or output interface.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show priority-flow-control statistics interface eth1
bridge : 2
interface : eth1
pause sent     pause received
==============================
5968061499624837205583457 4861
```

© 2021 IP Infusion Inc. Proprietary

SECTION 10 Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *VRRP Configuration*
- Chapter 2, *VRRP IPv6 Configuration*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 VRRP Configuration

This chapter provides an overview of Virtual Router Redundancy Protocol (VRRP) and its implementation with OcNOS. VRRP eliminates the risk of a single point of failure inherent in a static default routing environment. It specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. One of the major advantages of VRRP is that it makes default path available without requiring configuration of dynamic routing on every end-host.

OcNOS only supports VRRP protocol version 3.

Terminology

Terms related to VRRP configuration are defined in the table below.

Backup Router	The VRRP router that is backing up an IP address. It assumes forwarding responsibility for the virtual IP address if the Master fails.
Critical IP	The IP address that a VRRP router sends/receives messages on for a particular session.
IP Address Owner	The VRRP Router that has the virtual router's IP address(es) as real interface address(es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, and so on
Master Router	The VRRP router that owns the IP address (i.e., is being backed up), and which is the default router for forwarding for that IP address.
Virtual IP	The IP address that is being backed up by a VRRP session.
Virtual Router	A router managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP addresses across a common LAN. A VRRP Router might backup one or more virtual routers.
VRRPv2 Router	A router running the Virtual Router Redundancy Protocol version 2. It might participate in one or more virtual routers.
VRRPv3 Router	A router running the Virtual Router Redundancy Protocol version 3. It might participate in one or more virtual routers.

VRRP Process

Typically, end hosts are connected to the enterprise network through a single router (first-hop router) that is in the same Local Area Network (LAN) segment. The most popular method of configuration is for the end hosts to configure statically this router as their default gateway. This minimizes configuration and processing overhead. As shown in Figure 1-32, the problem with this configuration is that it produces a single point of failure if this first-hop router fails.

© 2021 IP Infusion Inc. Proprietary

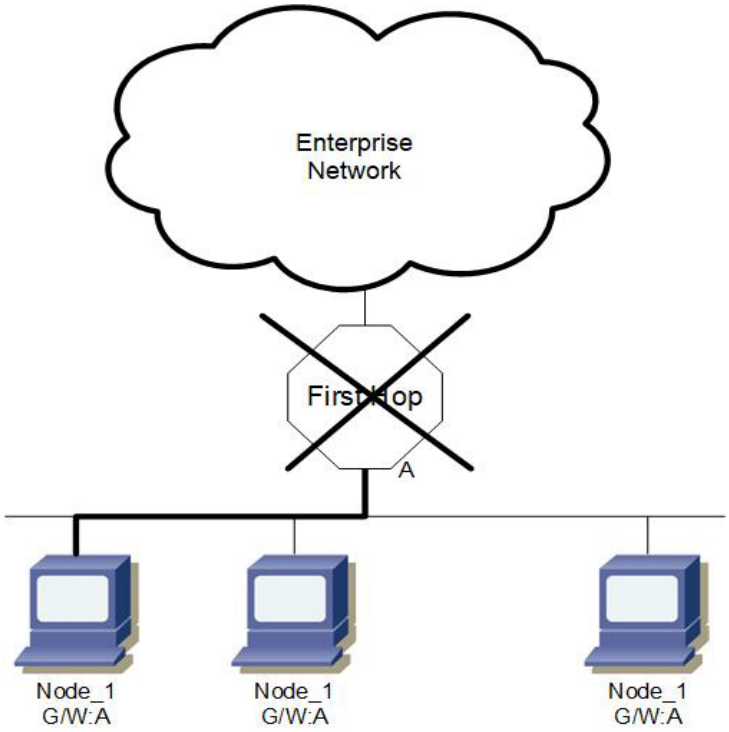


Figure 1-32: VRRP Process - First-Hop Not Reachable

The Virtual Router Redundancy Protocol attempts to solve this problem by introducing the concept of a virtual router, composed of two or more VRRP routers on the same subnet as shown in Figure 1-33. The concept of a virtual IP address is also introduced, which is the address that end hosts configure as their default gateway. One of the routers called the “Master” forwards packets on behalf of this IP address.

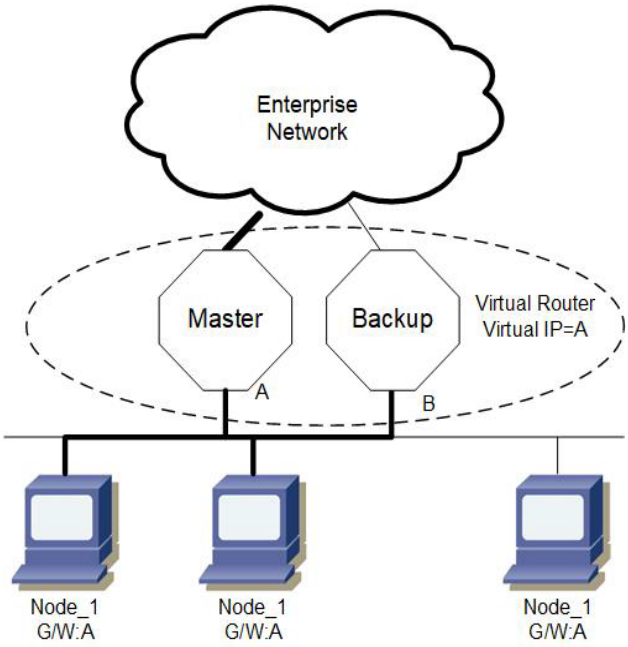


Figure 1-33: VRRP Process - Master and Backup VR

As shown in Figure 1-34, if the Master router fails, one of the other routers (Backup) assumes forwarding responsibility for it.

© 2021 IP Infusion Inc. Proprietary

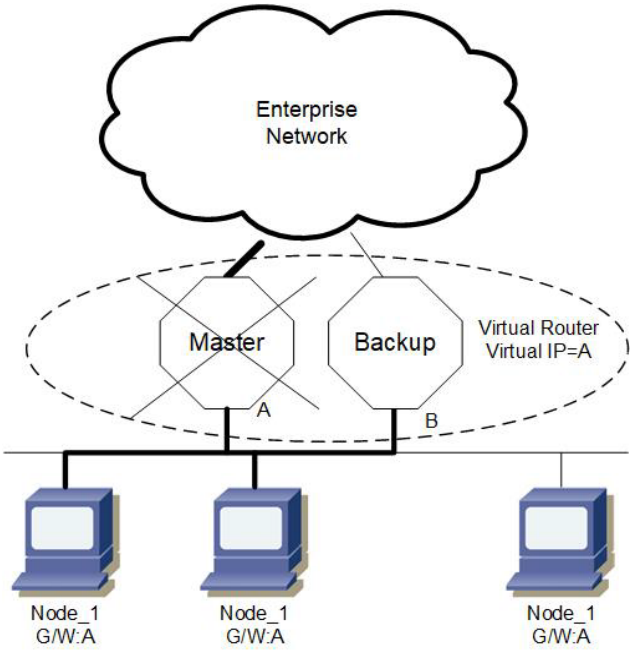


Figure 1-34: VRRP Process - Master Down and Backup Takeover

At first glance, the configuration in might not seem very useful, as it doubles the cost, and leaves one router idle at all times. This, however, can be avoided by creating two virtual routers and splitting the traffic between them.

Note: Adding a default route in the kernel on the interface that is used for VRRP might cause loss of network connectivity. According to the VRRP guidelines, when the VRRP session changes, the MAC address for the machine that attains the master state also changes. The change causes the default route from the kernel to disappear and leads to loss of connectivity. To avoid this situation, add the default route in the NSM and not in the kernel. This ensures that the default route remains on the machine across changes in the VRRP state.

To add default route through NSM, run the following command in NSM:

```
ip route 0.0.0.0/0 <IPADDRESS>
```

where `<IPADDRESS>` is the IP address of the default gateway.

Note: Use the l2-move allow-first-frame command to avoid a “double master” scenario where there is continuous MAC movement while flapping a Layer 2 switch interface that is connecting to VRRP nodes. Give the `l2-move allow-first-frame` command in both interfaces of a Layer 2 switch that is connecting to VRRP nodes.

One Virtual Router

In this configuration, the end-hosts install a default route to the IP address of virtual router 1(VRID = 1), and both routers R1 and R2 run VRRP. R1 is configured to be the Owner for virtual router 1 (VRID = 1) and R2 as a Backup for virtual router 1. If R1 fails, R2 will take over virtual router 1 and its IP addresses, and provide uninterrupted service for the hosts. Configuring only one virtual router doubles the cost, and leaves R2 idle at all times.

Topology

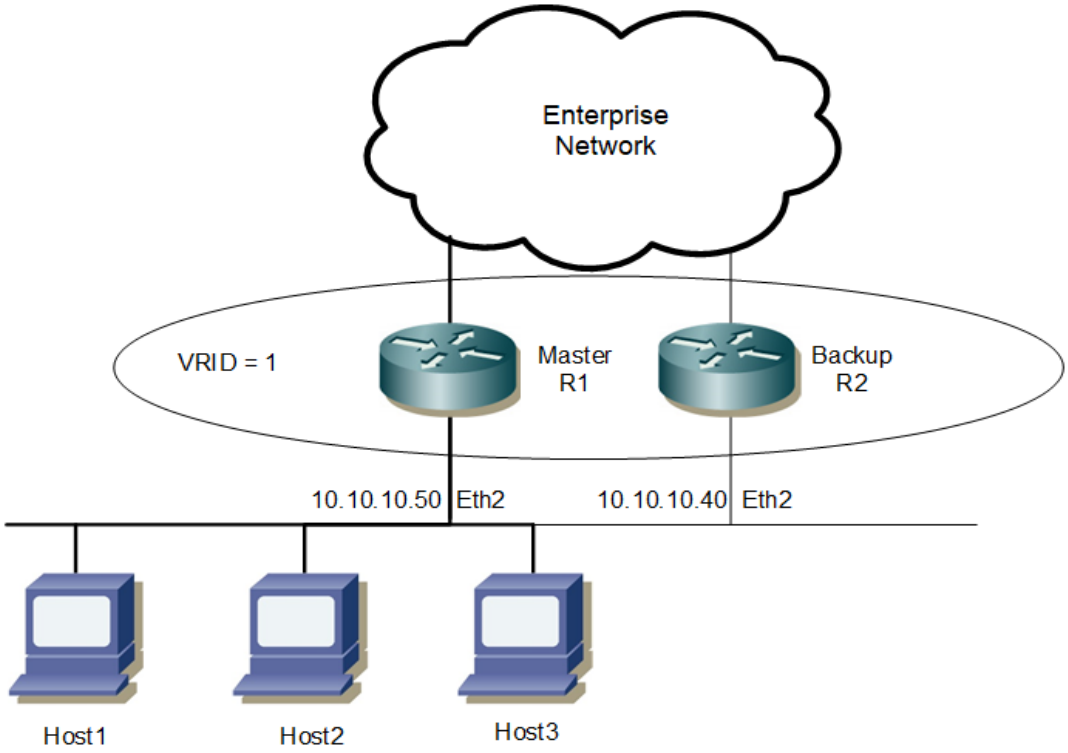


Figure 1-35: VRRP with One Virtual Router

R1

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth2`	Create a VRRP instance for interface eth2.
`(config-router)#virtual-ip 10.10.10.50 owner`	Set the virtual IP address for the VRRP session. Define the default state (owner) of the VRRP router within the virtual router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#v2-compatible`	Enable the v2-compatible
`(config-router)#authentication text abcd`	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters.
`(config-router)#enable`	Enable the VRRP session on the router.

R2

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth2`	Create a VRRP instance for interface eth2.
`(config-router)#virtual-ip 10.10.10.50`	Set the virtual IP address for the VRRP session.

© 2021 IP Infusion Inc. Proprietary

(config-router)#priority 200	Configure the priority to 200 (less than 255), because R2 is the Backup router.
(config-router)#preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
(config-router)#advertisement-interval 100	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
(config-router)#v2-compatible	Enable the v2-compatible
(config-router)#authentication text abcd	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters.
(config-router)#enable	Enable the VRRP session on the router.

Validation

R1

```
R1#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth1
 State: AdminUp   - Master
 Virtual IP address: 10.10.10.50 (Owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.50
 Operational master IP address: 10.10.10.50
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 45 seconds (4500 centi sec)
 Master uptime: 0 hours 2 minutes 34 seconds (15400 centi sec)
 Accept mode: FALSE
 Preempt mode: TRUE
 Auth-type: simple text, String: abcd
Multicast membership on IPv4 interface eth1: JOINED
V2-Compatible: TRUE


R1#
```

R2

```
R2#show vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
```

```
VRRP Id: 1 on interface: eth1
 State: AdminUp   - Backup
 Virtual IP address: 10.10.10.50 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.40
 Operational master IP address: 10.10.10.50
 Priority is 200
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 21 seconds (2100 centi sec)
 Skew time: 21 centi sec
 Master Down Interval: 380 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
Auth-type: simple text, String: abcd
Multicast membership on IPv4 interface eth1: JOINED
V2-Compatible: TRUE


R2#
```

Two Virtual Routers

In the previous, one virtual router example, R2 is not backed up by R1. This example illustrates how to back up R2 by configuring a second virtual router. In this configuration, R1 and R2 are two virtual routers, and the hosts split their traffic between R1 and R2. R1and R2 functions as backups for each other.

© 2021 IP Infusion Inc. Proprietary

Topology

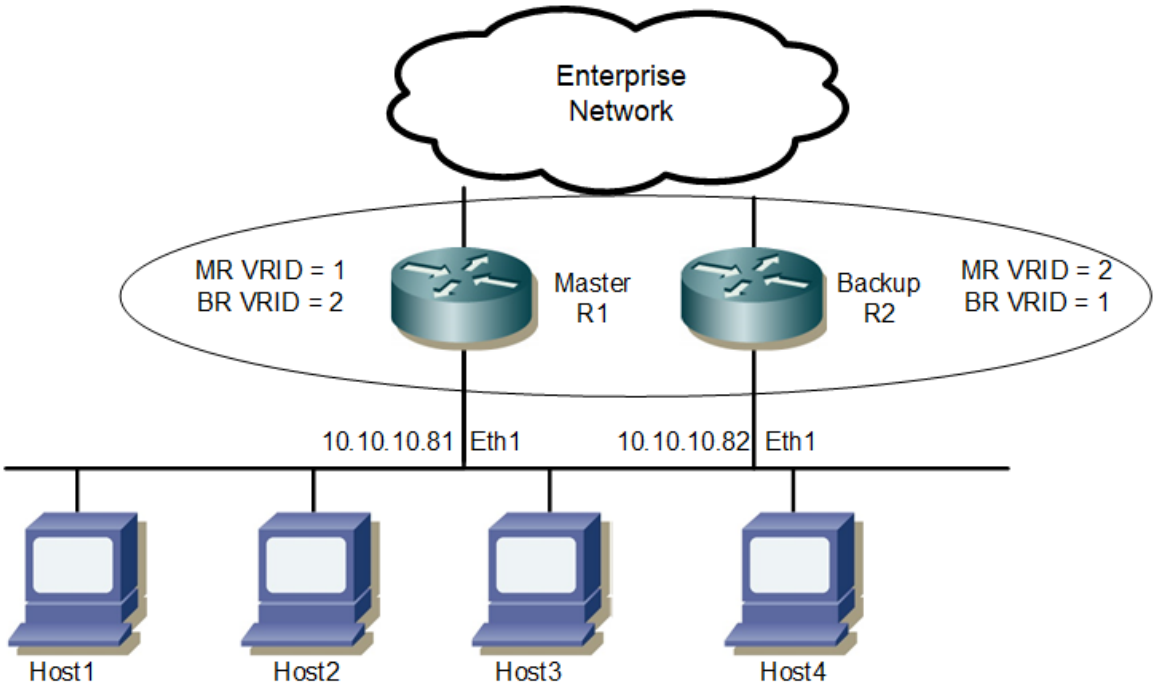


Figure 1-36: Configuring VRRP with Two Virtual Routers

R1

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth1`	Create a VRRP instance for interface eth1.
`(config-router)#virtual-ip 10.10.10.81 owner`	Set the virtual IP address for the VRRP session. Define the default state (owner) of the VRRP router within the virtual router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#v2-compatible`	Enable the v2-compatible
`(config-router)#authentication text abcd`	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters.
`(config-router)#enable`	Enable the VRRP session 1 on the router.
`(config-router)#exit`	Exit `Router` mode and enter the `Configure` mode.
`(config)#router vrrp 2 eth1`	Create a VRRP instance for interface eth1.
`(config-router)#virtual-ip 10.10.10.82`	Set the virtual IP address for the VRRP session.
`(config-router)#priority 200`	Configure the priority to 200 (less than 255), because R2 is the Backup router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.

© 2021 IP Infusion Inc. Proprietary

`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#v2-compatible`	Enable the v2-compatible
`(config-router)#authentication text abcd`	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters.
`(config-router)#enable`	Enable the VRRP session two on the router.

R2

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth1`	Create a VRRP instance for interface eth1.
`(config-router)#virtual-ip 10.10.10.81`	Set the virtual IP address for the VRRP session.
`(config-router)#priority 200`	Configure the priority to 200 (less than 255), because R2 is the Backup router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#v2-compatible`	Enable the v2-compatible
`(config-router)#authentication text abcd`	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters.
`(config-router)#enable`	Enable the VRRP session 1 on the router.
`(config-router)#exit`	Exit the `Router` mode and enter the `Configure` mode.
`(config)#router vrrp 2 eth1`	Create a VRRP instance for interface eth1
`(config-router)#virtual-ip 10.10.10.82 owner`	Set the virtual IP address for the VRRP session. Define the default state (owner) of the VRRP router within the virtual router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#v2-compatible`	Enable the v2-compatible
`(config-router)#authentication text abcd`	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters.
`(config-router)#enable`	Enable the VRRP session two on the router.

Validation

The following outputs on R1and R2 display the complete configuration for each session on R1 and R2. In session one, R1 is the master router, and in session two R2 is the master router.

R1

```
R1#sh vrrp 1 eth1
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
```


© 2021 IP Infusion Inc. Proprietary

```
Address family IPv4
VRRP Id: 1 on interface: eth1
 State: AdminUp   - Master
 Virtual IP address: 10.10.10.81 (Owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.81
 Operational master IP address: 10.10.10.81
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 1 minutes 25 seconds (8500 centi sec)
 Master uptime: 0 hours 2 minutes 34 seconds (15400 centi sec)
 Accept mode: FALSE
 Preempt mode: TRUE
 Auth-type: simple text, String: abcd
 Multicast membership on IPv4 interface eth1: JOINED
 V2-Compatible: TRUE


R1#sh vrrp 2 eth1
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 2 on interface: eth1
 State: AdminUp   - Backup
 Virtual IP address: 10.10.10.82 (Not-owner)
 Virtual MAC address is 0000.5e00.0102
 Operational primary IP address: 10.10.10.81
 Operational master IP address: 10.10.10.82
 Priority is 200
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 2 minutes 3 seconds (12300 centi sec)
 Skew time: 21 centi sec
 Master Down Interval: 380 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Auth-type: simple text, String: abcd
 Auth-type: simple text, String: abcd
 Multicast membership on IPv4 interface eth1:
 JOINED V2-Compatible: TRUE


R1#
```

R2

```
R2#sh vrrp 1 eth1
VRRP Version: 3
```

```
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth1
 State: AdminUp   - Backup
 Virtual IP address: 10.10.10.81 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.10.10.82
 Operational master IP address: 10.10.10.81
 Priority is 200
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 37 seconds (3700 centi sec)
 Skew time: 21 centi sec
 Master Down Interval: 380 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Auth-type: simple text, String: abcd
 Multicast membership on IPv4 interface eth1:
 JOINED V2-Compatible: TRUE


R2#sh vrrp 2 eth1
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 2 on interface: eth1
 State: AdminUp   - Master
 Virtual IP address: 10.10.10.82 (Owner)
 Virtual MAC address is 0000.5e00.0102
 Operational primary IP address: 10.10.10.82
 Operational master IP address: 10.10.10.82
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 12 seconds (1200 centi sec)
 Master uptime: 0 hours 2 minutes 34 seconds (15400 centi sec)
 Accept mode: FALSE
 Preempt mode: TRUE
 Auth-type: simple text, String: abcd
 Multicast membership on IPv4 interface eth1:
 JOINED V2-Compatible: TRUE


R2#
```


© 2021 IP Infusion Inc. Proprietary

Two Backup Routers

In this configuration, Host B could be a gateway router. As such, interface eth1 on Routers R1, R2, and R3, and the gateway router, would run the IGP protocol.

Topology

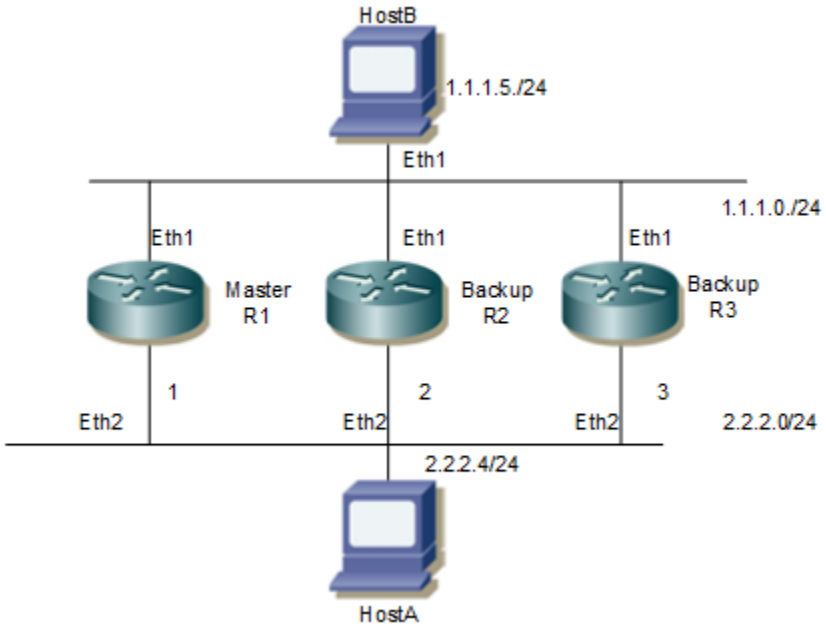


Figure 1-37: Configuring VRRP with Two Backup Routers

R1

`#configure terminal`	Enter the Configure mode.
`(config)#interface eth2`	Enter interface mode for eth2.
`(config-if)#ip address 2.2.2.1/24`	Configure the IP address for interface eth2 to be in network 0.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Enter interface mode for eth1.
`(config-if)#ip address 1.1.1.1/24`	Configure the IP address for interface eth1 to be in network 1.
`(config-if)#exit`	Exit interface mode.
`(config)#router vrrp 1 eth2`	Create a VRRP instance for interface eth2.
`(config-router)#virtual-ip 2.2.2.1 owner`	Configure R1 as the owner.
`(config-router)#advertisement-interval 100`	Configure the default value for the advertisement interval. The configurable range is 5 to 4095 centi seconds (value must be a multiple of 5).
`(config-router)#preempt-mode true`	Set `true` as the default value for the field.
`(config-router)#v2-compatible`	Enable the v2-compatible

© 2021 IP Infusion Inc. Proprietary

`(config-router)#authentication text abcd`	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters.
`(config-router)#enable`	Enable the VRRP session on the router.
`(config-router)#exit`	Exit Router mode.

R2

`(config)#configure terminal`	Enter the Configure mode.
`(config)#interface eth2`	Enter interface mode for eth2.
`(config-if)#ip address 2.2.2.2/24`	Configure the IP address for interface eth2 to be in network 0.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ip address 1.1.1.2/24`	Configure the IP address for interface `eth1` to be in network 1.
`(config-if)#exit`	Exit interface mode.
`(config)#router vrrp 1 eth2`	Create a VRRP instance for interface eth2.
`(config-router)#virtual-ip 2.2.2.1`	Configure R2 as the backup.
`(config-router)#advertisement-interval 100`	Configure the default value for the advertisement interval. The configurable range is 5 to 4095 centi seconds (value must be a multiple of 5).
`(config-router)#priority 100`	Set the default value for the backup router.
`(config-router)#preempt-mode true`	Set `true` as the default value for the field.
`(config-router)#v2-compatible`	Enable the v2-compatible
`(config-router)#authentication text abcd`	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters.
`(config-router)#enable`	Enable the VRRP session on the router.
`(config-router)#exit`	Exit Router mode.

R3

`#configure terminal`	Enter the Configure mode.
`(config)#interface eth2`	Enter interface mode for eth2.
`(config-if)#ip address 2.2.2.3/24`	Configure the IP address for interface eth2 to be in network 0.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Enter interface mode for eth1.
`(config-if)#ip address 1.1.1.3/24`	Configure the IP address for interface eth1 to be in network 1.
`(config-if)#exit`	Exit interface mode.
`(config)#router vrrp 1 eth2`	Create a VRRP instance for interface eth2.
`(config-router)#virtual-ip 2.2.2.1`	Configure R3 as the backup.
`(config-router)#advertisement-interval 100`	Configure the default value for the advertisement interval. The configurable range is 5 to 4095 centi seconds (value must be a multiple of 5).

© 2021 IP Infusion Inc. Proprietary

`(config-router)#priority 254`	Configure the priority for R3. The configurable range is 1-255.
`(config-router)#preempt-mode true`	Set `true` as the default value for the field.
`(config-router)#v2-compatible`	Enable the v2-compatible
`(config-router)#authentication text abcd`	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters.
`(config-router)#enable`	Enable the VRRP session on the router.
`(config-router)#exit`	Exit Router mode.

Validation

Router 1

```
R1#show vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Master
 Virtual IP address: 2.2.2.1 (Owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 2.2.2.1
 Operational master IP address: 2.2.2.1
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 9 minutes 6 seconds (54600 centi sec)
 Master uptime: 0 hours 2 minutes 34 seconds (15400 centi sec)
 Accept mode: FALSE
 Preempt mode: TRUE
 Auth-type: simple text, String: abcd
 Multicast membership on IPv4 interface eth2: JOINED
 V2-Compatible: TRUE
```

Router 2

```
R2#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Backup
 Virtual IP address: 2.2.2.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 2.2.2.2
 Operational master IP address: 2.2.2.1
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 11 minutes 28 seconds (68800 centi sec)
```

```
 Skew time: 60 centi sec
 Master Down Interval: 380 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Auth-type: simple text, String: abcd
 Multicast membership on IPv4 interface eth2: JOINED
 V2-Compatible: TRUE
```

Router 3

```
R3#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Backup
 Virtual IP address: 2.2.2.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 2.2.2.3
 Operational master IP address: 2.2.2.1
 Priority is 254
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 14 minutes 23 seconds (86300 centi sec)
 Skew time: 0 centi sec
 Master Down Interval: 380 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Auth-type: simple text, String: abcd
 Multicast membership on IPv4 interface eth2: JOINED
 V2-Compatible: TRUE
```

Ping Output at Host A

```
HOSTA#ping 1.1.1.5
Press CTRL+C to exit
PING 1.1.1.5 (1.1.1.5) 56(84) bytes of data.
64 bytes from 1.1.1.5: icmp_seq=1 ttl=63 time=1.40 ms
64 bytes from 1.1.1.5: icmp_seq=2 ttl=63 time=1.09 ms
```

Disabling the Master/Owner

`#configure terminal`	Enter the Configure mode.
`(config)#router vrrp 1 eth2`	Create a VRRP instance for interface eth2.
`(config-router)#disable`	Disable the VRRP session.

Output After Disabling the Master

Router 1

```
R1#sh vrrp
VRRP Version: 3
VMAC enabled
```


© 2021 IP Infusion Inc. Proprietary

```
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminDown - Init (admin state down)
 Virtual IP address: 2.2.2.1 (Owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 2.2.2.1
 Operational master IP address: 2.2.2.1
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 0 minutes 0 seconds (0 centi sec)
 Skew time: 0 centi sec
 Master Down Interval: 380 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Auth-type: simple text, String: abcd
 Multicast membership on IPv4 interface eth2: JOINED
 V2-Compatible: TRUE
```

Router 3

```
R3#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Master
 Virtual IP address: 2.2.2.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 2.2.2.3
 Operational master IP address: 2.2.2.3
 Priority is 254
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 40 minutes 55 seconds (245500 centi sec)
 Master uptime: 0 hours 2 minutes 34 seconds (15400 centi sec)
 Accept mode: FALSE
 Preempt mode: TRUE
 Auth-type: simple text, String: abcd
 Multicast membership on IPv4 interface eth2: JOINED
 V2-Compatible: TRUE

HOSTA#ping 1.1.1.5
Press CTRL+C to exit
PING 1.1.1.5 (1.1.1.5) 56(84) bytes of data.
64 bytes from 1.1.1.5: icmp_seq=1 ttl=63 time=1.40 ms
64 bytes from 1.1.1.5: icmp_seq=2 ttl=63 time=1.09 m
```

Interface Tracking

The need for VRRP Interface Tracking arose because VRRPv3 was unable to track the gateway interface status. The VRRP Interface Tracking feature provides dynamic failover of an entire circuit, in the event that one member of the group fails. It introduces the concept of a circuit, where two or more Virtual Routers on a single system can be grouped. In the event that a failure occurs, and one of the Virtual Routers performs the Master to Backup transition, the other Virtual Routers in the group are notified, and are forced into the Master to Backup transition, so that both incoming and outgoing packets are routed through the same gateway router, eliminating the problem for Firewall/NAT environments.

Note: VRRP Interface Tracking feature allows you to track the state of an upstream Interface and update the VRRP router priority accordingly. Up to 5 interfaces can be tracked per VRRP session for upstream interfaces and Interface tracking will be disabled when the session is the owner of the VIP.

To configure VRRP Interface Tracking, each circuit is configured to have a corresponding priority-delta value, which is passed to VRRP when a failure occurs. The priority of each Virtual Router on the circuit is decremented by the priority-delta value, causing the VR Master to VR Backup transition.

In this example, two routers, R1 and R2, are configured as backup routers with different priorities. The priority-delta value is configured to be greater than the difference of both the priorities. R1 is configured to have a priority of 150, and R2 has a priority of 50. R1, with a greater priority, is the Virtual Router Master. The priority-delta value is 110, greater than 100 (150 minus 50). On R1, when the external interface xe41, xe50/1 and xe50/2 fails, the priority of R1 becomes 40 (150 minus 110). Since R2 has a greater priority (50) than R1, R2 becomes the VR Master, and routing of packages continues without interruption. When this VR Backup (R1) is up again, it regains its original priority (150), and becomes the VR Master again.

© 2021 IP Infusion Inc. Proprietary

Topology

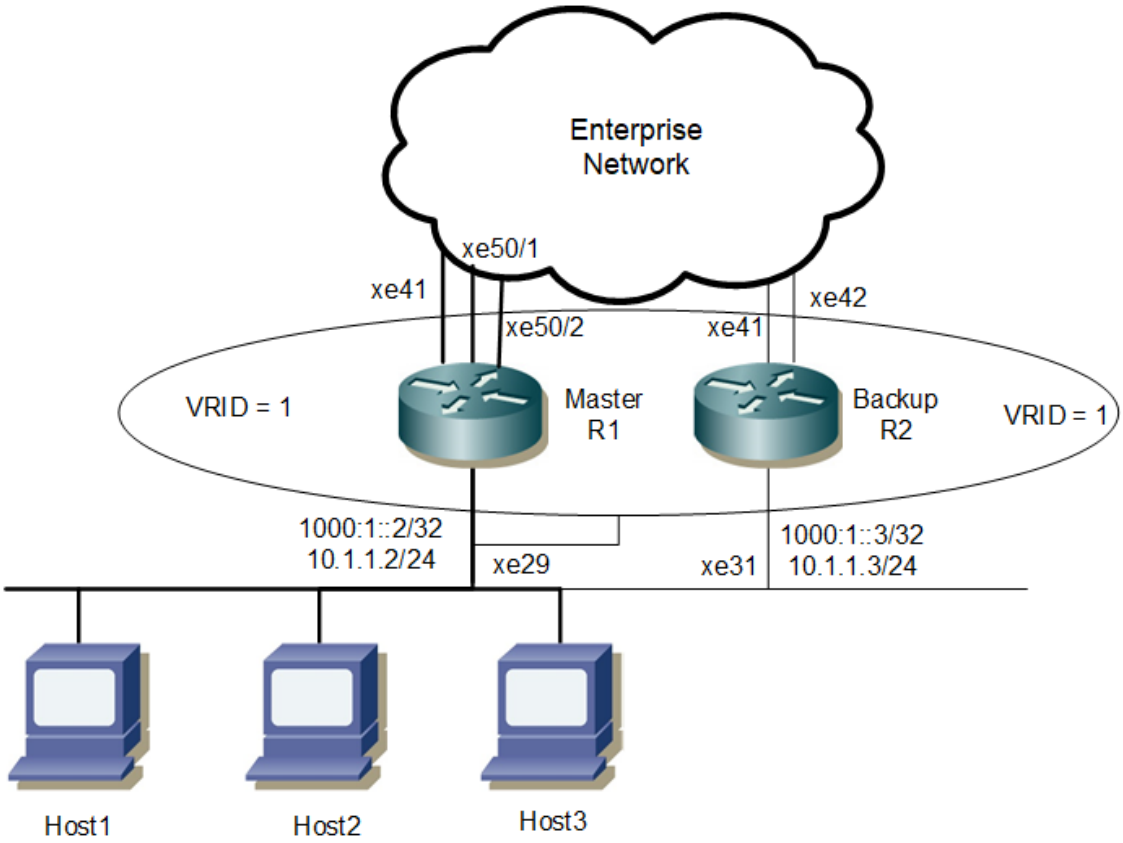


Figure 1-38: VRRP Interface Tracking

R1

`(config)#configure terminal`	Enter the `Configure` mode.
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN aware bridge.
`(config)#vlan 1001-1002 bridge 1`	Create VLAN 1001,1002 and map it to bridge 1.
`(config)#interface xe29`	Enter interface mode.
`(config-if)#switchport`	Configure switch port.
`(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group to l2 interface with spanning-tree Disable.
`(config-if)#switchport mode trunk`	Configure switch port mode as trunk.
`(config-if)#switchport trunk allowed vlan add 1001,1002`	Allow vlan 1001 ,1002 on the interface.
`(config-if)#interface vlan1.1001`	Enter the vlan interface
`(config-if)#ip address 10.1.1.2/24`	Configure ipv4 address
`(config-if)#ipv6 address 1000:1::2/32`	Configure ipv6 address
`(config-if)#ipv6 router ospf area 0.0.0.0`	Tag ospfv3 instance on interface with area 0
`(config-if)#exit`	Exit the interface mode
`(config)#router vrrp 1 vlan1.1001`	Create a new ipv4 VRRP instance for interface vlan1.1001

© 2021 IP Infusion Inc. Proprietary

(config-router)#virtual-ip 10.1.1.1	Set the virtual IP address for the VRRP session
(config-router)#priority 150	Configure the priority to 150
(config-router)#circuit-failover xe41 70	Configure the priority-delta value to be 70. In case of failover, this priority-delta value is subtracted from the current VR Master.
(config-router)#circuit-failover xe50/1 10	Configure the priority-delta value to be 10. In case of failover, this priority-delta value is subtracted from the current VR Master.
(config-router)#circuit-failover xe50/2 30	Configure the priority-delta value to be 10. In case of failover, this priority-delta value is subtracted from the current VR Master.
(config-router)#v2-compatible	Enable the v2-compatible
(config-router)#authentication text abcd	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters.
(config-router)#enable	Enable the VRRP session on the router.
(config-router)#exit	Exit the router mode.
(config)#router ipv6 vrrp 1 vlan1.1001	Create a new ipv6 VRRP instance for interface vlan1.1001.
(config-router)#virtual-ipv6 fe80::1	Set the virtual IPv6 address for the VRRP session.
(config-router)#priority 150	Configure the priority to 150
(config-router)#circuit-failover xe41 70	Configure the priority-delta value to be 70. In case of failover, this priority-delta value is subtracted from the current VR Master.
(config-router)#circuit-failover xe50/1 10	Configure the priority-delta value to be 10. In case of failover, this priority-delta value is subtracted from the current VR Master.
(config-router)#circuit-failover xe50/2 30	Configure the priority-delta value to be 10. In case of failover, this priority-delta value is subtracted from the current VR Master.
(config-router)#enable	Enable the VRRP session on the router.
(config-router)#exit	Exit the router mode
(config)#interface xe50/1	Enter interface mode
(config-if)#ip address 20.1.1.1/24	Configure ipv4 address
(config-if)#ipv6 address 2000::1/64	Configure ipv6 address
(config-if)#ipv6 router ospf area 0.0.0.0	Tag ospfv3 instance on interface with area 0
(config-if)#interface xe50/2	Enter interface mode
(config-if)#ip address 30.1.1.1/24	Configure ipv4 address
(config-if)#ipv6 address 3000::1/64	Configure ipv6 address
(config-if)#ipv6 router ospf area 0.0.0.0	Tag ospfv3 instance on interface with area 0
(config-if)#interface xe41	Enter interface mode
(config-if)#ip address 60.1.1.1/24	Configure ipv4 address
(config-if)#ipv6 address 6000::1/64	Configure ipv6 address
(config-if)#ipv6 router ospf area 0.0.0.0	Tag ospfv3 instance on interface with area 0
(config-if)#exit	Exit interface and configure mode

© 2021 IP Infusion Inc. Proprietary

R2

(config)#bridge 1 protocol rstp vlan-bridge	Create a RSTP VLAN aware bridge with bridge-id.
(config)#vlan 1001-1002 bridge 1	Create VLAN 1001,1002 and map it to bridge 1
(config)#interface xe31	Enter interface mode
(config-if)#switchport	Configure switch port
(config-if)#bridge-group 1 spanning-tree disable	Configure bridge group to l2 interface with spanning-tree Disable
(config-if)#switchport mode trunk	Configure switch port mode as trunk
(config-if)#switchport trunk allowed vlan add 1001,1002	Allow vlan 1001 ,1002 on the interface
(config-if)#interface vlan1.1001	Enter the vlan interface
(config-if)#ip address 10.1.1.3/24	Configure ipv4 address
(config-if)#ipv6 address 1000:1::3/32	Configure ipv6 address
(config-if)#ipv6 router ospf area 0.0.0.0	Tag ospfv3 instance on interface with area 0
(config-if)#exit	Exit interface mode
(config)#router vrrp 1 vlan1.1001	Create a router ipv4 VRRP instance for interface vlan1.1001.
(config-router)#virtual-ip 10.1.1.1	Set the virtual IP address for the VRRP session.
(config-router)#priority 50	Configure the priority to 50 (less than 150), because R2 is the VR Backup router.
(config-router)#v2-compatible	Enable the v2-compatible
(config-router)#authentication text abcd	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters.
(config-router)#enable	Enable the VRRP session
(config-router)#exit	Exit the router mode
(config)#router ipv6 vrrp 1 vlan1.1001	Create a router ipv6 VRRP ipv6 instance for interface vlan1.1001.
(config-router)#virtual-ipv6 fe80::1	Set the virtual IPv6 address for the VRRP session.
(config-router)#priority 50	Configure the priority to 50 (less than 150), because R2 is the VR Backup router.
(config-router)#exit	Exit the router mode
(config)#interface xe41	Enter interface mode
(config-if)#ip address 80.1.1.1/24	Configure ipv4 address
(config-if)#ipv6 address 8000::1/64	Configure ipv6 address
(config-if)#ipv6 router ospf area 0.0.0.0	Tag ospfv3 instance on interface with area 0
(config-if)#interface xe42	Enter interface mode
(config-if)#ip address 90.1.1.1/24	Enter the tracked interface
(config-if)#ipv6 address 9000::1/64	Configure ipv6 address
(config-if)#ipv6 router ospf area 0.0.0.0	Tag ospfv3 instance on interface with area 0
(config-if)#exit	Exit interface and configure mode

© 2021 IP Infusion Inc. Proprietary

Validation

```
R1# show vrrp 1 vlan1.1001
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv4
VRRP Id: 1 on interface: vlan1.1001
 State: AdminUp   - Master
 Virtual IP address: 10.1.1.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.1.1.2
 Operational master IP address: 10.1.1.2
 Configured priority: 150, Current priority: 150
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 1 minutes 12 seconds (7200 centi sec)
 Master uptime: 0 hours 2 minutes 34 seconds (15400 centi sec)
 Accept mode: TRUE
 Preempt mode: TRUE
 Monitored circuit: xe41, Priority Delta: 70, Status: UP
 Monitored circuit: xe50/1, Priority Delta: 10, Status: UP
 Monitored circuit: xe50/2, Priority Delta: 30, Status: UP
Auth-type: simple text, String: abcd
Multicast membership on IPv4 interface vlan1.1001: JOINED V
2-Compatible: TRUE

R1#
R2#show vrrp 1 vlan1.1001
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv4
VRRP Id: 1 on interface: vlan1.1001
 State: AdminUp   - Backup
 Virtual IP address: 10.1.1.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.1.1.3
 Operational master IP address: 10.1.1.2
 Priority is 50
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 7 hours 52 minutes 53 seconds (2837300 centi sec)
 Skew time: 80 centi sec
 Master Down Interval: 380 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Auth-type: simple text, String: abcd
 Multicast membership on IPv4 interface vlan1.1001: JOINED
 V2-Compatible: TRUE

R2#
R1#show vrrp ipv6 1 vlan1.1001
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
```


© 2021 IP Infusion Inc. Proprietary

```
Address family IPv6
VRRP Id: 1 on interface: vlan1.1001
 State: AdminUp   - Master
 Virtual IP address: fe80::1 (Not-owner)
 Virtual MAC address is 0000.5e00.0201
 Operational primary IP address: fe80::ba6a:97ff:fe3c:de9d
 Operational master IP address: fe80::ba6a:97ff:fe3c:de9d
 Configured priority: 150, Current priority: 150
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 3 minutes 54 seconds (23400 centi sec)
 Master uptime: 0 hours 2 minutes 34 seconds (15400 centi sec)
 Accept mode: TRUE
 Preempt mode: TRUE
 Monitored circuit: xe41, Priority Delta: 70, Status: UP
 Monitored circuit: xe50/1, Priority Delta: 10, Status: UP
 Monitored circuit: xe50/2, Priority Delta: 30, Status: UP
 Multicast membership on IPv6 interface  vlan1.1001: JOINED
 V2-Compatible: FALSE
R1#
R2#show vrrp ipv6 1 vlan1.1001
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv6
VRRP Id: 1 on interface: vlan1.1001
 State: AdminUp   - Backup
 Virtual IP address: fe80::1 (Not-owner)
 Virtual MAC address is 0000.5e00.0201
 Operational primary IP address: fe80::82a2:35ff:fe35:135f
 Operational master IP address: fe80::ba6a:97ff:fe3c:de9d
 Priority is 50
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 7 hours 55 minutes 11 seconds (2851100 centi sec)
 Skew time: 80 centi sec
 Master Down Interval: 380 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv6 interface  vlan1.1001: JOINED
 V2-Compatible: FALSE
R2#
```

After shut down of all tracked interfaces (xe50/1, xe50/2 and xe41) in R1:

```
R1#show vrrp 1 vlan1.1001
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv4
VRRP Id: 1 on interface: vlan1.1001
 State: AdminUp   - Backup
 Virtual IP address: 10.1.1.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.1.1.2
 Operational master IP address: 10.1.1.3
 Configured priority: 150, Current priority: 40
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
```

```
 Virtual router uptime: 0 hours 7 minutes 46 seconds (46600 centi sec)
 Skew time: 84 centi sec
 Master Down Interval: 380 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Monitored circuit: xe41, Priority Delta: 70, Status: DOWN
 Monitored circuit: xe50/1, Priority Delta: 10, Status: DOWN
 Monitored circuit: xe50/2, Priority Delta: 30, Status: DOWN
 Auth-type: simple text, String: abcd
Multicast membership on IPv4 interface vlan1.1001: JOINED
V2-Compatible: TRUE
R1#
R2#show vrrp 1 vlan1.1001
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv4
VRRP Id: 1 on interface: vlan1.1001
 State: AdminUp   - Master
 Virtual IP address: 10.1.1.1 (Not-owner)
 Virtual MAC address is 0000.5e00.0101
 Operational primary IP address: 10.1.1.3
 Operational master IP address: 10.1.1.3
 Priority is 50
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 7 hours 57 minutes 41 seconds (2866100 centi sec)
 Master uptime: 0 hours 2 minutes 34 seconds (15400 centi sec)
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface vlan1.1001: JOINED
 V2-Compatible: FALSE
R2#
R1#show vrrp ipv6 1 vlan1.1001
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv6
VRRP Id: 1 on interface: vlan1.1001
 State: AdminUp   - Backup
 Virtual IP address: fe80::1 (Not-owner)
 Virtual MAC address is 0000.5e00.0201
 Operational primary IP address: fe80::ba6a:97ff:fe3c:de9d
 Operational master IP address: fe80::82a2:35ff:fe35:135f
 Configured priority: 150, Current priority: 40
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 0 hours 8 minutes 43 seconds (52300 centi sec)
 Skew time: 84 centi sec
 Master Down Interval: 380 centi sec
 Accept mode: TRUE
 Preempt mode: TRUE
 Monitored circuit: xe41, Priority Delta: 70, Status: DOWN
 Monitored circuit: xe50/1, Priority Delta: 10, Status: DOWN
 Monitored circuit: xe50/2, Priority Delta: 30, Status: DOWN
 Multicast membership on IPv6 interface  vlan1.1001: JOINED
 V2-Compatible: FALSE
```

 © 2021 IP Infusion Inc. Proprietary

```
R1#
R2#show vrrp ipv6 1 vlan1.1001
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv6
VRRP Id: 1 on interface: vlan1.1001
 State: AdminUp   - Master
 Virtual IP address: fe80::1 (Not-owner)
 Virtual MAC address is 0000.5e00.0201
 Operational primary IP address: fe80::82a2:35ff:fe35:135f
 Operational master IP address: fe80::82a2:35ff:fe35:135f
 Priority is 50
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Virtual router uptime: 7 hours 59 minutes 4 seconds (2874400 centi sec)
 Master uptime: 0 hours 2 minutes 34 seconds (15400 centi sec)
 Accept mode: TRUE
 Preempt mode: TRUE
 Multicast membership on IPv6 interface  vlan1.1001: JOINED
 V2-Compatible: FALSE
R2#
```

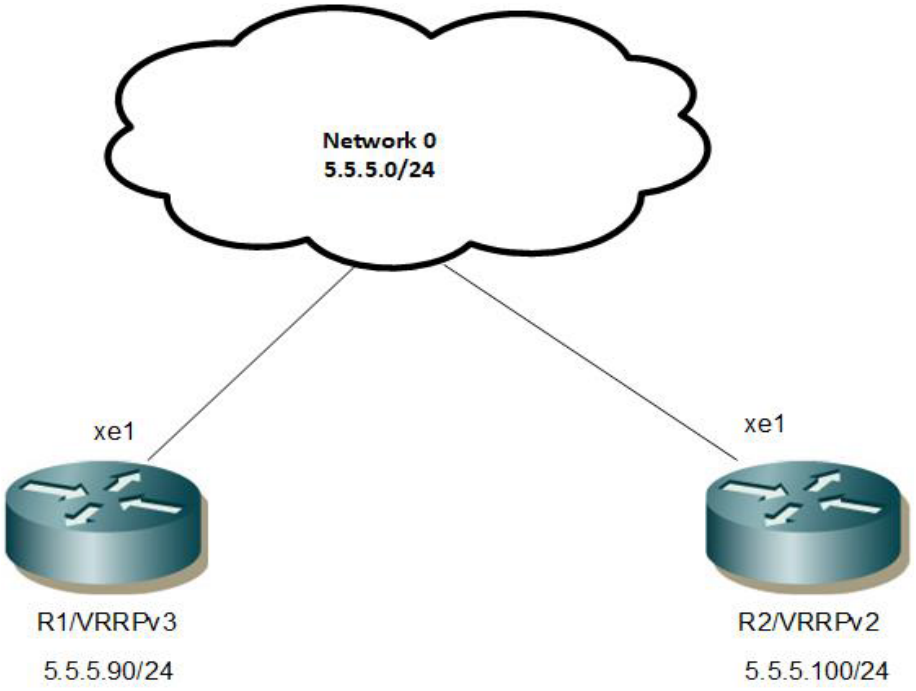
VRRP-Backward Compatibility

This section contains VRRP Backward Compatibility configuration examples.

The backward compatibility feature which implements version 3 of VRRP protocol recognizes the presence of VRRP version 2 compatible routers in the network and performs all operations normally. This support is intended for upgrade scenarios and is not recommended for permanent deployments. This should only occur when a router is transitioning from VRRPv2 to VRRPv3.

VRRP Backward Compatibility is applicable only for VRRP IPv4.

Topology



R1

`#configure terminal`	Enter the Configure mode.
`(config)# interface xe1`	Enter Interface configuration mode.
`(config-if)# ip address 5.5.5.90/24`	Configure IP address on the interface.
`(config-if)#exit`	Exit from configuration mode.
`(config)# router vrrp 1 xe1`	Configure VRRP on DUT with Virtual router Identifier as 1 on the interface xe1.
`(config-router)#virtual-ip 5.5.5.190`	Configure Virtual-IP address as the interface IP address of Owner which is not actually present in the LAN.
`(config-router)#v2-compatible`	Enable the v2-compatible
`(config-router)#authentication text abcd`	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters
`(config-router)#enable`	Enable VRRP session on DUT.
`(config-router)#exit`	Exit router VRRP mode.
`(config)#vrrp compatible-v2 enable`	Enable VRRP-Backward compatibility feature on a VRRPv3 running router.

R2

`#configure terminal`	Enter the Configure mode.
`(config)# interface xe1`	Enter Interface configuration mode.
`(config-if)# ip address 5.5.5.100/24`	Configure IP address on the interface.
`(config-if)#exit`	Exit from configuration mode.

© 2021 IP Infusion Inc. Proprietary

(config)#router vrrp 1 xe1	Configure VRRP on DUT with Virtual router Identifier as 1 on the interface xe1.
(config-router)#virtual-ip 5.5.5.190	Configure Virtual-IP address as the interface IP address of Owner which is not actually present in the LAN.
(config-router)#v2-compatible	Enable the v2-compatible
(config-router)#authentication text abcd	Configure the authentication text to specify that as simple text for vrrpv2 packets, accept only 8 characters
(config-router)#enable	Enable VRRP session on DUT.
(config-router)#end	Exit router VRRP mode.

Validation

R1

```
OcNOS#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility enabled

Address family IPv4
VRRP Id: 1 on interface: xe1
State: AdminUp  - Master
Virtual IP address: 5.5.5.190 (Not-owner)
Virtual MAC address is 0000.5e00.0101
Operational primary IP address: 5.5.5.90
Operational master IP address: 5.5.5.90
Priority is 100
Advertisement interval: 100 centi sec
Master Advertisement interval: 100 centi sec
Virtual router uptime: 0 hours 2 minutes 32 seconds (15200 centi sec)
Master uptime: 0 hours 2 minutes 28 seconds (14800 centi sec)
Accept mode: TRUE
Preempt mode: TRUE
Auth-type: simple text, String: abcd
Multicast membership on IPv4 interface xe1: JOINED
V2-Compatible: TRUE
```

R2

```
OcNOS#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: xe1
State: AdminUp   - Backup
Virtual IP address: 5.5.5.190 (Not-owner)
Virtual MAC address is 0000.5e00.0101
Operational primary IP address: 5.5.5.100
Operational master IP address: 5.5.5.90
```

```
Priority is 100
Advertisement interval: 100 centi sec
Master Advertisement interval: 100 centi sec
Virtual router uptime: 0 hours 1 minutes 11 seconds (7100 centi sec)
Skew time: 60 centi sec
Master Down Interval: 360 centi sec
Accept mode: TRUE
Preempt mode: TRUE
Auth-type: simple text, String: abcd
Multicast membership on IPv4 interface xe1: JOINED
V2-Compatible: TRUE
```

Redundancy Using VRRP and OSPF: Two Virtual Routers

This example illustrates a configuration of two routers between two end-hosts. R1 and R2 are two virtual routers functioning as backups for each other, with VRRP running on the 10.10.12.0/24 network (LAN), and OSPF running on the 10.10.10.0/24 network (ISP).

Topology

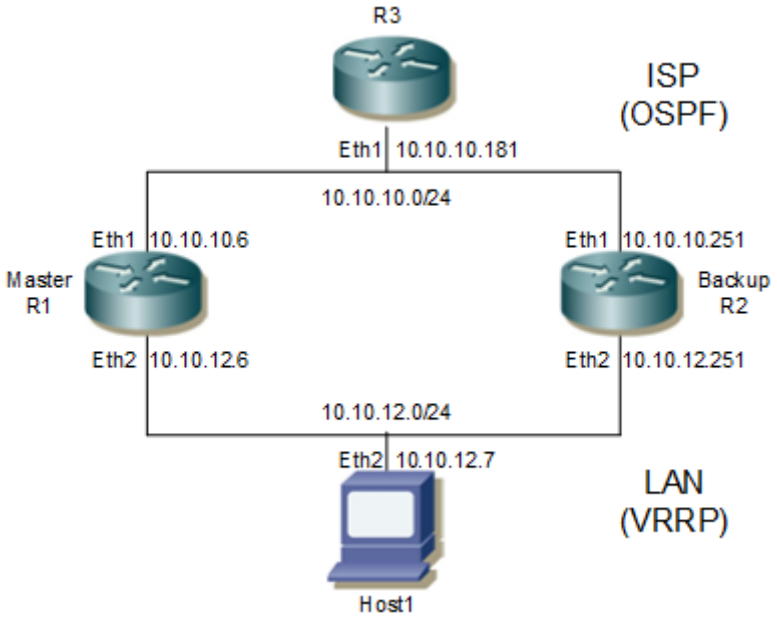


Figure 1-39: Redundancy Using VRRP and OSPF

In Figure 1-39:

- R3 is an OSPF router representing an OSPF network to an ISP.
- R1 is the VRRP Master/OSPF router.
- R2 is the VRRP Backup/OSPF router.
- Host 1 is an end-host.

VRRP handles any failure of the Master's link to the LAN. Failures in the OSPF network that could cause the Master to lose routing information would cause packets from Host 1 that are targeted for R3 to be dropped. Running VRRP on

© 2021 IP Infusion Inc. Proprietary

the OSPF network to create redundancy is undesirable, because doing so would cause erroneous VRRP packets to be sent to the ISP.

An alternative method to achieve redundancy is to run OSPF on the LAN side. By running OSPF on the LAN, any routing information lost by the Master would be regained from the Backup on the LAN interface, resulting in ICMP redirects to R2 for traffic received from Host 1. To reduce OSPF control traffic, R1 and R2 are configured as Area Border Routers (ABR), and the LAN is configured as a stub network to reduce LSA advertisement traffic on the LAN. Before enabling OSPF on the LAN, verify that VRRP is running with R1 as the Master and R2 as the Backup.

```
R1#show vrrp
 VrId <1>
 State is Master
 Virtual IP is 10.10.12.6 (IP owner)
 Interface is eth1
 Priority is 255
 Advertisement interval: 5 centi sec
 Preempt mode is TRUE
R2#show vrrp
 VrId <1>
  State is Backup
  Virtual IP is 10.10.12.6 (Not IP owner)
  Interface is eth1
  Priority is 100
  Advertisement interval: 5 centi sec
  Preempt mode is TRUE
```

Steps to configure OSPF on the LAN are given below.

R3

`#configure terminal`	Enter the Configure mode.
`(config)#router ospf 1`	Configure the routing process and specify the process ID (`1`). The process ID should be a unique integer.
`(config-router)#ospf router-id 10.10.10.181`	Specify the OSPF router ID.
`(config-router)#timers spf exp 0 0`	Set `timers` to minimum time for quick convergence.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs and associate the area ID (0).

R1

`#configure terminal`	Enter the Configure mode.
`(config)#router ospf 1`	Configure the routing process and specify the process ID (`1`). The process ID should be a unique integer.
`(config-router)#ospf router-id 10.10.12.6`	Specify the OSPF router ID.
`(config-router)#area 1 stub`	Define area 1 as a stub network.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs and associate the area ID (0).
`(config-router)#network 10.10.12.0/24 area 1`	Define the other interface (`10.10.12.0/24`) on which OSPF runs and associate the area ID (`1`)

R2

`#configure terminal`	Enter the Configure mode.
`(config)#router ospf 1`	Configure the routing process, and specify the process ID (`1`). The process ID should be a unique integer
`(config-router)#ospf router-id 10.10.12.251`	Specify the OSPF router ID.
`(config-router)#area 1 stub`	Define area 1 as a stub network.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs and associate the area ID (`0`).
`(config-router)#network 10.10.12.0/24 area 1`	Define the other interface (`10.12.10.0/24`) on which OSPF runs and associate the area ID (`1`)

Verification

1. Set gateway on the end-host (statically):

```
(root@host1)#route add -net 10.10.10.0 netmask 255.255.255.0 gw 10.10.12.6
```

2. Verify end-host reachability via traceroute:

```
(root@host1)#traceroute 10.10.10.181
traceroute to 10.10.10.181 (10.10.10.181), 30 hops max, 38 byte packets
1 10.10.12.6 (10.10.12.6) 0.835 ms 0.350 ms 0.341 ms
2 10.10.10.181 (10.10.10.181) 9.557 ms 0.572 ms 0.545 ms
```

3. Bring down eth2 of R1:

```
[root@r1 sbin]#ifconfig eth2 down
```

4. Verify end-host reachability via traceroute:

```
(root@host1)#traceroute 10.10.10.181
traceroute to 10.10.10.181 (10.10.10.181), 30 hops max, 38 byte packets
1 10.10.12.6 (10.10.12.6) 0.461 ms 0.352 ms 0.334 ms
2 10.10.12.251 (10.10.12.251) 0.425 ms 0.432 ms 0.410 ms
3 10.10.10.181 (10.10.10.181) 0.691 ms 0.639 ms 0.607 ms
```

5. Bring up eth2 of R1:

```
[root@r1 sbin]#ifconfig eth2 up
```

6. Verify end-host reachability via traceroute:

```
(root@host1)#traceroute 10.10.10.181
traceroute to 10.10.10.181 (10.10.10.181), 30 hops max, 38 byte packets
1 10.10.12.6 (10.10.12.6) 0.457 ms 0.356 ms 0.443 ms
2 10.10.10.181 (10.10.10.181) 0.698 ms 0.642 ms 0.618 ms
```


© 2021 IP Infusion Inc. Proprietary

Virtual Router Redundancy Protocol Command Reference

Contents

This document contains these chapters:

- Chapter 1, *VRRP Commands*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 VRRP Commands

This chapter describes the commands for VRRP.

- accept-mode
- advertisement-interval
- authentication text
- circuit-failover
- debug vrrp
- disable
- enable
- l2-move allow-first-frame
- operational-ip
- preempt-mode
- priority
- router vrrp
- show debugging vrrp
- show running-config router vrrp
- show vrrp
- show vrrp summary
- show vrrp <1-255>
- show vrrp (global | ipv4) statistics
- snmp restart vrrp
- switch-back-delay
- undebug vrrp
- virtual-ip
- vrrp compatible-v2
- vrrp vmac

© 2021 IP Infusion Inc. Proprietary

accept-mode

Use this command to enable accept mode for the session

Use the `no` parameter with this command to restore the default setting.

Command Syntax

```
accept-mode true
accept-mode false
```

Parameter

None

Default

By default, accept mode for the session is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to set and unset the accept mode.

```
#configure terminal
(config)#router vrrp 2 eth0
(config-router)#accept-mode false
```


© 2021 IP Infusion Inc. Proprietary

advertisement-interval

Use this command to configure the advertisement interval of a virtual router. This is the length of time, in seconds, between each advertisement sent from the master to its backup(s). The master virtual router sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the master virtual router. The VRRP advertisements are encapsulated in IP packets and sent to the multicast address assigned to the VRRP group (224.0.0.18). Advertisements are sent every second by default.

Note: VRRP Master router and backup routers should be configured with the same advertisement interval. If there is a mismatch in the configuration, VRRP goes to the INIT state.

Use the `no` parameter with this command to restore the default setting.

Command Syntax

```
advertisement-interval <5-4095>
no advertisement-interval
```

Parameter

`<5-4095>`	Specify the advertisement interval in centi-seconds (in multiples of 5) when VRRPv3 is enabled

Default

By default, advertisements are sent every second

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to configure an advertisement interval of 50 centi-seconds for the virtual router with VR ID 2 on interface eth0.

```
#configure terminal
(config)#router ip vrrp 2 eth0
(config-router)#advertisement-interval 50
```

authentication text

Authenticates VRRPv2 packets received from other routers in the group. If configured authentication, all routers within the VRRP group must use the same authentication string. Authentication is supported only for VRRPv2 packets. V2-compatibility must be enabled.

If both master and backup having same authentication, then one node act as master and another node act as a backup based on priority. If both master and backup having different authentication, both nodes acting as a master.

Use the `no` parameter with this command to remove an authentication.

Command Syntax

```
authentication text TEXT-STRING
no authentication text
```

Parameter

`TEXT-STRING`	Password, maximum eight alphanumeric characters

Default

By default, authentication is disabled.

Command Mode

Router mode

Applicability

This command was introduced in OcNOS DC version 4.2.

Examples

```
#configure terminal
(config)#router vrrp 1 eth3
(config-router)#v2-compatible
(config-router)#authentication text abc_123
(config-router)#end

#configure terminal
(config)#router vrrp 1 eth3
(config-router)#no authentication text
(config-router)#end
```


© 2021 IP Infusion Inc. Proprietary

circuit-failover

Use this command to enable the VRRP circuit-failover feature.

Use the `no` form of this command to disable this feature.

Command Syntax

```
circuit-failover IFNAME <1-253>
no circuit-failover (IFNAME|)
```

Parameters

`IFNAME`	Interface of the router that is monitored by the virtual router. This is usually an upstream interface. Should the interface go down, another router, configured as backup within the VRRP group, may take over as a master.
`<1-253>`	Priority delta value. The value by which the virtual router decrements its priority value during a circuit failover event. Configure this value to be greater than the difference of priorities between the master and backup routers.

Default

By default, circuit failover is disabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to configure circuit failover for the VRRP session with VR ID 1. Interface eth1 is considered the monitored interface.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#circuit-failover eth1 30
```

debug vrrp

Use this command to specify debugging options for VRRP.

Use the `no` parameter with this command to disable debugging.

Command Syntax

```
debug vrrp (all|event|packet [send|recv|])
no debug vrrp (all|event|packet [send|recv|])
```

Parameters

`all`	Specify debugging options for all VRRP events.
`event`	Specify debugging options for VRRP event troubleshooting.
`packet`	Specify debugging options for VRRP packets
`send`	Specify the debug option set for sent packets.
`recv`	Specify the debug option set for received packets.

Command Mode

Configure mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to enable all VRRP debug options.

```
#configure terminal
(config)#debug vrrp all
```

The example below shows how to enable debugging options for VRRP events.

```
#configure terminal
(config)#debug vrrp events
```

The example below shows how to enable debug options for VRRP packets sent.

```
#configure terminal
(config)#debug vrrp packet send
```

The example below shows how to enable debug options for VRRP packets received.

```
#configure terminal
(config)#debug vrrp packet recv
```


© 2021 IP Infusion Inc. Proprietary

disable

Use this command to disable a VRRP session on the router (to stop the router from participating in virtual routing). When this command is configured, a backup Router assumes the Role of Master depending on its priority.

Command Syntax

```
disable
```

Parameters

None

Default

By default, VRRP session on the router is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below shows how to disable a VRRP session.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#disable
```

enable

Use this command to enable a VRRP session on the router (to make it participate in virtual routing). To make any changes to the VRRP configuration, first disable the router from participating in virtual routing using the `disable` command.

Note: Configure the virtual IP address and define an interface for the VRRP session (using the `virtual-ip` and `interface` commands) before using this command.

Command Syntax

```
enable
```

Parameters

None

Default

By default, VRRP session on the router is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below shows how to enable a VRRP session with VR ID 1 on interface eth0.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#enable
```


© 2021 IP Infusion Inc. Proprietary

l2-move allow-first-frame

Use this command to avoid a “double master” scenario where there is continuous MAC movement while flapping a Layer 2 switch interface that is connecting to VRRP nodes. Give this command in both interfaces of a Layer 2 switch that is connecting to VRRP nodes.

Use the `no` form of this command to remove this behavior.

Command Syntax

```
l2-move allow-first-frame
```

```
no l2-move allow-first-frame
```

Parameters

None

Default

By default, this behavior is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.7.

Examples

```
#configure terminal
(config)#interface xe2
(config)#l2-move allow-first-frame
```

operational-ip

Use this command to set the primary IPv4 address.

Use the no parameter with this command to remove a primary IPv4 address.

Command Syntax

```
operational-ip A.B.C.D
no operational-ip
```

Parameters

A.B.C.D	IPv4 address.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#operational-ip 1.2.3.4
```


© 2021 IP Infusion Inc. Proprietary

preempt-mode

Use this command to configure preempt mode. If set to `true`, the highest priority backup is always the master when the default master is unavailable. If set to `false`, a higher priority backup does not preempt a lower priority backup which is acting as master.

When the master router fails, the backup routers come online in priority order — highest to lowest. Preempt mode set to `true` allows a higher priority backup router to relieve a lower priority backup.

By default, a preemptive scheme is enabled whereby a higher priority backup virtual router that becomes available takes over for the backup virtual router that was elected to become master virtual router. This preemptive scheme can be disabled using the `preempt-mode false` command. If preemption is disabled, the backup virtual router that is currently elected as Master does not transition to backup again when the alternate backup router with higher priority becomes available.

Command Syntax

```
preempt-mode (true|false)
```

Parameters

`true`	Specify that preemption is enabled.
`false`	Specify that preemption is disabled.

Default

By default, preempt mode is true

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to enable the preempt mode.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#preempt-mode false

#configure terminal
(config)#router vrrp 1 eth0
(config-router)#preempt-mode true
```

priority

Use this command to configure the priority of a virtual router. The value of 255 (decimal) is reserved for the router that owns the IPvX address associated with the virtual router. The value of 0 (zero) is reserved for the Master router to indicate it is releasing responsibility for the virtual router. Higher values indicate higher priorities. Priority value to be used by this VRRP router in Master election

If the priority is high, the highest priority acts as a master. If the priority is low, lowest priority which is acting as backup.

Use the `no` parameter with this command to remove a priority and set the default value.

Command Syntax

```
priority <1-254>
no priority
```

Parameter

`<1-254>`	Priority of a virtual router.

Default

100 (non-owner)

255 (owner)

Command Mode

Router mode

Applicability

This command was introduced in OcNOS DC version 4.2.

Examples

The example below shows how to configure priority 50 for the virtual router with VR ID 2 on interface eth0.

```
#configure terminal
(config)#router ip vrrp 2 eth0
(config-router)#priority 200
```


© 2021 IP Infusion Inc. Proprietary

router vrrp

Use this command to enable a VRRP routing process.

Use the `no` form of this command to disable a VRRP routing process.

Command Syntax

```
router vrrp <1-255> IFNAME
no router vrrp <1-255> IFNAME
```

Parameters

`<1-255>`	Virtual router identifier
`IFNAME`	Interface name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router vrrp 1 eth0
```

show debugging vrrp

Use this command to display the set VRRP debugging option.

Command Syntax

```
show debugging vrrp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging vrrp
VVRRP debugging status:
VRRP event debugging is on
VRRP packet debugging is on
```


© 2021 IP Infusion Inc. Proprietary

show running-config router vrrp

Use this command to show the running configuration for VRRP.

Command Syntax

```
show running-config router vrrp
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below shows the running configuration of VRRP. Virtual Router is configured as Master and Owner of IP address.

```
#show running-config router vrrp
!
router vrrp 1 eth0
 virtual-ip 39.0.0.24 owner
 advertisement-interval 5
 preempt-mode false
 enable
!
```

show vrrp

Use this command to display a list of virtual router identifiers that are configured on the router.

Command Syntax

```
show vrrp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vrrp

R1#show vrrp
VrId <1>
State is Master
Virtual IP is 10.10.12.6 (IP owner)
Interface is eth0
Priority is 255
Advertisement interval: 5 centi sec
Preempt mode is TRUE

R2#show vrrp
VrId <1>
State is Backup
Virtual IP is 10.10.12.6 (Not IP owner)
Interface is eth0
Priority is 100
Advertisement interval: 5 centi sec
Preempt mode is TRUE
```

Table 1-226 Explains the show command output fields.

Table 1-226: show vrrp output fields

Field	Description
VrID	Type of vr identifier by the system on the interface.
State	VRRP State: Master — The interface is acting as the master router interface. Backup —The interface is acting as the backup router interface.
Virtual IP	List of virtual IP addresses configured on the interface.
Interface	Name of the logical interface.

© 2021 IP Infusion Inc. Proprietary

Field	Description
Priority	Configured VRRP priority for the interface.
Advertisement interval	Configured VRRP advertisement interval.
Preempt mode	Whether preemption is allowed on the interface.

show vrrp summary

Use this command to display a brief list of virtual router identifiers that are configured on the router.

Command Syntax

```
show vrrp summary
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.2.

Example

```
#show vrrp summary
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Interface  Admin  IpVersion  VRGroup  VRState  Priority    VIP          InterfaceIp
eth3       Up     IPv4       255      Master   255         66.0.0.1     66.0.0.1
eth3       Up     IPv6         1      Master   250         fe80::1      fe80::2
Total Number of IPv4 VRRP group 1
Total Number of IPv6 VRRP group 1
```

Table 1-227 explains the show command output fields.

Table 1-227: show vrrp summary output fields

Field	Description
interface	Interface name on which vrrp session is active.
Admin	Administrative state of the session Up/Down.
IpVersion	Internet protocol version IPv4 or IPv6.
VRGroup	Vrrp Group the router is part of.
priority	Configured VRRP priority for the interface.
VRState	VRRP State: Master - The interface is acting as the master router interface. Backup -The interface is acting as the backup router interface.
VIP	List of virtual IP addresses configured on the interface.
InterfaceIp	Primary IP address on the interface.

© 2021 IP Infusion Inc. Proprietary

show vrrp <1-255>

Use this command to display VRRP information for a virtual router.

Command Syntax

```
show vrrp <1-255> IFNAME
```

Parameters

<1-255>	Virtual router identifier
IFNAME	Interface name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
R1#show vrrp 7 xe1
VRRP Version: 3

VMAC enabled

Backward Compatibility disabled

Address family IPv4

VRRP Id: 7 on interface: xe1

State: AdminUp - Master

Virtual IP address: 10.10.10.81 (Owner)

Priority is 255

Advertisement interval: 100 centi sec

Master Advertisement interval: 100 centi sec

Skew time: 0 centi sec

Accept mode: FALSE

Preempt mode: TRUE

Multicast membership on IPv4 interface xe1: JOINED
```

© 2021 IP Infusion Inc. Proprietary

```
R2#show vrrp 7 xe1
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv4
VRRP Id: 7 on interface: xe1
State: AdminUp - Backup
Virtual IP address: 10.10.10.81 (Not-Owner)
Priority is 100
Advertisement interval: 100 centi sec
Master Advertisement interval: 100 centi sec
Skew time: 0 centi sec
Accept mode: FALSE
Preempt mode: TRUE
Multicast membership on IPv4 interface xe1: JOINED
```


© 2021 IP Infusion Inc. Proprietary

show vrrp (global | ipv4) statistics

Use this command to display VRRP global or ipv4 router statistics.

Command Syntax

```
show vrrp (global | ipv4 ) statistics
```

Parameters

`global`	Global (VRRP Router)
`ipv4`	VRRP IPv4 router

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.8.

Example

```
#show vrrp global statistics
 RRP Global Statistics
 Checksum Errors  : 0
 Version Errors   : 0
 VRid Errors      : 0
 Discontinuity Time: 00 hour, 00 min, 00 sec


#sh vrrp ipv4 statistics
Address family IPv4
VRRP Id: 1 on interface: xe1
Master Transitions: 0
Advertisements Rcvd: 0
Pkts Rcvd with IP TTL Errors: 0
Pkts Rcvd with Zero Priority: 0
Pkts Sent with Zero Priority: 0
Pkts Rcvd with Invalid TYPE: 0
Pkts Rcvd with Packet Length Errors: 0
Pkts Rcvd with IP Count Mismatch: 0
Discontinuity Time: 00 hour, 00 min, 00 sec
Refresh Rate: 1000 ms
```

© 2021 IP Infusion Inc. Proprietary

snmp restart vrrp

Use this command to restart SNMP in Virtual Routing Redundancy Protocol (VRRP).

Command Syntax

```
snmp restart vrrp
```

Parameters

None

Default

By default, SNMP restart is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#snmp restart vrrp
```


© 2021 IP Infusion Inc. Proprietary

switch-back-delay

Use this command to set a switch-back delay timer for the master VRRP router. This feature prevents the original master VRRP router from transitioning back to the master state after coming back online until the configured delay timer has expired.

Command Syntax

```
switch-back-delay <1-500000>
no switch-back-delay
```

Parameters

<1-500000>	Specify a switch-back delay in milliseconds.

Command Mode

Router mode

Default

By default, the switch-back delay is set to 0

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The example below shows how to set a switch-back delay timer of 7000 milliseconds.

```
#configure terminal
(config)#router vrrp 5 eth1
(config-router)#switch-back-delay 7000
```

undebug vrrp

Use this command to disable debugging options for VRRP.

Command Syntax

```
undebug vrrp (all|event|packet [send|recv|])
no undebug vrrp (all|event|packet [send|recv|])
```

Parameters

`all`	Specify debugging options for all VRRP events.
`event`	Specify debugging options for VRRP event troubleshooting.
`packet`	Specify debugging options for VRRP packets
`send`	Specify the debug option set for sent packets.
`recv`	Specify the debug option set for received packets.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#undebug vrrp all
```

The example below shows how to disable debug options for VRRP events.

```
#undebug vrrp events
```

The example below shows how to disable debug options for VRRP packets sent.

```
#undebug vrrp packet send
```

The example below shows how to disable debug options for VRRP packets received.

```
#undebug vrrp packet recv
```


© 2021 IP Infusion Inc. Proprietary

virtual-ip

Use this command to set the virtual IP address for the VRRP virtual router as VRRP Owner. This is the IP address used by end hosts to address their default gateway.

The VRRP Owner of the Virtual IP address only responds to packets destined to the Virtual IP address (for example, ICMP packets destined to the Virtual IP address).

Use the `no` parameter with this command to remove a virtual IP address assignment.

Syntax Description

```
virtual-ip A.B.C.D (owner|)
no virtual-ip
```

Parameters

`A.B.C.D`	Specify the virtual IP address of the interface that participates in virtual routing.
`owner`	Specify the IP address as the owner.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below shows how to configure the router as VRRP owner.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#virtual-ip 10.10.20.30 owner
```

The example below removes the virtual IP address assignment.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#no virtual-ip
```

vrrp compatible-v2

Use this command to enable the backward-compatibility feature. When enabled, both VRRPv3 and VRRPv2 inter-operation are supported.

Command Syntax

```
vrrp compatible-v2 (enable| disable)
```

Parameters

`enable`	Enable VRRPv2 inter-operation
`disable`	Disable VRRPv2 inter-operation

Default

By default, vrrp compatible-v2 is enabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#vrrp compatible-v2 enable
```


© 2021 IP Infusion Inc. Proprietary

vrrp vmac

Use this command to enable or disable Virtual MAC (VMAC).

This command affects all VRRP groups in a router. On a single network segment, multiple VRRP groups can be configured, each using a different VMAC. The use of VMAC addressing allows for faster switchover when a backup router assumes the master role. When this command is used to enable a VMAC, the virtual router forwards packets with a special-purpose multicast VMAC address (0:0:5e:0:01:<VR ID>). Otherwise, it forwards with is interface's physical address.

The VMAC address is assigned to a router interface at the time the VRRP group is enabled in the router.

Command Syntax

```
vrrp vmac (enable|disable)
```

Parameters

`enable`	Enable virtual MAC addressing.
`disable`	Disable virtual MAC addressing and use physical MAC addressing.

Default

By default, VMAC is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below shows how to enable a virtual MAC address on the router.

```
#configure terminal
(config)#vrrp vmac enable
```

The example below shows how to disable a virtual MAC address on the router.

```
#configure terminal
(config)#vrrp vmac disable
```

© 2021 IP Infusion Inc. Proprietary

SECTION 11 Bidirectional Forwarding Detection

Bidirectional Forwarding Detection Configuration Guide

Contents

This document contains these chapters and appendices:

- Chapter 1, *Base BFD Configuration*
- Chapter 2, *BFD Protocol Configurations*
- Chapter 3, *BFD Static Route Configuration*
- Chapter 4, *BFD Authentication*
- Chapter 5, *BFD with VRF Configuration*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Base BFD Configuration

This chapter provides the steps for configuring the base Bidirectional Forwarding Detection (BFD) setup.

Overview

This section provides an overview of Bidirectional Forwarding Detection (BFD). BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols like BGP, EIGRP, IS-IS, and OSPF. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators.The configuration and command reference for BFD is given in the following chapters in this section.

Topology



Figure 1-40: Basic Topology of Three Routers

BFD Echo Function

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 10.1.1.2`	Configure BFD session on interface.
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#bfd echo`	Enable BFD echo mode.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#bfd session 10.1.1.2 10.1.1.1`	Configure BFD session on interface.
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#bfd echo`	Enable BFD echo mode.

Validation

R1

```
#show bfd session detail
```

```
Session Interface Index : 3             Session Index : 1
nterface name : eth1
Lower Layer : IPv4                      Version : 1
Session Type : Single Hop               Session State : Up
Local Discriminator : 1                 Local Address : 10.1.1.1/32
Remote Discriminator : 1                Remote Address : 10.1.1.2/32
Local Port : 49152                      Remote Port : 3784
Local Echo Port : 49153
Options :
Echo Enabled
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250             Min Rx: 250             Multiplier: 3
Neg Tx: 2000            Neg Rx: 2000            Neg detect mult: 3
Min echo Tx: 1000       Min echo Rx: 1000       Neg echo intrvl: 1000
Storage type : 2
Sess down time : 00:00:01
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000010a               Pkt Out : 00000000000001f7
Echo Out : 00000000000000ab             IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000          IPv6 Pkt Out : 0000000000000000
UP Count : 57                           UPTIME : 00:00:00

Protocol Client Info:
BFD-> Client ID: 28     Flags: 4
------------------------------------------------------
Number of Sessions:    1
```

R2

```
#show bfd session detail

Session Interface Index : 3             Session Index : 1
Interface name : eth1
Lower Layer : IPv4                      Version : 1
Session Type : Single Hop               Session State : Up
Local Discriminator : 1                 Local Address : 10.1.1.2/32
Remote Discriminator : 1                Remote Address : 10.1.1.1/32
Local Port : 49152                      Remote Port : 3784
Local Echo Port : 49153
Options :
Echo Enabled
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250             Min Rx: 250             Multiplier: 3
Neg Tx: 2000            Neg Rx: 2000            Neg detect mult: 3
Min echo Tx: 1000       Min echo Rx: 1000       Neg echo intrvl: 1000
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled
```


© 2021 IP Infusion Inc. Proprietary

```
Counters values:
Pkt In : 00000000000000ad                Pkt Out : 0000000000000105
Echo Out : 0000000000000063              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 33                            UPTIME : 00:00:03

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------
Number of Sessions:    1
```

Note: Bfd echo is supported in software-bfd implementation.

BFD Slow Timer

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 10.1.1.2`	Configure BFD session on interface.
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#bfd slow-timer 1000`	Configure BFD `slow-timer` in milliseconds.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#bfd session 10.1.1.2 10.1.1.1`	Configure BFD session on interface.
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#bfd slow-timer 1000`	Configure BFD `slow-timer` in milliseconds.

Note: Bfd slow-timer is supported in software-bfd implementation.

BFD Multihop Peer Timer

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface loopback`	Enter interface mode
`R1(config-if)#ip address 1.1.1.1/32 secondary`	Specify IP address
`R1(config-if)#bfd session  1.1.1.1 3.3.3.3 multihop`	Configure BFD session on interface.
`R1(config-if)#exit`	Exit interface mode
`R1(config)#interface eth1`	Enter interface Mode
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#router ospf 1`	Enter router OSPF mode
`R1(config-router)#network 10.1.1.0/24 area 0`	Advertise the network to area 0
`R1(config-router)#redistribute connected`	Configuring redistribution
`R1(config-router)#exit`	Exit router OSPF mode
`R1(config)#bfd multihop-peer 3.3.3.3 interval 100 minrx 100 multiplier 3`	Configure BFD multihop-peer timer and reception intervals in milliseconds and the Hello multiplier.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface loopback`	Enter interface mode
`R2(config-if)#ip address 2.2.2.2/32 secondary`	Specify IP address
`R2(config-if)#exit`	Exit interface mode
`R2(config)#interface eth1`	Enter interface mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#interface eth2`	Enter interface Mode.
`R2(config-if)#ip address 20.1.1.2/24`	Assign IP address for interface
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#router ospf 1`	Enter router OSPF mode
`R2(config-router)#network 10.1.1.0/24 area 0`	Advertise the network to area 0
`R2(config-router)#network 20.1.1.0/24 area 0`	Advertise the network to area 0
`R2(config-router)#redistribute connected`	Configuring redistribution
`R2(config-router)#exit`	Exit router OSPF mode

R3

`R3#configure terminal`	Enter the Configure mode.
`R3#(config)#interface loopback`	Enter interface mode
`R3(config-if)#ip address 3.3.3.3/32 secondary`	Specify IP address

© 2021 IP Infusion Inc. Proprietary

`R3(config-if)#bfd session 3.3.3.3 1.1.1.1 multihop`	Configure BFD session on interface
`exit`	Exit interface mode
`R1(config)#interface eth2`	Enter interface Mode
`R1(config-if)#ip address 20.1.1.3/24`	Assign IP address for interface
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#router ospf 1`	Enter router OSPF mode
`R1(config-router)#network 20.1.1.0/24 area 0`	Advertise the network to area 0
`R1(config-router)#redistribute connected`	Configuring redistribution
`R1(config-router)#exit`	Exit router OSPF mode
`R1(config)#bfd multihop-peer 1.1.1.1 interval 100 minrx 100 multiplier 3`	Configure BFD multihop-peer timer and reception intervals in milliseconds and the Hello multiplier.

Validation

R1

```
ROUTER-1#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
========================================================================================

Session Interface Index : 0                    Session Index : 2
Lower Layer : IPv4 Version : 1
Session Type : Multihop Arbit Path            Session State : Up
Local Discriminator : 2                       Local Address : 10.1.1.1/32
Remote Discriminator : 1                      Remote Address : 20.1.1.3/32
Local Port : 49153                            Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 100               Min Rx: 100              Multiplier: 5
Neg Tx: 100               Neg Rx: 100              Neg detect mult: 5
Min echo Tx: 1000         Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000028711              Pkt Out : 00000000000000028708
Echo Out : 00000000000000000000            IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                               UPTIME : 00:42:13

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
```

```
    ------------------------------------------------------------
    Number of Sessions:    1
```

R3

```
    #show bfd session detail

    Session Interface Index : 0
    Interface name : eth1                       Session Index : 1
    Lower Layer : IPv4                          Version : 1
    Session Type : Multihop Arbit Path          Session State : Up
    Local Discriminator : 1                     Local Address : 20.1.1.3/32
    Remote Discriminator : 1                    Remote Address : 10.1.1.1/32
    Local Port : 49152                          Remote Port : 4784
    Options :

    Diagnostics : None

    Timers in Milliseconds :
    Min Tx: 100               Min Rx: 100               Multiplier: 3
    Neg Tx: 100               Neg Rx: 100               Neg detect mult: 3
    Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
    Storage type : 2
    Sess down time : 00:00:00
    Bfd GTSM Disabled
    Bfd Authentication Disabled

    Counters values:
    Pkt In : 00000000000001df                  Pkt Out : 00000000000001e0
    Echo Out : 0000000000000000                IPv6 Echo Out : 0000000000000000
    IPv6 Pkt In : 0000000000000000             IPv6 Pkt Out : 0000000000000000
    UP Count : 1                               UPTIME : 00:01:26

    Protocol Client Info:
    BFD-> Client ID: 28      Flags: 4
    ------------------------------------------------------------
    Number of Sessions:    1
```

Note: Minimum multihop bfd configurable timer is 50 ms

BFD Single-hop Session Timer

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 10.1.1.2`	Configure BFD session on interface.
`R1(config-if)#bfd interval 100 minrx 100 multiplier 4`	Configure BFD single-hop sessions timer and reception interval in millisecond and the Hello multiplier.
`R1(config-if)#exit`	Exit from interface mode.

© 2021 IP Infusion Inc. Proprietary

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#bfd session 10.1.1.2 10.1.1.1`	Configure BFD session on interface.
`R2(config-if)#bfd interval 100 minrx 100 multiplier 4`	Configure BFD single-hop sessions timer and reception interval in millisecond and the Hello multiplier.
`R2(config-if)#exit`	Exit from interface mode.

Validation:

R1

```
#show bfd session detail

Session Interface Index : 3
Interface name : eth1                       Session Index : 1
Lower Layer : IPv4                          Version : 1
Session Type : Single Hop                   Session State : Up
Local Discriminator : 1                     Local Address : 10.1.1.1/32
Remote Discriminator : 1                    Remote Address : 10.1.1.2/32
Local Port : 49152                          Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 100              Min Rx: 100              Multiplier: 4
Neg Tx: 100              Neg Rx: 100              Neg detect mult: 4
Min echo Tx: 100         Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000156e                   Pkt Out : 0000000000001748
Echo Out : 000000000000019b                 IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000              IPv6 Pkt Out : 0000000000000000
UP Count : 139                              UPTIME : 00:14:23

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

R2

```
#show bfd session detail

Session Interface Index : 3
Interface name : eth1                       Session Index : 1
```

```
    Lower Layer : IPv4                          Version : 1
    Session Type : Single Hop                   Session State : Up
    Local Discriminator : 1                     Local Address : 10.1.1.2/32
    Remote Discriminator : 1                    Remote Address : 10.1.1.1/32
    Local Port : 49152                          Remote Port : 3784
    Options :

    Diagnostics : None

    Timers in Milliseconds :
    Min Tx: 100               Min Rx: 100               Multiplier: 4
    Neg Tx: 100               Neg Rx: 100               Neg detect mult: 4
    Min echo Tx: 100          Min echo Rx: 1000         Neg echo intrvl: 0
    Storage type : 2
    Sess down time : 00:00:00
    Bfd GTSM Disabled
    Bfd Authentication Disabled

    Counters values:
    Pkt In : 000000000000181d                   Pkt Out : 00000000000019ab
    Echo Out : 00000000000001b5                 IPv6 Echo Out : 0000000000000000
    IPv6 Pkt In : 0000000000000000              IPv6 Pkt Out : 0000000000000000
    UP Count : 145                              UPTIME : 00:15:19

    Protocol Client Info:
    BFD-> Client ID: 28      Flags: 4
    ------------------------------------------------------------
    Number of Sessions:    1
```

Note: Minimum singlehop bfd configurable timer is 3 ms for hardware-bfd implementation and 50 ms for software-bfd implementation.

BFD Echo Interval

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 10.1.1.2`	Configure BFD session on interface.
`R1(config-if)#bfd echo interval 100`	.
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#bfd echo`	Enable BFD echo mode.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#bfd session 10.1.1.2 10.1.1.1`	Configure BFD session on interface.

© 2021 IP Infusion Inc. Proprietary

`R1(config-if)#bfd echo interval 100`	.
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#bfd echo`	Enable BFD echo mode.

Validation

R1

```
#sh bfd session detail

Session Interface Index : 3
Interface name : eth1                    Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Down
Local Discriminator : 1                  Local Address : 10.1.1.1/32
Remote Discriminator : 1                 Remote Address : 10.1.1.2/32
Local Port : 49152                       Remote Port : 3784
Local Echo Port : 49153
Options :
Echo Enabled
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250              Min Rx: 250              Multiplier: 3
Neg Tx: 2000             Neg Rx: 2000             Neg detect mult: 3
Min echo Tx: 100         Min echo Rx: 1000        Neg echo intrvl: 1000
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000001ea                Pkt Out : 0000000000000398
Echo Out : 0000000000000147              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 109                           UPTIME : 00:00:00

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

R2

```
#sh bfd session detail

Session Interface Index : 3
Interface name : eth1                    Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Down
Local Discriminator : 1                  Local Address : 10.1.1.2/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
Local Port : 49152                       Remote Port : 3784
Local Echo Port : 49153
Options :
```

```
    Echo Enabled
    Diagnostics : None

    Timers in Milliseconds :
    Min Tx: 250               Min Rx: 250               Multiplier: 3
    Neg Tx: 2000              Neg Rx: 2000              Neg detect mult: 3
    Min echo Tx: 100          Min echo Rx: 1000         Neg echo intrvl: 1000
    Storage type : 2
    Sess down time : 00:00:01
    Bfd GTSM Disabled
    Bfd Authentication Disabled

    Counters values:
    Pkt In : 000000000000028f                Pkt Out : 00000000000003b8
    Echo Out : 0000000000000183              IPv6 Echo Out : 0000000000000000
    IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
    UP Count : 129                           UPTIME : 00:00:00

    Protocol Client Info:
    BFD-> Client ID: 28      Flags: 4
    ------------------------------------------------------------
    Number of Sessions:    1
```

Note: Only supported for software-bfd implementation.

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 BFD Protocol Configurations

This chapter describes the BFD protocol configurations.

OSPF—BFD Single-Hop Session

This section provides the steps for configuring BFD for Single-Hop OSPF.

Topology



Figure 2-41: Single-Hop OSPF Topology

R1

R1(config)#int lo

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface lo`	Enter the Interface configuration mode for lo
`R1(config-if)#ip address 1.1.1.1/32 secondary`	Assign IP Address
`R1(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP Address
`R1(config-if)#exit`	Exit the Interface configuration mode.
`R1(config)#router ospf 100`	Enter the Router mode for OSPF.
`R1(config-router)#network 10.1.1.0/24 area 1`	Advertise network `10.1.1.0/24` in OSPF `area 1`.
`R1(config-router)#network 1.1.1.1/32 area 1`	Advertise loopback network `1.1.1.1/32` in OSPF `area 1`.
`R1(config-router)#bfd all-interfaces`	Enable BFD for all neighbors.
`R1(config-router)#exit`	Exit the router mode

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP Address
`R2(config-if)#exit`	Exit the Interface configuration mode.
`R2(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R2(config-if)#ip address 20.1.1.1/24`	Assign IP Address
`R2(config-if)#exit`	Exit the Interface configuration mode
`R2(config)#router ospf 100`	Enter the Router mode for OSPF.
`R2(config-router)#network 10.1.1.0/24 area 1`	Advertise network `10.1.1.0/24` in OSPF `area 1`.
`R2(config-router)#network 20.1.1.0/24 area 1`	Advertise network `20.1.1.0/24` in OSPF `area 1`.

© 2021 IP Infusion Inc. Proprietary

`R2(config-router)#network 2.2.2.2/32 area 1`	Advertise loopback network `2.2.2.2/32` in OSPF `area 1`.
`R2(config-router)#bfd all-interfaces`	Enable BFD for all neighbors.
`R2(config)#int lo`	Enter the Interface configuration mode for lo
`R2(config-if)#ip address 2.2.2.2/32 secondary`	Assign IP Address
`R2(config-router)#exit`	Exit the router mode.

R3

`R3#configure terminal`	Enter the Configure mode.
`R3(config)#interface lo`	Enter the Interface configuration mode for lo
`R3(config-if)#ip address 3.3.3.3/32 secondary`	Assign IP Address
`R3(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R3(config-if)#ip address 20.1.1.1/24`	Assign IP Address.
`R3(config-if)#exit`	Exit the Interface configuration mode.
`R3(config)#router ospf 100`	Enter the Router mode for OSPF.
`R3(config-router)#network 20.1.1.0/24 area 1`	Advertise network `20.1.1.0/24` in OSPF `area 1.`
`R3(config-router)#network 3.3.3.3/32 area 1`	Advertise loopback network `3.3.3.3/32` in OSPF `area 1.`
`R3(config-router)#bfd all-interfaces`	Enable BFD for all neighbors
`R3(config-router)#exit`	Exit the router mode.

Validation

R1

```
R1#show ip ospf n

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface   Instance ID
2.2.2.2           1   Full/Backup      00:00:35    10.1.1.2            xe23          0


R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface  Down-
Reason  Remote-Addr
1                    1              IPv4        Single-Hop     Up         00:02:55
xe23       NA                   10.1.1.2/32
257                  0              IPv4        Multi-Hop      Up          00:00:18
xe8         NA                    3.3.3.3/32
Number of Sessions:    2
```


© 2021 IP Infusion Inc. Proprietary

```
R1#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================
====

Session Interface Index : 10023          Interface name :xe23
Session Index : 1
Lower Layer : IPv4                                Version : 1
Session Type : Single Hop                    Session State : Up
Local Discriminator : 1                        Local Address : 10.1.1.1/32
Remote Discriminator : 1                     Remote Address : 10.1.1.2/32
Local Port : 49152                                Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                    Neg Rx: 250                    Neg detect mult: 3
Min echo Tx: 1000          Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000814                Pkt Out : 00000000000000000814
Pkts Drop : 00000000000000000000          Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000           IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                 UPTIME : 00:02:59

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 0                   Session Index : 257
Lower Layer : IPv4                                Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 257                      Local Address : 1.1.1.1/32
Remote Discriminator : 0                     Remote Address : 3.3.3.3/32
Local Port : 49153                                 Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                  Min Rx: 250                  Multiplier: 3
```

```
Neg Tx: 0                        Neg Rx: 0                        Neg detect mult: 0
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000000                Pkt Out : 00000000000000000107
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 0                                                UPTIME : 00:00:00
R3#show bfd session
BFD process for VRF: (DEFAULT VRF)
================================================================================
Sess-Idx Remote-Disc Lower-Layer Sess-Type Sess-State UP-Time Interface    Down-Reason
Remote-Addr
1          1      IPv4       Single-Hop   Up     00:04:33   eth2           NA
20.1.1.3/32
--------------------------------------------------------------------------------

R1#show bfd session detail
======================================================

Session Interface Index : 3
Interface name : eth1                    Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.1.1.1/32
Remote Discriminator : 1                 Remote Address : 10.1.1.2/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250              Min Rx: 250              Multiplier: 3
Neg Tx: 250              Neg Rx: 250              Neg detect mult: 3
Min echo Tx: 1000        Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000cf3                Pkt Out : 0000000000000cfc
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:12:12
```


© 2021 IP Infusion Inc. Proprietary

```
Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    1

R2#show bfd session detail
============================================================

Session Interface Index : 3
Interface name : eth1                    Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.1.1.2/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250              Min Rx: 250              Multiplier: 3
Neg Tx: 250              Neg Rx: 2000             Neg detect mult: 3
Min echo Tx: 1000        Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000d6f                Pkt Out : 0000000000000da5
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:12:39

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------

Session Interface Index : 4
Interface name : eth1                    Session Index : 2
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                  Local Address : 20.1.1.1/32
Remote Discriminator : 1                 Remote Address : 20.1.1.2/32
Local Port : 49153                       Remote Port : 3784
Options :

Diagnostics : None
```

```
Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000d30                Pkt Out : 0000000000000d5e
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:12:24
```

R2

```
R2#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface  Instance ID
1.1.1.1           1   Full/DR          00:00:32      10.1.1.1           xe9/3       0
3.3.3.3           1   Full/Backup    00:00:40     20.1.1.2           xe17/1     0


R2#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface   Down-
Reason  Remote-Addr
1               1               IPv4            Single-Hop    Up         00:02:33
xe9/3           NA          10.1.1.1/32
2               1               IPv4            Single-Hop    Up         00:01:54
xe17/1          NA          20.1.1.2/32
Number of Sessions:    2


R2#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================

Session Interface Index : 10023          Interface name :xe9/3
Session Index : 1
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                     Local Address : 10.1.1.2/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
Local Port : 49152                            Remote Port : 3784
```


© 2021 IP Infusion Inc. Proprietary

```
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                   Multiplier: 3
Neg Tx: 250                   Neg Rx: 250                   Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000713                Pkt Out : 00000000000000000714
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                UPTIME : 00:02:37

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 10053          Interface name :xe17/1
Session Index : 2
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                 Session State : Up
Local Discriminator : 2                      Local Address : 20.1.1.1/32
Remote Discriminator : 1                  Remote Address : 20.1.1.2/32
Local Port : 49153                              Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                    Multiplier: 3
Neg Tx: 250                   Neg Rx: 250                   Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000535              Pkt Out : 00000000000000000537
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
```

```
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                UPTIME : 00:01:58

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    2
```

R3

```
R3#show ip ospf n

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface   Instance ID
2.2.2.2           1     Full/DR         00:00:36    20.1.1.1          xe17/10       0


R3#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface   Down-
Reason  Remote-Addr
1                    2           IPv4            Single-Hop      Up         00:01:21
xe17/1             NA           20.1.1.1/32
257                  1           IPv4              Multi-Hop              Up
00:00:00      xe6                NA           1.1.1.1/32
Number of Sessions:    2
Total number of Established sessions 2


R3#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================

Session Interface Index : 10053          Interface name :xe17/1
Session Index : 1
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                     Local Address : 20.1.1.2/32
Remote Discriminator : 2                 Remote Address : 20.1.1.1/32
Local Port : 49152                            Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                    Neg Rx: 250                    Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
```


© 2021 IP Infusion Inc. Proprietary

```
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000391                  Pkt Out : 00000000000000000391
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                UPTIME : 00:01:26

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 0                    Session Index : 257
Lower Layer : IPv4                                  Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 257                       Local Address : 3.3.3.3/32
Remote Discriminator : 1                       Remote Address : 1.1.1.1/32
Local Port : 49153                                  Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                        Min Rx: 250                    Multiplier: 3
Neg Tx: 250                        Neg Rx: 250                    Neg detect mult:250
Min echo Tx: 1000              Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000000                  Pkt Out : 00000000000000000047
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 0                                                UPTIME : 00:00:00

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    2
```

OSPF—BFD Multi-Hop Session

This section provides the steps for configuring BFD for OSPF multi-hop sessions.

Topology

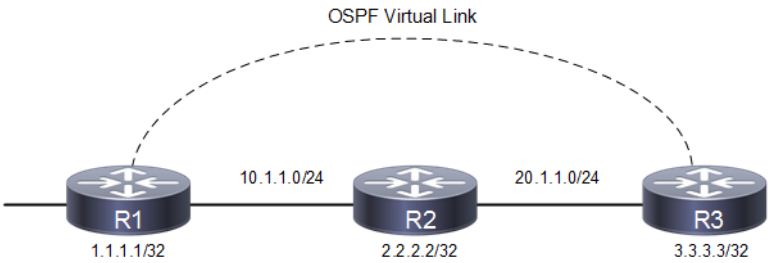


Figure 2-42: Multi-hop OSPFv2 Topology

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#router ospf 100`	Enter the Router mode for OSPF.
`R1(config-router)#ospf router-id 1.1.1.1`	OSPF router ID in IPv4 format
`R1(config-router)#bfd all-interfaces`	Enable BFD for all neighbors
`R1(config-router)#network 10.1.1.0/24 area 1`	Advertise network `20.1.1.0/24` in OSPF `area 1`.
`R1(config-router)#network 1.1.1.1/32 area 1`	Advertise loopback network `1.1.1.1/32` in OSPF `area 1`.
`R1(config-router)#network 30.1.1.0/24 area 0`	Advertise network `30.1.1.0/24` in OSPF `area 0`.
`R1(config-router)#area 1 virtual-link 3.3.3.3 fall-over bfd`	Create a virtual link to R3 with BFD.

R2

`R2#configure terminal`	Enter the Configure mode
`R2(config)#router ospf 100`	Enter the Router mode for OSPF.
`R2(config-router)#ospf router-id 2.2.2.2`	OSPF router ID in IPv4 format
`R1(config-router)#bfd all-interfaces`	Enable BFD for all neighbors
`R2(config-router)#network 10.1.1.0/24 area 1`	Advertise network `10.1.1.0/24` in OSPF `area 1`.
`R2(config-router)#network 20.1.1.0/24 area 1`	Advertise network `20.1.1.0/24` in OSPF `area 1`.
`R2(config-router)#network 2.2.2.2/32 area 1`	Advertise loopback network `2.2.2.2/32` in OSPF `area 1`.

R3

`R3#configure terminal`	Enter the Configure mode.
`R3(config)#router ospf 100`	Enter the Router mode for OSPF.
`R3(config-router)#ospf router-id 3.3.3.3`	OSPF router ID in IPv4 format

© 2021 IP Infusion Inc. Proprietary

`R1(config-router)#bfd all-interfaces`	Enable BFD for all neighbors
`R3(config-router)#network 20.1.1.0/24 area 1`	Advertise network `20.1.1.0/24` in OSPF `area 1`.
`R3(config-router)#network 3.3.3.3/32 area 1`	Advertise loopback network `3.3.3.3/32` in OSPF `area 1`.
`R3(config-router)#area 1 virtual-link 1.1.1.1 fall-over bfd`	Create a virtual link to R1 with BFD.

Validation

```
R1#sh bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
257          257              IPv4       Multi-Hop       Up        00:00:54
NA         NA                   20.1.1.2/32

Number of Sessions:    1


R2#sh bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
Number of Sessions:    0



R3#sh bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
257       257         IPv4        Multi-Hop   Up         00:01:46  NA       NA
10.1.1.1/32

Number of Sessions:    1


R1#sh bfd session detail

BFD process for VRF: (DEFAULT VRF)
========================================================================================

Session Interface Index : 0             Session Index : 257
Lower Layer : IPv4                      Version : 1
Session Type : Multihop Arbit Path      Session State : Up
```

```
Local Discriminator : 257               Local Address : 10.1.1.1/32
Remote Discriminator : 257              Remote Address : 20.1.1.2/32
Local Port : 49152                      Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000606             Pkt Out : 00000000000000000605
Pkts Drop : 00000000000000000000          Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000           IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000        IPv6 Pkt Out : 00000000000000000000
UP Count : 1                              UPTIME : 00:02:13

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    1



R2#sh bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================
Number of Sessions:    0
R2#


R3#sh bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================

Session Interface Index : 0             Session Index : 257
Lower Layer : IPv4                      Version : 1
Session Type : Multihop Arbit Path      Session State : Up
Local Discriminator : 257               Local Address : 20.1.1.2/32
Remote Discriminator : 257              Remote Address : 10.1.1.1/32
Local Port : 49152                      Remote Port : 4784
```


© 2021 IP Infusion Inc. Proprietary

```
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000529              Pkt Out : 00000000000000000530
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                               UPTIME : 00:01:56

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

BFD Configuration in IS-IS

This section provides the steps for configuring BFD for the IS-IS protocol.

Topology

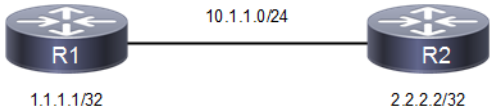


Figure 2-43: Basic Topology for BFD-ISIS

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface mode.
`R1(config-if)#ip address 10.1.1.1/24`	Configure IP address.
`R2(config-if)#ip router isis`	Configure ISIS router
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#router isis`	Enter the Router mode for IS-IS.

`R1(config-router)#net 10.0000.0000.0001.00`	Advertise network `10.0000.0000.0001.00` in IS-IS.
`R1(config-router)#bfd all-interfaces`	Enable BFD for all neighbors.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface mode.
`R2(config-if)#ip address 10.1.1.2/24`	Configure IP address.
`R2(config-if)#ip router isis`	Configure ISIS router
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#router isis`	Enter the Router mode for IS-IS.
`R2(config-router)#net 10.0000.0000.0002.00`	Advertise network `10.0000.0000.0002.00` in IS-IS.
`R2(config-router)#bfd all-interfaces`	Enable BFD for all neighbors.

Validation

```
R1#show bfd session

    BFD process for VRF: (DEFAULT VRF)
    ========================================================================
    =======
    Sess-Idx Remote-Disc Lower-Layer Sess-Type Sess-State UP-Time Interface
    Down-Reason Remote-Addr
    1                    1           IPv4             Single-Hop       Up
    00:00:42      eth1           NA                     10.1.1.1/32

    Number of Sessions:    1

    R2#show bfd session

    BFD process for VRF: (DEFAULT VRF)
    ========================================================================
    =======
    Sess-Idx Remote-Disc Lower-Layer Sess-Type Sess-State UP-Time Interface
    Down-Reason  Remote-Addr
    1            1            IPv4    Single-Hop  Up  00:10:23      eth1
    NA       10.1.1.2/32
    1            1            IPv4    Single-Hop  Up  00:10:23      eth2
    NA       20.1.1.2/32
    Number of Sessions:    2

R1#show bfd session detail
=======================================================

Session Interface Index : 3
Interface name : eth1                    Session Index : 2
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                  Local Address : 10.1.1.1/32
Remote Discriminator : 3                 Remote Address : 10.1.1.2/32
Local Port : 49153                       Remote Port : 3784
```


© 2021 IP Infusion Inc. Proprietary

```
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000027b                Pkt Out : 0000000000000278
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:02:19

Protocol Client Info:
ISIS-> Client ID: 6      Flags: 4
------------------------------------------------------------
Number of Sessions:    1

R2#sh bfd session detail
============================================================

Session Interface Index : 3
Interface name : eth1                    Session Index : 3
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 3                  Local Address : 10.1.1.2/32
Remote Discriminator : 2                 Remote Address : 10.1.1.1/32
Local Port : 49154                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000002db                Pkt Out : 00000000000002dd
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
```

```
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:02:42

Protocol Client Info:
ISIS-> Client ID: 6      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

BFD Configuration in BGP

This section provides the steps for configuring BFD for the BGP protocol.

Topology



Figure 2-44: Basic Topology for BFD in BGP

R1

`R1#configure terminal`	Enter configure mode
`R1(config)# interface lo`	Enter interface mode
`R1(config-if)#ip address 1.1.1.1/32 secondary`	Configure the IP address on loopback interface.
`R1(config-if)#bfd session 1.1.1.1 3.3.3.3 multihop`	Enable BFD multihop session
`R1(config)#router ospf 100`	Enter Router mode for OSPF
`R1(config-router)# ospf router-id 1.1.1.1`	Configure router-id in OSPF
`R1(config-router)# network 1.1.1.1/32 area 0.0.0.1`	Advertise network 1.1.1.1/32 in OSPF area 1.
`R1(config-router)# network 10.1.1.0/24 area 0.0.0.1`	Advertise network 10.1.1.0/24 in OSPF area 1.
`R1(config)#router bgp 100`	Enter Router mode for BGP
`R1(config-router)# neighbor 3.3.3.3 remote-as 100`	Add the neighbor 3.3.3.3 to remote-as 100.
`R1(config-router)# neighbor 3.3.3.3 fall-over bfd`	Enable BFD option for neighbor `multihop`
`R1(config-router)#neighbor 3.3.3.3 update-source lo`	Add neighbor 3.3.3.3 to update-source lo.
`R1(config-router)#neighbor 10.1.1.2 remote-as 100`	Add neighbor 10.1.1.2 to remote-as 100.
`R1(config-router)# neighbor 10.1.1.2 fall-over bfd`	Enable BFD option for neighbor
`R1(config-router)#end`	Exit from Router BGP mode

© 2021 IP Infusion Inc. Proprietary

R2

`R2#configure terminal`	Enter configure mode
`R2(config)# interface lo`	Enter interface mode
`R2(config-if)#ip address 2.2.2.2/32 secondary`	Configure the IP address on loopback interface.
`R2(config)#router ospf 100`	Enter Router mode for OSPF
`R2(config-router)#ospf router-id 2.2.2.2`	Configure router-id in OSPF
`R2(config-router)# network 2.2.2.2/32 area 0.0.0.1`	Advertise network 1.1.1.1/32 in OSPF area 1.
`R2(config-router)#network 10.1.1.0/24 area 0.0.0.1`	Advertise network 10.1.1.0/24 in OSPF area 1.
`R2(config-router)# network 20.1.1.0/24 area 0.0.0.1`	Advertise network 20.1.1.0/24 in OSPF area 1.
`R2(config)#router bgp 100`	Enter Router mode for BGP
`R2(config-router)# neighbor 10.1.1.1 remote-as 100`	Add neighbor 10.1.1.1 to remote-as 100.
`R2(config-router)#neighbor 10.1.1.1 fall-over bfd`	Enable BFD option for neighbor
`R2(config-router)# neighbor 20.1.1.2 remote-as 100`	Add neighbor 20.1.1.2 to remote-as 100.
`R2(config-router)# neighbor 20.1.1.2 fall-over bfd`	Enable BFD option for neighbor
`R2(config-router)#end`	Exit from Router BGP mode

R3

`R3#configure terminal`	Enter configure mode
`R3(config)# interface lo`	Enter interface mode
`R3(config-if)#ip address 3.3.3.3/32 secondary`	Configure IP address on loopback interface.
`R1(config-if)#bfd session 3.3.3.3 1.1.1.1 multihop`	Enable BFD multihop session
`R3(config)#router ospf 100`	Enter Router mode for OSPF
`R3(config-router)#ospf router-id 3.3.3.3`	Configure router-id in OSPF
`R3(config-router)# network 3.3.3.3/32 area 0.0.0.1`	Advertise network 3.3.3.3/32 in OSPF area 1.
`R3(config-router)# network 20.1.1.0/24 area 0.0.0.1`	Advertise network 20.1.1.0/24 in OSPF area 1.
`R3(config)#router bgp 100`	Enter Router mode for BGP
`R3(config-router)# neighbor 1.1.1.1 remote-as 100`	Add neighbor 1.1.1.1 to remote-as 100.
`R3(config-router)# neighbor 1.1.1.1 fall-over bfd multihop`	Enable BFD option for neighbor
`R3(config-router)#neighbor 1.1.1.1 update-source lo`	Add neighbor 1.1.1.1 to update-source lo.

`R3(config-router)# neighbor 20.1.1.1 remote-as 100`	Add neighbor 20.1.1.1 to remote-as 100.
`R3(config-router)#neighbor 20.1.1.1 fall-over bfd`	Enable BFD option for neighbor
`R3(config-router)#end`	Exit from Router BGP mode

Validation

R1

```
R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface   Instance ID
2.2.2.2           1   Full/Backup      00:00:35    10.1.1.2            eth1         0
R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
=====
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface  Down-
Reason  Remote-Addr
1                   1             IPv4        Single-Hop     Up         00:02:55
eth1      NA                  10.1.1.2/32
257                 0             IPv4        Multi-Hop      Up          00:00:18
NA         NA                    3.3.3.3/32
Number of Sessions:    2


R1#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================
====

Session Interface Index : 10023          Interface name :eth1
Session Index : 1
Lower Layer : IPv4                              Version : 1
Session Type : Single Hop                    Session State : Up
Local Discriminator : 1                         Local Address : 10.1.1.1/32
Remote Discriminator : 1                     Remote Address : 10.1.1.2/32
Local Port : 49152                              Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                   Multiplier: 3
```


© 2021 IP Infusion Inc. Proprietary

```
Neg Tx: 250                    Neg Rx: 250                    Neg detect mult: 3
Min echo Tx: 1000          Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000814                Pkt Out : 00000000000000000814
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                  UPTIME : 00:02:59

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 0                    Session Index : 257
Lower Layer : IPv4                                 Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 257                      Local Address : 1.1.1.1/32
Remote Discriminator : 0                      Remote Address : 3.3.3.3/32
Local Port : 49153                                  Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                   Multiplier: 3
Neg Tx: 0                       Neg Rx: 0                       Neg detect mult: 0
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000000                Pkt Out : 00000000000000000107
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out : 00000000000000000000
UP Count : 0                                                  UPTIME : 00:00:00
```

R2

```
R2#show ip ospf neighbor

Total number of full neighbors: 2
```

```
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface  Instance ID
1.1.1.1           1   Full/DR         00:00:32      10.1.1.1          eth1         0
3.3.3.3           1   Full/Backup     00:00:40     20.1.1.2           eth2         0


R2#show bfd session

BFD process for VRF: (DEFAULT VRF)
=================================================================================
=====
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface   Down-
Reason  Remote-Addr
1               1               IPv4            Single-Hop    Up         00:02:33
eth1            NA              10.1.1.1/32
2               1               IPv4            Single-Hop    Up         00:01:54
eth2            NA              20.1.1.2/32
Number of Sessions:    2


R2#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
=================================================================================
====

Session Interface Index : 10023          Interface name :eth1
Session Index : 1
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                     Local Address : 10.1.1.2/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
Local Port : 49152                            Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                   Multiplier: 3
Neg Tx: 250                   Neg Rx: 250                   Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000713               Pkt Out : 00000000000000000714
Pkts Drop : 00000000000000000000          Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000           IPv6 Echo Out : 00000000000000000000
```

 © 2021 IP Infusion Inc. Proprietary

```
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                UPTIME : 00:02:37

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 10053          Interface name :eth2
Session Index : 2
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                     Local Address : 20.1.1.1/32
Remote Discriminator : 1                 Remote Address : 20.1.1.2/32
Local Port : 49153                             Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                    Multiplier: 3
Neg Tx: 250                   Neg Rx: 250                   Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000535              Pkt Out : 00000000000000000537
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                               UPTIME : 00:01:58

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    2
```

R3

```
R3#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface   Instance ID
2.2.2.2           1     Full/DR         00:00:36    20.1.1.1          eth1            0


R3#show bfd session
```

```
BFD process for VRF: (DEFAULT VRF)
================================================================================
=====
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface   Down-
Reason  Remote-Addr
1                    2          IPv4            Single-Hop      Up         00:01:21
eth1            NA                20.1.1.1/32
257                  1          IPv4            Multi-Hop       Up        00:00:00
NA              NA                1.1.1.1/32
Number of Sessions:    2
Total number of Established sessions 2


R3#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================
====

Session Interface Index : 10053          Interface name :eth1
Session Index : 1
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                     Local Address : 20.1.1.2/32
Remote Discriminator : 2                 Remote Address : 20.1.1.1/32
Local Port : 49152                            Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                   Multiplier: 3
Neg Tx: 250                    Neg Rx: 250                   Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000391                Pkt Out : 00000000000000000391
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                UPTIME : 00:01:26

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------
```


© 2021 IP Infusion Inc. Proprietary

```
Session Interface Index : 0                    Session Index : 257
Lower Layer : IPv4                                  Version : 1
Session Type : Multihop Arbit Path        Session State : Up
Local Discriminator : 257                     Local Address : 3.3.3.3/32
Remote Discriminator : 1                     Remote Address : 1.1.1.1/32
Local Port : 49153                                  Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                        Min Rx: 250                      Multiplier: 3
Neg Tx: 250                        Neg Rx: 250                      Neg detect mult:250
Min echo Tx: 1000              Min echo Rx: 1000          Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000000                 Pkt Out : 00000000000000000047
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 0                                                UPTIME : 00:00:00

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    2
```

BFD Configuration in RIP

This section provides the steps for configuring BFD for the RIP protocol.

Topology

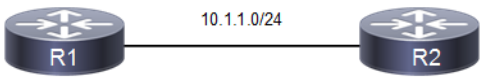


Figure 2-45: Basic Topology for BFD in RIP

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth2`	Enter interface mode.

`R1(config-if)#ip address 10.1.1.1/24`	Configure IP address.
`R2(config-if)#ip router isis`	Configure ISIS router
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#router rip`	Enter the Router mode for RIP.
`R1(config-router)#network 10.1.1.0/24`	Advertise network `10.1.1.0/24` in RIP.
`R1(config-router)#bfd all-interfaces`	Enable BFD for all neighbors.
	or
`R1(config-router)#neighbor 10.1.1.2 fall-over bfd`	Enable BFD for a specific RIP neighbor

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface mode.
`R2(config-if)#ip address 10.1.1.2/24`	Configure IP address.
`R2(config-if)#ip router isis`	Configure ISIS router
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#router rip`	Enter the Router mode for RIP.
`R2(config-router)#network 10.1.1.0/24`	Advertise network `10.1.1.0/24` in RIP.
`R2(config-router)#bfd all-interfaces`	Enable BFD for all neighbors.
	or
`R2(config-router)#neighbor 10.1.1.1 fall-over bfd`	Enable BFD for a specific RIP neighbor.

Validation

R1

```
R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
=================================================================================1
Sess-Idx Remote-Disc Lower-Layer Sess-Type Sess-State UP-Time Interface    Down-Reason
Remote-Addr
1                    1          IPv4           Single-Hop      Up         00:00:42
eth1           NA                    10.1.1.1/32

Number of Sessions:    1

R1#show bfd session detail
=========================================================

Session Interface Index : 3
Interface name : eth1                    Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.1.1.67/32
```


© 2021 IP Infusion Inc. Proprietary

```
Remote Discriminator : 1                Remote Address : 10.1.1.68/32
Local Port : 49152                      Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250             Min Rx: 250             Multiplier: 3
Neg Tx: 250             Neg Rx: 2000            Neg detect mult: 3
Min echo Tx: 1000       Min echo Rx: 1000       Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000040               Pkt Out : 000000000000003f
Echo Out : 0000000000000000             IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000          IPv6 Pkt Out : 0000000000000000
UP Count : 1                            UPTIME : 00:00:16

Protocol Client Info:
RIP-> Client ID: 2       Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

R2

```
R2#show bfd session


BFD process for VRF: (DEFAULT VRF)
================================================================================
Sess-Idx Remote-Disc Lower-Layer Sess-Type Sess-State UP-Time Interface     Down-Reason
Remote-Addr
1          1            IPv4    Single-Hop  Up  00:10:23      eth1           NA
10.1.1.2/32
1          1            IPv4    Single-Hop  Up  00:10:23      eth2           NA
20.1.1.2/32
Number of Sessions:    2

R2#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Remote-Addr
1          1            IPv4         Single-Hop  Up          00:00:10  10.1.1.67/32
Number of Sessions:    1

--------------------------------------------------------------------------------

R2#show bfd session detail
======================================================

Session Interface Index : 3
```

```
Interface name : eth1                    Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.1.1.68/32
Remote Discriminator : 1                 Remote Address : 10.1.1.67/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250              Min Rx: 250              Multiplier: 3
Neg Tx: 250              Neg Rx: 250              Neg detect mult: 3
Min echo Tx: 1000        Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000055                Pkt Out : 0000000000000057
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:00:22

Protocol Client Info:
RIP-> Client ID: 2       Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 BFD Static Route Configuration

This chapter describes the configurations for BFD static routes.

In order to establish alternate paths to destinations that have the least possible delay it is important to quickly detect any changes to static route validity. BFD detects the liveliness of a static route's nexthop and then uses the nexthop's reachability information to determine whether routes are valid. Using BFD to reach a static route's nexthop also ensures that a static route is inserted in the forwarding database only when the nexthop neighbor is reachable.

Topology

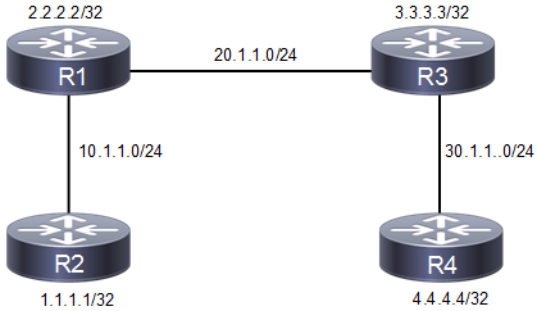


Figure 3-46: BFD Static Route Basic Topology

R1

`R1(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address on interface.
`R1(config-if)#exit`	Exit the Interface configuration mode.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#ip route 30.1.1.0/24 20.1.1.3`	Configure static route.
`R2(config)#ip bfd static all-interfaces`	Enable BFD for all static routes.
`R2(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R2(config-if)#ip static bfd`	Enable static BFD on the interface.
`R2(config-if)#ip address 20.1.1.2/24`	Assign IP address on interface.
`R2(config-if)#exit`	Exit the Interface configuration mode.
`R2(config)#ip static 30.1.1.0/24 20.1.1.3 fall-over bfd enable`	Enable static BFD at static route level.
`R2(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address on interface.
`R2(config-if)#exit`	Exit the Interface configuration mode.

R3

`R3#configure terminal`	Enter the Configure mode.
`R3(config)#ip route 10.1.1.0/24 20.1.1.2`	Configure static route.
`R3(config)#ip bfd static all-interfaces`	Enable BFD for all static routes.
`R3(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R3(config-if)#ip address 20.1.1.3/24`	Assign IP address on interface.
`R3(config-if)#ip static bfd`	Enable static BFD at interface level.
`R3(config-if)#exit`	Exit the Interface configuration mode.
`R3(config)#ip static 10.1.1.0/24 20.1.1.2 fall-over bfd enable`	Enable static BFD at static route level.
`R3(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R3(config-if)#ip address 30.1.1.2/24`	Assign IP address on interface.
`R3(config-if)#exit`	Exit the Interface configuration mode.

R4

`R3(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R3(config-if)#ip address 30.1.1.1/24`	Assign IP address on interface.
`R3(config-if)#exit`	Exit the Interface configuration mode.

Validation

R2

```
R2#show bfd session


BFD process for VRF: (DEFAULT VRF)
=================================================================================
=======
Sess-Idx Remote-Disc Lower-Layer Sess-Type Sess-State UP-Time Interface
Down-Reason  Remote-Addr
1           1            IPv4    Single-Hop  Up  00:10:23      eth1
NA       10.1.1.2/32
1           1            IPv4    Single-Hop  Up  00:10:23      eth2
NA       20.1.1.2/32
Number of Sessions:    2

R2#show bfd session detail
=======================================================

Session Interface Index : 3             Session Index : 5
Interface name : eth1
Lower Layer : IPv4                      Version : 1
Session Type : Single Hop               Session State : Up
Local Discriminator : 5                 Local Address : 20.1.1.2/32
Remote Discriminator : 1                Remote Address : 20.1.1.3/32
Local Port : 49156                      Remote Port : 3784
Options :
```


© 2021 IP Infusion Inc. Proprietary

```
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000a29                Pkt Out : 0000000000000bb6
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:09:34

Protocol Client Info:
RIB-> Client ID: 42      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

R3

```
R3#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
=======
Sess-Idx Remote-Disc Lower-Layer Sess-Type Sess-State UP-Time Interface
Down-Reason  Remote-Addr
1           1       IPv4        Single-Hop   Up      00:04:33   eth2
NA           20.1.1.3/32


R3#sh bfd session detail
======================================================

Session Interface Index : 3              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 20.1.1.3/32
Remote Discriminator : 5                 Remote Address : 20.1.1.2/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled
```

```
Counters values:
Pkt In : 0000000000000a59                Pkt Out : 0000000000000a53
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:09:41

Protocol Client Info:
RIB-> Client ID: 42      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 BFD Authentication

This chapter provides BFD authentication configuration examples.

Overview

Bidirectional Forwarding Detection (BFD) is a protocol intended to detect faults in the bidirectional path between two forwarding engines, including physical interfaces, sub-interfaces, and data link. It operates independently of media, data protocols, and routing protocols. A session will be created between links. When BFD links is hacked, the link may be falsely declared to be down, or falsely declared to be up. To overcome this type of situations, need to use authentication on BFD. Using this we can mitigate threats from attackers.

OcNOS supports the following authentication types:

- Simple password
- Keyed/Meticulous MD5
- Keyed/Meticulous SHA1

Among these types, meticulous SHA1 is the strongest one.

Authentication is optionally enabled on BFD sessions. By default, it is disabled and is configurable via CLI. When authentication is enabled, BFD packets will exchange with authentication section (based on the configured auth type). Receiving system will examine the authentication section of the packet; if it is successful then it will accept. Otherwise, it will discard. Keyed/Meticulous MD5 authentication is not supported on hw-bfd implementation on Broadcom chipsets. Also, key-chain option isn't supported on hw-bfd implementation.

Enabling BFD Authentication

On a Router BFD authentication can be enabled for multiple keys & or single key support over a BFD sessions:

- Using Key-chain, for multiple key support
- Using Key-ID, for single key support

OcNOS supports BFD Authentication for IPv4, with single-hop & multihop. Enabling BFD Authentication for Single-hop for IPv4, using key chain. In this example, the BFD session is configured between R1 & R2 using multiple key (using key chain).

Once the BFD session is up, the authentication is enabled on both the routers, with the authentication type as simple password. We can enable the authentication on BFD session using any one of the above-mentioned authentication type, with the identical authentication Type on both side.

Topology

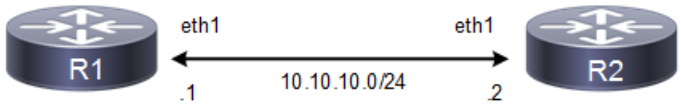


Figure 4-47: Basic Topology of Two Routers

Router 1 (R1)

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#key chain myKeyChain`	Configure the key chain by assigning the string to it.
`R1(config-keychain)#key 14`	Configure key-ID for the key chain. Multiple keys can be configured for same key chain but only one will be used for authentication.
`R1(config-keychain-key)#key-string R1`	Assign the key-string to the key.
`R1(config-keychain)#key 15`	Configure the key-ID for the key chain.
`R1(config-keychain-key)#key-string myKey`	Assign the key-string to the key.
`R1(config-keychain-key)#exit`	Exit from the Key mode.
`R1(config-keychain)#exit`	Exit from the Key Chain mode.
`R1(config)#interface eth1`	Enter the Interface configuration mode.
`R1(config-if)#bfd session 10.10.10.1 10.10.10.2`	Enable the BFD session between peers.
`R1(config-if)#bfd auth type simple key-chain myKeyChain`	Enable the Authentication for BFD as Type-simple password. Note: Configure authentication type as any one of mentioned types.
`R1(config-if)#exit`	Exit interface mode.

Router 2 (R2)

`R2(config)#key chain myKeyChain`	Configure the key chain by assigning the string to it.
`R2(config-keychain)#key 14`	Configure key-ID for the key chain. Multiple keys can be configured for same key chain but only one will be used for authentication.
`R2(config-keychain-key)#key-string R1`	Assign the key-string to the key.
`R2(config-keychain)#key 15`	Configure the key-ID for the key chain.
`R2(config-keychain-key)#key-string myKey`	Assign the key-string to the key.
`R2(config-keychain-key)#exit`	Exit from the Key mode.
`R2(config-keychain)#exit`	Exit from the Key Chain mode.
`R2R2(config)#interface eth1`	Enter the Interface configuration mode.
`R2(config-if)#bfd session 10.10.10.2 10.10.10.1`	Enable the BFD session between peers.
`R2(config-if)#bfd auth type simple key-chain myKeyChain`	Enable the Authentication for BFD as Type-simple password. Note: Configure authentication type as any one of mentioned types.
`R2(config-if)#exit`	Exit interface mode.

Validation

Check for Session to be single-hop, up with the remote address as of R2 in “show bfd session” & in “show bfd session detail”, check for BFD authentication is enabled with authentication type- configured.

```
R1#show bfd session

BFD process for VRF: (DEFAULT VRF)
```


© 2021 IP Infusion Inc. Proprietary

```
================================================================================
===========
Sess-Idx  Remote-Disc   Lower-Layer  Sess-Type  Sess-State  UP-Time
Interface  Down-Reason   Remote-Add
1                1                          IPv4              Single-Hop
Up          00:00:32      eth1              NA           10.1.1.1/32

Number of Sessions:    1

R1#show bfd session detail
BFD process for VRF: (DEFAULT VRF)
================================================================
Session Interface Index : 3
Interface name :eth1
Session Index : 1
Lower Layer : IPv4                                          Version : 1
Session Type : Single Hop
Session State : Up
Local Discriminator : 1
Local Address : 10.1.1.2/32
Remote Discriminator : 1                                          Remote
Address : 10.1.1.1/32
Local Port : 49152
Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                    Neg Rx: 250                    Neg detect
mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Enabled
Authentication type : simple
Authentication Key-id : 14

Counters values:
Pkt In : 00000000000000005569               Pkt Out : 00000000000000006463
Echo Out : 00000000000000000464            IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out :
00000000000000000000
UP Count : 2                                                  UPTIME :
00:00:35

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
----------------------------------------------------------
Number of Sessions:    1



R2#show bfd session
```

```
BFD process for VRF: (DEFAULT VRF)
================================================================================
=======
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface  Down-Reason  Remote-Addr
1               1                  IPv4            Single-Hop      Up
00:00:09       eth1           NA             10.1.1.2/32
Number of Sessions:    1

R2#show bfd session detail
BFD process for VRF: (DEFAULT VRF)
================================================================================
======
Session Interface Index : 3             Interface name :eth1
Session Index : 1
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                      Local Address : 10.1.1.1/32
Remote Discriminator : 1                 Remote Address : 10.1.1.2/32
Local Port : 49152                             Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                    Neg Rx: 250                    Neg detect
mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Enabled
Authentication type : simple
Authentication Key-id : 14

Counters values:
Pkt In : 00000000000000005530                Pkt Out : 00000000000000006288
Echo Out : 00000000000000000438           IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out :
00000000000000000000
UP Count : 2                                                    UPTIME :
00:00:12

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

Enabling BFD Authentication for Single-hop for IPv4, Using Key-ID

In this example, the BFD session is configured between R1 and R2 using single key (using key-ID). Once the BFD session is up, the authentication is enabled on both the routers, with the authentication type as keyed-MD5. We can

© 2021 IP Infusion Inc. Proprietary

enable the authentication on BFD session using any one of the above mentioned authentication type, with the Identical authentication type on both side.

Topology

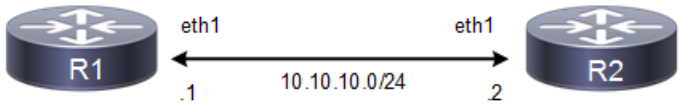


Figure 4-48: Basic Topology of Two Routers

Router 1 (R1)

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter the Interface configuration mode.
`R1(config-if)#bfd session 10.10.10.1 10.10.10.2`	Enable the BFD session between peers. Note: For IPv6, provide the IPv6 source and destination addresses for the BFD session.
`R1(config-if)#bfd auth type keyed-md5 key-id 10 key myKey`	Enable the Authentication for BFD as Type keyed-MD5. Note: Configure authentication type as any one of mentioned types.
`R1(config-if)#exit`	Exit interface mode.

Router 2 (R2)

`R2(config)#interface eth1`	Enter the Interface configuration mode.
`R2(config-if)#bfd session 10.10.10.2 10.10.10.1`	Enable the BFD session between peers. Note: For IPv6, provide the IPv6 source and destination addresses for the BFD session.
`R2(config-if)#bfd auth type keyed-md5 key-id 10 key myKey`	Enable the Authentication for BFD as Type keyed-MD5. Note: Configure authentication type as any one of mentioned types.
`R2(config-if)#exit`	Exit interface mode.

Validation

Check for Session to be single-hop, up with the remote address as of R2 in “show bfd session” & in “show bfd session detail”, check for BFD authentication is enabled with authentication type- configured.

```
R1#show bfd session
BFD process for VRF: (DEFAULT VRF)
=================================================================================
=======
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface   Down-Reason  Remote-Addr
1             1                    IPv4           Single-Hop    Up
00:00:37      eth1           NA           10.1.1.1/32
Number of Sessions:    1

R1#show bfd session detail
BFD process for VRF: (DEFAULT VRF)
```

```
================================================================================
======
Session Interface Index : 3                Interface name :eth1
Session Index : 1
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                  Session State : Up
Local Discriminator : 1                       Local Address : 10.1.1.2/32
Remote Discriminator : 1                   Remote Address : 10.1.1.1/32
Local Port : 49152                            Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                      Min Rx: 250                      Multiplier: 3
Neg Tx: 250                      Neg Rx: 250                      Neg detect
mult: 3
Min echo Tx: 1000          Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Enabled
Authentication type : keyed-md5
Authentication Key-id : 10

Counters values:
Pkt In : 00000000000000006970                 Pkt Out : 00000000000000007881
Echo Out : 00000000000000000464            IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out :
00000000000000000000
UP Count : 4                                  UPTIME : 00:00:39

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1



R2#show bfd session
BFD process for VRF: (DEFAULT VRF)
================================================================================
=======
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface   Down-Reason  Remote-Addr
1                  1                    IPv4              Single-Hop
Up          00:00:55        eth1          NA           10.1.1.2/32
Number of Sessions:    1

R2#show bfd session detail
BFD process for VRF: (DEFAULT VRF)
================================================================================
======

Session Interface Index : 3              Interface name :eth1
Session Index : 1
```


© 2021 IP Infusion Inc. Proprietary

```
Lower Layer : IPv4                              Version : 1
Session Type : Single Hop                    Session State : Up
Local Discriminator : 1                        Local Address : 10.1.1.1/32
Remote Discriminator : 1                    Remote Address : 10.1.1.2/32
Local Port : 49152                                Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                      Min Rx: 250                      Multiplier: 3
Neg Tx: 250                      Neg Rx: 250                      Neg detect
mult: 3
Min echo Tx: 1000          Min echo Rx: 1000          Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Enabled
Authentication type : keyed-md5
Authentication Key-id : 10

Counters values:
Pkt In : 00000000000000007127                  Pkt Out : 00000000000000007907
Echo Out : 00000000000000000438             IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 5                                    UPTIME : 00:00:58

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 BFD with VRF Configuration

This chapter shows using BFD with a non-default VRF for OSPFv2 and OSPFv3.

Topology

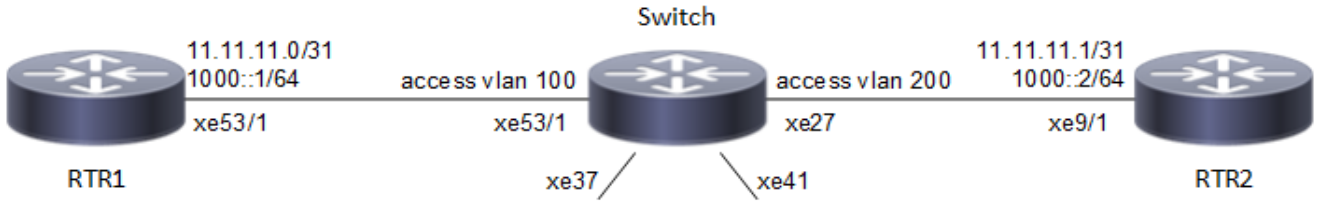


Figure 5-49: BFD user-defined VRF

RTR1

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrf10`	Create vrf instance with vrf10 and enter into vrf mode
`(config-vrf)#exit`	Exit from vrf mode
`(config)#interface xe53/1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf10`	Enable vrf forwarding on interface
`(config-if)#ip address 11.11.11.0/31`	Assign IPv4 address in /31 mask.
`(config-if)#ipv6 address 1000::1/64`	Assign IPv6 address in /64 mask.
`(config-if)#ipv6 router ospf area 0 tag vrf10`	Tag ospfv3 instance on interface with vrf10 for area 0
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 65535 vrf10`	Enter into ospf vrf configuration mode
`(config-router)#router-id 1.1.1.1`	Assign router ID 1.1.1.1 for ospf process 65535
`(config-router)#bfd all-interfaces`	Enable bfd for all-interface into ospf
`(config-router)#network 11.11.11.0/31 area 0`	Enable routing for network 11.11.11.0/31 in area 0
`(config-router)#exit`	Exit from ospf vrf configuration mode
`(config)#router ipv6 vrf ospf vrf10`	Enter into ipv6 ospf vrf configuration mode
`(config-router)#router-id 2.2.2.2`	Assign router-id 2.2.2.2 for ipv6 ospf process
`(config-router)#bfd all-interfaces`	Enable bfd for all-interface into ospf
`(config-router)#exit`	Exit from ipv6 ospf vrf configuration mode

Switch

`#configure terminal`	Enter configure mode.
`(config)#bridge 32 protocol rstp vlan-bridge`	Create a RSTP VLAN aware bridge with bridge-id 32
`(config)#vlan 100 bridge 32`	Create VLAN 100 and map it to bridge 32

© 2021 IP Infusion Inc. Proprietary

(config)#vlan 200 bridge 32	Create VLAN 200 and map it to bridge 32
(config)#interface xe53/1	Enter interface mode
(config-if)#switchport	Make it port as L2 interface
(config-if)#bridge-group 32	Configure bridge group to l2 interface
(config-if)#switchport mode access	Set the layer 2 interface as access interface
(config-if)#switchport access vlan 100	Map the VLAN 100 to access interface
(config-if)#exit	Exit interface mode.
(config)#interface xe27	Enter interface mode
(config-if)#switchport	Make it port as L2 interface
(config-if)#bridge-group 32	Configure bridge group to l2 interface
(config-if)#switchport mode access	Set the layer 2 interface as access interface
(config-if)#switchport access vlan 200	Map the VLAN 200 to access interface
(config-if)#exit	Exit interface mode.
(config)#interface xe37	Enter interface mode
(config-if)#switchport	Make it port as L2 interface
(config-if)#bridge-group 32	Configure bridge group to l2 interface
(config-if)#switchport mode access	Set the layer 2 interface as access interface
(config-if)#switchport access vlan 100	Map the vlan 100 to access interface
(config-if)#exit	Exit interface mode.
(config)#interface xe41	Enter interface mode
(config-if)#switchport	Make it port as L2 interface
(config-if)# bridge-group 32 spanning-tree disable	Configure bridge group to l2 interface with spanning-tree disable
(config-if)#switchport mode access	Set the layer 2 interface as access interface
(config-if)#switchport access vlan 200	Map the VLAN 200 to access interface
(config-if)#exit	Exit interface mode.

RTR2

#configure terminal	Enter configure mode.
(config)#ip vrf vrf10	Create VRF instance with vrf10 and enter into vrf mode
(config-vrf)#exit	Exit from vRf mode
(config)#interface xe9/1	Enter interface mode
(config-if)#ip vrf forwarding vrf10	Enable vrf forwarding on interface
(config-if)#ip address 11.11.11.1/31	Assign IPv4 address in /31 mask.
(config-if)#ipv6 address 1000::2/64	Assign IPv6 address in /64 mask.
(config-if)#ipv6 router ospf area 0 tag vrf10	Tag ospfv3 instance on interface with vrf10 for area 0
(config-if)#exit	Exit interface mode.
(config)#router ospf 65535 vrf10	Enter into OSPF VRF configuration mode
(config-router)#router-id 3.3.3.3	Assign router ID 3.3.3.3 for OSPF process 65535

© 2021 IP Infusion Inc. Proprietary

(config-router)#bfd all-interfaces	Enable BFD for all-interface into OSPF
(config-router)#network 11.11.11.0/31 area 0	Enable routing for network 11.11.11.0/31 in area 0
(config-router)#exit	Exit from OSPF VRF configuration mode
(config)#router ipv6 vrf ospf vrf10	Enter into ipv6 OSPF VRF configuration mode
(config-router)#router-id 4.4.4.4	Assign router-id 4.4.4.4 for ipv6 OSPF process
(config-router)#bfd all-interfaces	Enable BFD for all-interface into OSPF
(config-router)#exit	Exit from ipv6 OSPF VRF configuration mode

Validation

RTR1

```
#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface   Instance ID
2.2.2.2           1   Full/Backup      00:00:35    10.1.1.2            xe23          0


#show bfd session

BFD process for VRF: (DEFAULT VRF)
=================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface  Down-
Reason  Remote-Addr
1                   1             IPv4        Single-Hop     Up         00:02:55
xe23       NA                  10.1.1.2/32
257                 0             IPv4        Multi-Hop      Up          00:00:18
xe8         NA                   3.3.3.3/32
Number of Sessions:    2


R1#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
=================================================================================

Session Interface Index : 10023          Interface name :xe23
Session Index : 1
Lower Layer : IPv4                              Version : 1
Session Type : Single Hop                  Session State : Up
Local Discriminator : 1                       Local Address : 10.1.1.1/32
Remote Discriminator : 1                   Remote Address : 10.1.1.2/32
Local Port : 49152                              Remote Port : 3784
Options :

Diagnostics : None
```

```
Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                    Neg Rx: 250                    Neg detect mult: 3
Min echo Tx: 1000          Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000814                  Pkt Out : 00000000000000000814
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                UPTIME : 00:02:59

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 0                    Session Index : 257
Lower Layer : IPv4                                 Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 257                      Local Address : 1.1.1.1/32
Remote Discriminator : 0                      Remote Address : 3.3.3.3/32
Local Port : 49153                                 Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                   Multiplier: 3
Neg Tx: 0                       Neg Rx: 0                       Neg detect mult: 0
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000000                Pkt Out : 00000000000000000107
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 0                                                UPTIME : 00:00:00

OcNOS#show bfd session vrf vrf10 detail
```


© 2021 IP Infusion Inc. Proprietary

```
BFD process for VRF: vrf10
========================================================================================

Session Interface Index : 4              Interface name :eth2
Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session

Counters values:
Pkt In : 00000000000000001184              Pkt Out : 00000000000000001184
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                               UPTIME : 00:04:21  State : Up
Local Discriminator : 1                  Local Address : 11.11.11.0/32
Remote Discriminator : 1                 Remote Address : 11.11.11.1/32
Local Port : 49152                       Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled
```

RTR2

```
#show ip ospf n

Total number of full neighbors: 2
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface  Instance ID
1.1.1.1           1   Full/DR          00:00:32      10.1.1.1           xe9/3       0
3.3.3.3           1   Full/Backup    00:00:40     20.1.1.2           xe17/1     0


#show bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface   Down-
Reason  Remote-Addr
1               1               IPv4            Single-Hop    Up         00:02:33
xe9/3            NA          10.1.1.1/32
2               1               IPv4            Single-Hop    Up         00:01:54
xe17/1          NA          20.1.1.2/32
```

```
Number of Sessions:    2


#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================

Session Interface Index : 10023          Interface name :xe9/3
Session Index : 1
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                     Local Address : 10.1.1.2/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
Local Port : 49152                            Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                   Multiplier: 3
Neg Tx: 250                   Neg Rx: 250                   Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000713               Pkt Out : 00000000000000000714
Pkts Drop : 00000000000000000000          Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000           IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                 UPTIME : 00:02:37

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
--------------------------------------------------------------

Session Interface Index : 10053          Interface name :xe17/1
Session Index : 2
Lower Layer : IPv4                            Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                     Local Address : 20.1.1.1/32
Remote Discriminator : 1                 Remote Address : 20.1.1.2/32
Local Port : 49153                            Remote Port : 3784
Options :

Diagnostics : None
```


© 2021 IP Infusion Inc. Proprietary

```
Timers in Milliseconds :
Min Tx: 250                   Min Rx: 250                    Multiplier: 3
Neg Tx: 250                   Neg Rx: 250                   Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000535              Pkt Out : 00000000000000000537
Pkts Drop : 00000000000000000000           Auth Pkts Drop : 00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out : 00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                               UPTIME : 00:01:58

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    2
```

RTR3

```
#show ip ospf n

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
2.2.2.2           1     Full/DR          00:00:36    20.1.1.1
xe17/10       0


#show bfd session

BFD process for VRF: (DEFAULT VRF)
================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface   Down-Reason  Remote-Addr
1                     2           IPv4             Single-Hop      Up
00:01:21    xe17/1             NA           20.1.1.1/32
257                    1           IPv4             Multi-Hop
Up         00:00:00      xe6                NA           1.1.1.1/32
Number of Sessions:    2
Total number of Established sessions 2


#show bfd session detail

BFD process for VRF: (DEFAULT VRF)
================================================================================

Session Interface Index : 10053          Interface name :xe17/1
Session Index : 1
```

```
Lower Layer : IPv4                              Version : 1
Session Type : Single Hop                    Session State : Up
Local Discriminator : 1                        Local Address : 20.1.1.2/32
Remote Discriminator : 2                     Remote Address : 20.1.1.1/32
Local Port : 49152                              Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                    Neg Rx: 250                    Neg detect mult:
3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000000391                  Pkt Out : 00000000000000000391
Pkts Drop : 00000000000000000000           Auth Pkts Drop :
00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000           IPv6 Pkt Out :
00000000000000000000
UP Count : 1                                                  UPTIME :
00:01:26

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 0                    Session Index : 257
Lower Layer : IPv4                                  Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 257                       Local Address : 3.3.3.3/32
Remote Discriminator : 1                      Remote Address : 1.1.1.1/32
Local Port : 49153                              Remote Port : 4784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                        Min Rx: 250                    Multiplier:
3
Neg Tx: 250                        Neg Rx: 250                    Neg detect
mult:250
Min echo Tx: 1000              Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
```

 © 2021 IP Infusion Inc. Proprietary

```
Pkt In : 00000000000000000000                    Pkt Out : 00000000000000000047
Pkts Drop : 00000000000000000000           Auth Pkts Drop :
00000000000000000000
Echo Out : 00000000000000000000            IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000          IPv6 Pkt Out :
00000000000000000000
UP Count : 0                                                    UPTIME :
00:00:00

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    2
```

BFD Over Static Routing IPv4 and IPv6

RTR1

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrf10`	Create vrf instance with vrf10 and enter into vrf mode
`(config-vrf)#exit`	Exit from vrf mode
`(config)#ip bfd vrf vrf10 static all-interfaces`	Enable global IPv4 bfd config for non-default vrf interfaces
`(config)#ipv6 bfd vrf vrf10 static all-interfaces`	Enable global IPv6 bfd config for non-default vrf interfaces
`(config)#interface xe53/1`	Enter interface mode
`(config-if)#ip vrf forwarding vrf10`	Enable vrf forwarding on interface
`(config-if)#ip address 11.11.11.0/31`	Assign IPv4 address in /31 mask.
`(config-if)#ipv6 address 1000::1/64`	Assign IPv6 address in /64 mask.
`(config-if)#exit`	Exit interface mode.
`(config)#ip route vrf vrf10 200.200.200.200/32 11.11.11.1 xe53/1`	Create IPv4 vrf static route for static bfd session
`(config)#ipv6 route vrf vrf10 2000::/64 1000::2 xe53/1`	Create IPv6 vrf static route for static bfd session
`(config)#exit`	Exit from configuration mode

RTR2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrf10`	Create vrf instance with vrf10 and enter into vrf mode
`(config-vrf)#exit`	Exit from vrf mode
`(config)#ip bfd vrf vrf10 static all-interfaces`	Enable global IPv4 bfd config for non-default vrf interfaces
`(config)#ipv6 bfd vrf vrf10 static all-interfaces`	Enable global IPv6 bfd config for non-default vrf interfaces

(config)#interface xe9/1	Enter interface mode for xe9/1
(config-if)#ip vrf forwarding vrf10	Enable vrf forwarding on interface
(config-if)#ip address 11.11.11.1/31	Assign IPv4 address in /31 mask.
(config-if)#ipv6 address 1000::2/64	Assign IPv6 address in /64 mask.
(config-if)#exit	Exit interface mode.
(config)# ip route vrf vrf10 100.100.100.100/32 11.11.11.0 xe9/1	Create IPv4 vrf static route for static bfd session
(config)# ipv6 route vrf vrf10 3000::2/64 1000::1 xe9/1	Create IPv6 vrf static route for static bfd session
(config)#exit	Exit from configuration mode

Validation

RTR1

```
#show bfd session vrf vrf10
 BFD process for VRF: vrf10
================================================================================
=============
Sess-Idx  Remote-Disc  Lower-Layer  Sess-Type  Sess-State  UP-Time  Inter-
face  Down-Reason  Remote-Addr
3                4             IPv4              Single-Hop      Up
00:14:13    xe53/ 1       NA              11.11.11.1/32
4                5             IPv6              Single-Hop      Up
00:13:24    xe53/ 1       NA              1000::2/128
Number of Sessions:    2


R1#show bfd session vrf vrf10 detail
BFD process for VRF: vrf10
================================================================================
==========

Session Interface Index : 4              Interface name :xe53/1
Session Index : 1
Lower Layer : IPv4                             Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                      Local Address : 11.11.11.0/32
Remote Discriminator : 1                 Remote Address : 11.11.11.1/32
Local Port : 49152                             Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                     Neg Rx: 250                     Neg detect
mult: 3
Min echo Tx: 1000          Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
```


© 2021 IP Infusion Inc. Proprietary

```
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000001184                    Pkt Out :
00000000000000001184
Echo Out : 0000000000000000000             IPv6 Echo Out :
0000000000000000000
IPv6 Pkt In : 0000000000000000000          IPv6 Pkt Out :
0000000000000000000
UP Count : 1                                                    UPTIME :
00:00:21

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------

Session Interface Index : 4              Interface name :xe53/1
Session Index : 2
Lower Layer : IPv6                             Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                      Local Address :
fe80::5054:ff:fed0:e0c1/128
Remote Discriminator : 2                 Remote Address :
fe80::5054:ff:fe3d:af2b/128
Local Port : 49153                             Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                      Min Rx: 250                    Multiplier: 3
Neg Tx: 250                     Neg Rx: 250                      Neg detect
mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000000000                     Pkt Out :
0000000000000000000
Echo Out : 0000000000000000000             IPv6 Echo Out :
0000000000000000000
IPv6 Pkt In : 00000000000000001158         IPv6 Pkt Out :
00000000000000001163
UP Count : 1                                     UPTIME : 00:00:14

Protocol Client Info:
OSPF6-> Client ID: 5     Flags: 4
------------------------------------------------------------
Number of Sessions:    2


R1#show bfd
BFD ID: 00      Start Time:Tue Mar 19 13:31:08 2019
```

```
 BFD Admin State: UP
Number of Sessions:    2
Slow Timer: 2000                      Image type: MONOLITHIC
Echo Mode: Disabled                BFD Notifications disabled
Next Session Discriminator:    3
```

RTR2

```
#show bfd session vrf vrf10
BFD process for VRF: vrf10
================================================================================
=======
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface  Down-Reason  Remote-Addr
4                  3                          IPv4              Single-Hop
Up       00:15:39    xe9/1       NA            11.11.11.0/32
5                  4                          IPv6              Single-Hop
Up          00:14:50      xe9/1          NA                1000::1/128
Number of Sessions:    2



R2#show bfd session vrf vrf10 detail
BFD process for VRF: vrf10
================================================================================
=======
Session Interface Index : 3              Interface name :xe9/1
Session Index : 1
Lower Layer : IPv4                             Version : 1
Session Type : Single Hop                 Session State : Up
Local Discriminator : 1                      Local Address : 11.11.11.1/32
Remote Discriminator : 1                  Remote Address : 11.11.11.0/32
Local Port : 49152                             Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                    Min Rx: 250                    Multiplier: 3
Neg Tx: 250                    Neg Rx: 250                    Neg detect
mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000001661                  Pkt Out : 00000000000000001665
Echo Out : 00000000000000000000           IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000         IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                                 UPTIME :
00:00:53

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
```


© 2021 IP Infusion Inc. Proprietary

```
    ------------------------------------------------------

    Session Interface Index : 3              Interface name :xe9/1
    Session Index : 2
    Lower Layer : IPv6                             Version : 1
    Session Type : Single Hop                Session State : Up
    Local Discriminator : 2                      Local Address :
    fe80::5054:ff:fe3d:af2b/128
    Remote Discriminator : 2                 Remote Address :
    fe80::5054:ff:fed0:e0c1/128
    Local Port : 49153                              Remote Port : 3784
    Options :

    Diagnostics : None

    Timers in Milliseconds :
    Min Tx: 250                    Min Rx: 250                    Multiplier: 3
    Neg Tx: 250                     Neg Rx: 250                   Neg detect
    mult: 3
    Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
    Storage type : 2
    Sess down time : 00:00:00
    Sess Down Reason : NA
    Bfd GTSM Disabled
    Bfd Authentication Disabled

    Counters values:
    Pkt In : 00000000000000000000                 Pkt Out : 00000000000000000000
    Echo Out : 00000000000000000000            IPv6 Echo Out :
    00000000000000000000
    IPv6 Pkt In : 00000000000000001642         IPv6 Pkt Out : 00000000000000001636
    UP Count : 1                                                 UPTIME :
    00:00:56

    Protocol Client Info:
    OSPF6-> Client ID: 5     Flags: 4
    ------------------------------------------------------------
    Number of Sessions:    2
```

RTR3

```
R3#show bfd
BFD ID: 00      Start Time:Mon Mar 18 15:55:46 2019
 BFD Admin State: UP
Number of Sessions:    2
Slow Timer: 2000                Image type: MONOLITHIC
Echo Mode: Disabled          BFD Notifications disabled
Next Session Discriminator:    3
```

© 2021 IP Infusion Inc. Proprietary

Bidirectional Forwarding Detection Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Bidirectional Forwarding Commands*
- Chapter 2, *Protocol Commands for BFD*
- Chapter 3, *BFD Static Route Commands*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Bidirectional Forwarding Commands

This chapter explains the commands used to configure Bidirectional Forwarding (BFD):

- accept-lifetime
- bfd auth type
- bfd
- bfd echo
- bfd echo interval
- bfd echo ipv4 source
- bfd-firmware
- bfd interval
- bfd multihop-peer
- bfd multihop-peer A.B.C.D interval
- bfd multihop-peer X:X::X:X interval
- bfd notification
- bfd session
- bfd slow-timer
- debug bfd
- hardware-profile micro-bfd
- key
- key chain
- key-string
- key-string encrypted
- send-lifetime
- show bfd
- show bfd interface
- show bfd session
- show bfd session A.B.C.D
- show bfd session ipv6
- show debugging bfd
- snmp restart bfd

© 2021 IP Infusion Inc. Proprietary

accept-lifetime

Use this command to specify the time period during which the authentication on a key chain is received as valid.

Use the `no` parameter with this command to negate this command.

Command Syntax

```
accept-lifetime HH:MM:SS MONTH <01-31> <1993-2035> HH:MM:SS MONTH <01-31> <1993-2035>
accept-lifetime HH:MM:SS MONTH <01-31> <1993-2035> infinite
accept-lifetime HH:MM:SS MONTH <01-31> <1993-2035> duration <1-2147483646>
no accept-lifetime
```

Parameters

`HH:MM:SS`	Specify the start time of accept-lifetime in hours, minutes and seconds.
`<01-31>`	Specify the day of the month to start. If the day is a single-digit, the leading 0 must be added, example: 01, 02, 03, etc.
`MONTH`	Specify the month of the year to start as the first three letters of the month with first letter in upper case, for example, Jan. (case sensitive).
`<1993-2035>`	Specify the year to start.
`HH:MM:SS`	Specify the end time of accept-lifetime in hours, minutes and seconds.
`<01-31>`	Specify the day of the month to end. If the day is a single-digit, the leading 0 must be added, example: 01, 02, 03, etc.
`MONTH`	Specify the month of the year to end as the first three letters of the month with first letter in caps, for example, Jan. (case sensitive).
`<1993-2035>`	Specify the year to end.
`duration`	Indicate the duration parameter.
`<1-2147483646>`	Specify the actual end time duration of a key in seconds.
`infinite`	Specify the end time to never expire.

Default

By default, accept-lifetime command is disabled

Command Mode

Keychain-key mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the setting of accept-lifetime for key1 on the key chain named mychain.

```
#configure terminal
(config)#key chain mychain
```

 © 2021 IP Infusion Inc. Proprietary

```
(config-keychain)#key 1
(config-keychain-key)#accept-lifetime 03:03:01 Dec 03 2004 04:04:02 Oct 06
2006
```

bfd auth type

Use this command to enable BFD authentication on an interface that has either an IPv4 or an IPv6 BFD session.

Use the `no` form of the command to disable BFD authentication.

Note: BFD authentication is not supported for single hop IPv4 sessions.

Command Syntax

```
bfd auth type (keyed-md5 | keyed-sha1 | meticulous-keyed-md5 | meticulous-keyed-
  sha1 | simple) key-id <0-255> <0|1> key (WORD)
no bfd auth
```

Parameters

`auth type`	Specify an authentication type.
`keyed-md5`	Specify a keyed message digest authentication type.
`simple`	Specify a simple authentication type.
`keyed-sha1`	Specify a keyed secure hashing algorithm authentication type.
`meticulous-keyed-md5`	Specify an authentication key meticulous keyed message digest authentication.
`meticulous-keyed-sha1`	Specify an authentication key meticulous keyed secure hashing algorithm authentication.
`key-id`	Indicate the `key-id` keyword.
`<0-255>`	Specify the key ID value.
`<0|1>`	0 Unencrypted password (key) 1 Encrypted password (key)
`key`	Indicate the `key` keyword.
`WORD`	Specify the authentication key name. Whitespaces is not allowed in key.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Do the following to configure a single-key support:

Use value 0 before the key parameter for plain text key.

Use value 1 before the key parameter for already encrypted key.

```
(config)#interface eth1
(config-if)#bfd auth type keyed-md5 key-id 10 0 key test-key
(config-if)#bfd auth type keyed-sha1 key-id 20 1 key 0x4d8ea8d7e9ee090b
```


© 2021 IP Infusion Inc. Proprietary

bfd

Use this command to enable and disable all the BFD sessions on this interface.

Command Syntax

```
bfd (enable|disable)
```

Parameters

`enable`	Enable BFD
`disable`	Disable BFD

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bfd disable
```

bfd echo

Use this command to set BFD sessions to echo mode.

Use the `no` form of the command to return a BFD session to its default mode.

Note: BFD echo mode is supported for IPv4 BFD single hop sessions only.

Command Syntax

```
bfd echo
no bfd echo
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bfd echo
```


© 2021 IP Infusion Inc. Proprietary

bfd echo interval

Use this command to set the BFD echo interval.

Use the `no` form of this command to reset the echo interval to its default value.

Command Syntax

```
bfd echo interval <50-4294967>
no bfd echo interval
```

Parameter

`<50-4294967>`	Transmit interval in milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command sets the BFD echo with no values.

```
#configure terminal
(config)#interface eth1
(config-if)#bfd echo interval 234
```

bfd echo ipv4 source

Use this command to set the echo ipv4 source address.

Use the `no` form of this command to reset the value.

Command Syntax

```
bfd echo ipv4 source A.B.C.D
no bfd echo ipv4 source
```

Parameter

`A.B.C.D`	Source IPv4 address.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following command displays the ipv4 source address value.

```
#configure terminal
(config)#interface eth1
(config-if)#bfd echo interval 234
(config-if)#bfd echo ipv4 source A.B.C.D
```


© 2021 IP Infusion Inc. Proprietary

bfd-firmware

Use this command to enable multi-hop or micro-BFD processing in hardware.

Note: For LAG interfaces, you must specify `micro-bfd`. With `micro-bfd` only single hop sessions are supported.

Command Syntax

```
bfd-firmware (multi-hop|micro-bfd)
```

Parameter

`multi-hop`	Enable multihop sessions
`micro-bfd`	Enable micro-BFD sessions (default)

Default

By default, micro-BFD sessions are enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bfd-firmware multi-hop
```

bfd interval

Use this command to configure BFD transmit and receive intervals, and the hello multiplier value.

Use the `no` form of the command to set the intervals and multiplier to their default values.

Command Syntax

```
bfd interval <3-999> minrx <3-999> multiplier <3-50>
no bfd interval
```

Parameters

`<3-999>`	Transmit interval in milliseconds.
`minrx`	Receive interval.
`<3-999>`	Receive interval in milliseconds.
`multiplier`	Hello multiplier.
`<3-50>`	Hello multiplier value.

Defaults

The default for the transmit and receive intervals is 250 milliseconds.

The default hello multiplier value is 3.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bfd interval 100 minrx 100 multiplier 5
(config-if)#
```


© 2021 IP Infusion Inc. Proprietary

bfd multihop-peer

Use this command to enable authentication over either a multihop IPv4 or IPv6 session

Use the `no` form of the command to disable BFD authentication.

Command Syntax

```
bfd multihop-peer (A.B.C.D | X:X::X:X) auth type (keyed-md5 | keyed-sha1 |
  meticulous-keyed-md5 | meticulous-keyed-sha1 | simple) key-id <0-255> <0|1> key
  (WORD)
no bfd multihop-peer (A.B.C.D) auth
```

Parameters

`A.B.C.D`	Specify an IPv4 address.
`X:X::X:X`	Specify
`auth type`	Specify an authentication type.
`simple`	Specify a simple authentication type.
`keyed-md5`	Specify a keyed message digest authentication type.
`keyed-sha1`	Specify a keyed secure hashing algorithm authentication type.
`meticulous-keyed-sha1`	Specify an authentication key Meticulous Keyed Secure hashing algorithm authentication type.
`meticulous-keyed-md5`	Specify an authentication key meticulous keyed message digest authentication.
`key-id`	Indicate the `key-id` keyword.
`<0-255>`	Specify the key ID value.
`<0|1>`	0 Unencrypted password (key) 1 Encrypted password (key)
`key`	Indicate the `key` keyword.
`WORD`	Specify the authentication key name. Whitespaces is not allowed in key.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Do the following to configure a single-key support:

Use value 0 before the key parameter for plain text key.

Use value 1 before the key parameter for already encrypted key.

```
#configure terminal
```

```
(config)#bfd multihop-peer 10.10.10.2 auth type keyed-md5 key-id 100 0 key
test-key
(config)#bfd multihop-peer 20.20.20.2 auth type keyed-sha1 key-id 200 1 key
0x4d8ea8d7e9ee090b
```


© 2021 IP Infusion Inc. Proprietary

bfd multihop-peer A.B.C.D interval

Use this command to configure IPv4 BFD multihop peer timer values.

Use the `no` form of the command to reset the IPv4 multihop peer timer value.

Command Syntax

```
bfd multihop-peer A.B.C.D interval <50-999> minrx <50-999> multiplier <3-50>
no bfd multihop-peer A.B.C.D interval
```

Parameters

`interval`	Indicate the interval parameter.
`<50-999>`	Specify the actual transmit interval in milliseconds.
`minrx`	Indicate the minrx parameter.
`<50-999>`	Specify the actual reception interval in milliseconds.
`multiplier`	Indicate the multiplier parameter.
`<3-50>`	Specify the actual hello multiplier value.

Command Mode

Configure mode

Default

Multiplier value is 3

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bfd multihop-peer 10.1.1.67 interval 100 minrx 100 multiplier 3
(config)#
```

bfd multihop-peer X:X::X:X interval

Use this command to configure an IPv6 BFD multihop peer timer values.

Use the `no` form of the command to reset the IPv6 multihop peer timer values.

Command Syntax

```
bfd multihop-peer X:X::X:X interval <50-999> minrx <50-999> multiplier <3-50>
no bfd multihop-peer X:X::X:X interval
```

Parameters

`interval`	Indicate the interval parameter.
`<50-999>`	Specify the actual transmit interval in milliseconds.
`minrx`	Indicate the minrx parameter.
`<50-999>`	Specify the actual reception interval in milliseconds.
`multiplier`	Indicate the multiplier parameter.
`<3-50>`	Specify the actual hello multiplier value.

Command Mode

Configure mode

Default

Default multiplier value is 3

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bfd multihop-peer 10.1.1.1 interval 100 minrx 100 multiplier 3
```


© 2021 IP Infusion Inc. Proprietary

bfd notification

Use this command to enable or disable BFD notification.

Command Syntax

```
bfd notification (enable | disable)
```

Parameters

`disable`	Disable BFD notification.
`enable`	Enable BFD notification.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bfd notification enable

(config)#bfd notification disable
```

bfd session

Use this command to create a BFD IPv4 or IPv6 session on an interface.

Use the no form of the command to delete a BFD session from an interface.

Command Syntax

```
interface <IFNAME>/bfd session (A.B.C.D | X:X::X:X) (A.B.C.D | X:X::X:X) (multihop)
  (non-persistent | admin-down | demand-mode)
```

Parameters

`A.B.C.D`	Source IPv4 address
`X:X::X:X`	Source IPv6 address
`multihop`	Multihop Session
`admin-down`	Administrative down session
`demand-mode`	Demand mode session
`non-persistent`	Non persistent session

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
OcNOS(config)#interface eth2
OcNOS(config-if)#bfd session 20.20.20.2 20.20.20.1 admin-down
OcNOS(config-if)#do sh run bfd
!
interface eth2
bfd session  20.20.20.2  20.20.20.1 admin-down
!
OcNOS(config-if)#no bfd session  20.20.20.2  20.20.20.1 admin-down
OcNOS(config-if)#do sh run bfd
!
interface eth2
bfd session  20.20.20.2  20.20.20.1
!
OcNOS(config-if)#bfd session 20.20.20.2 20.20.20.1 admin-down
OcNOS(config-if)#do sh run bfd
!
interface eth2
bfd session  20.20.20.2  20.20.20.1 admin-down
!
OcNOS(config-if)#no bfd session 20.20.20.2 20.20.20.1
OcNOS(config-if)#do sh run bfd
!
```


© 2021 IP Infusion Inc. Proprietary

bfd slow-timer

Use this command to set a BFD slow timer interval.

Use the `no` form of the command to reset the timer to default values.

Command Syntax

```
bfd slow-timer <1000-30000>
no bfd slow-timer
```

Parameter

`<1000-30000>`	Interval for the slow-timer in milliseconds

Command Mode

Configure mode

Default

Default slow-timer value is 2000

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bfd slow-timer 1500
(config)#
```

debug bfd

Use this command to enable debugging for BFD.

Use the `no` form of the command to disable all debugging for BFD.

Command Syntax

```
debug bfd (all|)
debug bfd (event|ipc-error|ipc-event|nsm|packet|session)
no debug bfd (all|)
no debug all
no debug bfd (event|ipc-error|ipc-event|nsm|packet|session)
```

Parameters

`all`	Enable all debugging.
`event`	Enable BFD event debugging.
`ipc-error`	Enable BFD IPC-error debugging
`ipc-event`	Enable BFD IPC-event debugging.
`nsm`	Enable BFD NSM debugging.
`packet`	Enable BFD packet debugging.
`session`	Enable BFD session debugging.

Command Mode

Exec, Privileged Exec and Configure Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug bfd all
#debug bfd event
#debug bfd ipc-error
#debug bfd ipc-event
#debug bfd nsm
#debug bfd packet
#debug bfd session
```


© 2021 IP Infusion Inc. Proprietary

hardware-profile micro-bfd

Use this command to enable micro-BFD support on hardware.

Note: Micro-bfd support is optional when a BFD session is configured over a LAG interface between two Qumran devices. It is mandatory to enable micro-bfd when the BFD session is configured over LAG interface between different platforms. When BFD sessions are configured over LAG interfaces, both Qumran nodes should have micro-bfd enabled or disabled.

Command Syntax

```
hardware-profile micro-bfd (enable|disable)
```

Parameter

`enable`	Enable micro-bfd support on Qumran
`disable`	Disable micro-bfd support on Qumran

Default

By default, micro-bfd support is disabled on Qumran.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)# hardware-profile micro-bfd enable
```

key

Use this command to manage, add or delete authentication keys in a key chain. This command allows you to enter the keychain-key mode to set a password for the key.

Command Syntax

```
key <0-2147483647>
no key <0-2147483647>
```

Parameters

`<0-2147483647>` Specify a key identifier.

Default

By default, BFD uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Command Mode

Keychain mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example configures a key number 1 and shows the change to keychain-key command mode.

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#
```


© 2021 IP Infusion Inc. Proprietary

key chain

Use this command to enter key chain mode to configure a key chain with a key chain name. This command allows you to enter the keychain mode to specify keys on this key chain.

Command Syntax

```
key chain WORD
no key chain WORD
```

Parameters

WORD	Specify the name of the key chain to manage.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the creation of a key chain named `mychain` and the change to keychain mode:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#
```

key-string

Use this command to define a password in plain-text to be used by a key.

The password is stored as encrypted, and is displayed in encrypted text when show running-config command is executed.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
key-string WORD
no key-string
```

Parameters

`WORD`	Specify a string of characters to be used as a password by the key. The length of the string should be between 1-80 characters.

Default

By default, password is not configured.

Command Mode

Keychain mode and Keychain-key mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following example, the password for `key 1` in the key chain named `mychain` is set to `prime`:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#key-string prime

(config-keychain)#key 1
(config-keychain-key)#no key-string
```


© 2021 IP Infusion Inc. Proprietary

key-string encrypted

Use this command to define a password in its encrypted format to be used by a key.

Use the `no` parameter with this command to disable this feature

Command Syntax

```
key-string encrypted WORD
no key-string encrypted
```

Parameters

`WORD`	Specify the encrypted string of characters to be used as a passoword by the key. The length of this string should be between 18-162 characters.

Default

By default, password is not configured.

Command Mode

Keychain mode and Keychain-key mode.

Applicability

This command was introduced in OcNOS version 4.1.

Examples:

In the following example, the encrypted password for key 1 in the key chain named mykeychain is set to 0xd6c50b442de47f70 (equivalent to "mychain" in plain-text):

```
#configure terminal
(config)#key chain mykeychain
(config-keychain)#key 1
(config-keychain-key)#key-string encrypted 0xd6c50b442de47f70
(config-keychain)#key 1
(config-keychain-key)#no key-string
```

send-lifetime

Use this command to specify the time period during which the authentication key on a key chain can be sent.

Use the `no` parameter with this command to negate this command.

Command Syntax

```
send-lifetime HH:MM:SS MONTH <01-31> <1993-2035> HH:MM:SS MONTH <01-31> <1993-2035>
send-lifetime HH:MM:SS MONTH <01-31> <1993-2035> infinite
send-lifetime HH:MM:SS MONTH <01-31> <1993-2035> duration <1-2147483646>
no send-lifetime
```

Parameters

`HH:MM:SS`	Specify the start time of send-lifetime in hours, minutes and seconds.
`<01-31>`	Specify the day of the month to start. If the day is a single-digit, the leading 0 must be added, example: 01, 02, 03, etc.
`MONTH`	Specify the month of the year to start as the first three letters of the month with first letter in upper case, for example, Jan. (case sensitive).
`<1993-2035>`	Specify the year to start.
`HH:MM:SS`	Specify the end time of send-lifetime in hours, minutes and seconds.
`<01-31>`	Specify the day of the month to end.
`MONTH`	Specify the month of the year to end as the first three letters of the month with first letter in upper case, for example, Jan. (case sensitive).
`<1993-2035>`	Specify the year to end.
`duration`	Indicate the duration parameter.
`<1-2147483646>`	Specify the actual end time duration of a key in seconds.
`infinite`	Specify the end time to never expire.

Command Mode

Keychain-key mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the setting of `send-lifetime` for `key 1` on the key chain named `mychain`:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#send-lifetime 03:03:01 Jan 03 2004 04:04:02 Dec 06 2006
```


© 2021 IP Infusion Inc. Proprietary

show bfd

Use this command to display information about the BFD process.

Command Syntax

```
show bfd
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd
BFD ID: 00      Start Time:Fri May 1 09:55:06 2009
Number of Sessions:     1
Slow Timer: 1000        Image type: MONOLITHIC
Echo Mode: Disabled     Next Session Discriminator:    2
#
```

Table 1-228 explains the output fields.

Table 1-228: show BFD fields

Entry	Description
BFD ID	ID number of the BFD session.
Start Time	The date and time when the BFD session was started
BFD Admin State	State of the BFD session: Initializing: session is initializing Up: session is up. Down: session is down
Number of Sessions	Number of BFD sessions running on the device.
Slow Timer	Required minimum transmission time for the BFD session.
Image Type	Distributed or Monolithic.
Echo Mode	Either enabled or disabled.
Next Session Discriminator	An opaque discriminator value that identifies each session on the device that is used to demultiplex multiple BFD sessions between the same pair of devices.

show bfd interface

Use this command to display details for an interface running BFD or for all interfaces configured for BFD.

Command Syntax

```
show bfd interface (ifindex <0-4294967295>|all|)
```

Parameters

`all`	Display all interfaces.
`ifindex`	Display an interface index.
`<0-4294967295>`	Display an ID of an interface in this range.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd interface all
Interface:         lo ifindex: 1 state:   UP
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5

Interface:       eth0 ifindex: 2 state:   UP
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5

Interface:       eth1 ifindex: 3 state: DOWN
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5

Interface:       sit0 ifindex: 4 state: DOWN
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5

Interface:       gre0 ifindex: 5 state: DOWN
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5
```


© 2021 IP Infusion Inc. Proprietary

Table 1-229 explains the output fields.

Table 1-229: show BFD interface fields

Entry	Description
interface	Interface on which BFD is running
ifindex	Interface index number
state	State of the BFD session for the interface: UP: session is up. DOWN: session is down
Interface level configuration	State of interface-level properties: echo on or off slow-timer (timer dampening) on or off
Min Tx	The minimum interval that the local device would like to use when transmitting BFD control packets.
Min Rx	The minimum interval between received BFD control packets that this device is capable of supporting
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving device in asynchronous mode.

show bfd session

Use this command to display BFD sessions.

Note: BFD Packet In and BFD Packet Out counters are not supported for Single Hop IPv4 BFD sessions on Qumran devices.

Command Syntax

```
show bfd session (detail|)
show bfd session vrf (WORD|all|default) (detail|)
```

Parameters

`detail`	Session details.
`WORD`	Sessions for this user-defined Virtual Routing and Forwarding instance name.
`all`	Show information for all Virtual Routing and Forwarding instances
`default`	Show information for only the default Virtual Routing and Forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bfd session detail
Session Interface Index : 3                Session Index : 1
Lower Layer : IPv4                         Version : 1
Session Type : Single Hop                  Session State : Down
Local Discriminator : 1                    Local Address : 19.19.19.2/32
Remote Discriminator : 0                   Remote Address : 19.19.19.1/32
Local Port : 49152                         Remote Port : 3784
Options :

Diagnostics: None

Timers in Milliseconds :
Min Tx: 20              Min Rx: 20              Multiplier: 5
Neg Tx: 0               Neg Rx: 0               Neg detect mult: 0
Min echo Tx: 20         Min echo Rx: 10         Neg echo intrvl: 0
Storage type: 2
Sess down time: 00:00:00
Bfd Authentication Enabled
Authentication type : simple
Auth-Key-Id: 47

Counters values:
Pkt In : 0000000000000000                  Pkt Out : 0000000000000011
Echo Out : 0000000000000000                IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000             IPv6 Pkt Out : 0000000000000000
UP Count : 0                               UPTIME : 00:00:00
```

 © 2021 IP Infusion Inc. Proprietary

```
Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------


#show bfd session vrf all

BFD process for VRF: vrf1
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface      Down-Reason  Remote-Addr
1          1           IPv4         Single-Hop  Up          00:05:38  eth1
NA           1.1.1.2/32
Number of Sessions:    1

BFD process for VRF: (DEFAULT VRF)
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface      Down-Reason  Remote-Addr
1          7           IPv4         Single-Hop  Up          00:03:31  eth3
NA           3.3.3.2/32
2          9           IPv4         Single-Hop  Up          00:00:45  eth4
NA           4.4.4.2/32
Number of Sessions:    2

BFD process for VRF: vrf2
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time
Interface      Down-Reason  Remote-Addr
1          6           IPv4         Single-Hop  Up          00:03:37  eth2
NA           2.2.2.2/32
Number of Sessions:    1
```

Table 1-230 explains the output fields.

Table 1-230: show bfd session detail fields

Entry	Description
Session Interface Index	ID number of the interface.
Session Index Sess-Idx	ID number of this BFD session.
Lower Layer	The lower layer protocol on which BFD is carried: IPv4 IPv6 MPLS LSP MPLS VCCV MPLS-TP
Version	Session version number; generally 1.

Table 1-230: show bfd session detail fields (Continued)

Entry	Description
Session Type Sess-Type	Single Hop Multihop Arbit Path Multihop OOB Signalled Multihop Unidirectional.
Session State Sess-State	The State of the session: Init: The session is initializing Up: The session is up. Down: The session is down AdminDown: The session has been administratively shutdown indefinitely.
Local Discriminator	A unique discriminator value generated by the transmitting device used to demultiplex multiple BFD sessions between the same pair of devices.
Local Address	Local address of the transmitting device.
Remote Discriminator Remote-Disc	The discriminator received from the corresponding remote device; zero if that value is unknown.
Remote Address Remote-Addr	Remote address of the receiving device.
Local Port	UDP port number of the transmitting device.
Remote Port	UDP port number of destination.
Options	Fate Shared Echo Enabled Demand Enabled Remote Demand Enbl Remote admin Down Poll seq Init.
Diagnostics	Performance diagnostics: None Control Detection Time Expired Echo Failed Neighbor Session Down Forwarding Plane Reset Path Down Concatenated Path Down Admin Down Reverse Concatenated Path Down
Min Tx	Minimum transmit interval.
Min Rx	Minimum receive interval.
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving system in asynchronous mode.
Neg Tx	Negotiated transmit interval.
Neg Rx	Negotiated receive interval in milliseconds.

© 2021 IP Infusion Inc. Proprietary

Table 1-230: show bfd session detail fields (Continued)

Entry	Description
Neg detect mult	Negotiated detection multiplier.
Min echo Tx	Minimum echo transmit interval in milliseconds.
Min echo Rx	Minimum echo receive interval in milliseconds.
Neg echo intrvl	Negotiated echo interval.
Storage type	SNMPv2 storage type (usually be set to 2): other(1) volatile(2) non-Volatile(3) permanent(4 read-Only(5)
Sess down time	Length of time this BFD session has been down.
Bfd GTSM	Whether the BFD session has enabled or disabled the Generalized TTL Security Mechanism (GTSM), which uses the time to live (TTL) or hop count to prevent off-link attackers from spoofing packets.
Bfd Authentication Enabled	When authentication is enabled.
Authentication type	Type of authentication: simple: Simple Password keyed-md5: Keyed message digest keyed-sha1: Keyed Secure hashing algorithm meticulous-keyed-md5: Meticulous Keyed message digest meticulous-keyed-sha1: Meticulous Keyed Secure hashing algorithm
Authentication Key-id	ID number of the authentication key.
Pkt In	Number of packets that have been received during this BFD session.
Pkt Out	Number of packets that have been transmitted during this BFD session.
Echo Out	Number of Echo-packets that have been transmitted during this BFD session.
IPv6 Pkt In	Number of IPv6 packets that have been received during this BFD session.
IPv6 Pkt Out	Number of IPv6 packets that have been transmitted during this BFD session.
UP Count	Number of times the BFD session has been up.
UPTIME	Length of time this BFD session has been up.
BGP-> Client ID	Protocol and module ID number of this BFD session’s neighboring device.
Flags	Session state of the neighboring device.
Interface	The interface on which the VRF resides.
Down-Reason	The reason causing the VRF to be down.

show bfd session A.B.C.D

Use this command to display information about an IPv4 BFD session neighbor.

Command Syntax

```
show bfd session A.B.C.D A.B.C.D (detail|)
show bfd session vrf WORD A.B.C.D A.B.C.D (detail|)
show bfd session A.B.C.D A.B.C.D <0-4294967295> (detail|)
show bfd session vrf WORD A.B.C.D A.B.C.D <0-4294967295> (detail|)
```

Parameters

WORD	Name of a specific Virtual Routing and Forwarding instance
A.B.C.D	Display the local IPv4 address.
A.B.C.D	Display the neighbor IPv4 address.
<0-4294967295>	Display the interface index of the address.
detail	Display detailed information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd session 10.1.1.66 10.1.1.67 3
Session Interface Index: 3     Session Index: 1
Lower Layer: IPv4     Single Hop
Session State: Up
Local Discriminator: 1 Remote Discriminator: 163
Local Address: 10.1.1.66/32    Remote Address: 10.1.1.67/32
Local Port: 49152      Remote Port: 3784
Timers in Milliseconds
Min Tx: 1000 Min Rx: 1000 Multiplier: 4
UP Count: 1 UPTIME: 00:10:08


#show bfd session vrf raj 130.1.1.1 130.1.1.2 detail

Session Interface Index : 10017          Interface name :xe16
Session Index : 2
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                  Local Address : 130.1.1.1/32
Remote Discriminator : 2                 Remote Address : 130.1.1.2/32
Local Port : 49153                       Remote Port : 3784
Options :
```

 © 2021 IP Infusion Inc. Proprietary

```
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : n/a                                  Pkt Out : n/a
Pkts Drop : 00000000000000000000              Auth Pkts Drop :
00000000000000000000
Echo Out : 00000000000000000000               IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000000000            IPv6 Pkt Out : 00000000000000000000
UP Count : 1                                  UPTIME : 00:01:38

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
```

Table 1-231 explains the output fields.

Table 1-231: Show BFD session fields

Entry	Description
Session Interface Index	ID number of the Interface.
Session Index	ID number for this BFD session.
Lower Layer	The lower layer protocol on which BFD is carried (IPv4 or IPv6).
Session State	The state of the session: Init: session is initializing Up: session is up. Down: session is down AdminDown: session has been administratively shutdown indefinitely
Local Discriminator	A unique value generated by the transmitting device used to demultiplex multiple BFD sessions between the same pair of devices.
Remote Discriminator	The discriminator received from the corresponding remote device. This field is zero if the value is unknown.
Local Address	Local address of the transmitting device.
Remote Address	Remote address of the receiving device.
Local Port	UDP port number of the transmitting device.
Remote Port	UDP port number of the receiving device.
Min Tx	Minimum transmit interval in milliseconds.

Table 1-231: Show BFD session fields

Entry	Description
Min Rx	Minimum receive interval in milliseconds.
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving system in asynchronous mode.
UP Count	The number of times the BFD session has been in up state.
UPTIME	The length of time this BFD session has been in the up state.

© 2021 IP Infusion Inc. Proprietary

show bfd session ipv6

Use this command to display information about an IPv6 BFD session neighbor.

Command Syntax

```
show bfd session ipv6 X:X::X:X X:X::X:X (detail|)
show bfd session ipv6 vrf WORD X:X::X:X X:X::X:X (detail|)
show bfd session ipv6 X:X::X:X X:X::X:X <0-4294967295> (detail|)
show bfd session ipv6 vrf WORD X:X::X:X X:X::X:X <0-4294967295> (detail|)
```

Parameters

WORD	Name of a specific Virtual Routing and Forwarding instance
X:X::X:X	Display the local IPv6 address.
X:X::X:X	Display the neighbor IPv6 address.
<0-4294967295>	Display the interface index of the address.
detail	Display detailed information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd session 2001::1222 2001::1223 3
Session Interface Index : 3     Session Index: 1
Lower Layer: IPv6     Single Hop
Session State : Up
Local Discriminator : 1 Remote Discriminator: 163
Local Address : 2001::1222/128    Remote Address: 2001::1223/128
Local Port : 49152      Remote Port: 3784
Timers in Milliseconds
Min Tx: 1000 Min Rx: 1000 Multiplier: 4
UP Count: 1 UPTIME: 00:06:03


#show bfd session ipv6 vrf raj fe80::ba6a:97ff:fed3:26c5
fe80::ba6a:97ff:fece:3bc5 detail

Session Interface Index : 10017          Interface name :xe16
Session Index : 259
Lower Layer : IPv6                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 259                Local Address :
fe80::ba6a:97ff:fed3:26
c5/128
```

```
Remote Discriminator : 257              Remote Address :
fe80::ba6a:97ff:fece:3
bc5/128
Local Port : 49152                      Remote Port : 3784
Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250             Min Rx: 250             Multiplier: 3
Neg Tx: 250             Neg Rx: 250             Neg detect mult: 3
Min echo Tx: 1000       Min echo Rx: 1000       Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess Down Reason : NA
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : n/a                            Pkt Out : n/a
Pkts Drop : 00000000000000000000        Auth Pkts Drop :
00000000000000000000
Echo Out : 00000000000000000000         IPv6 Echo Out :
00000000000000000000
IPv6 Pkt In : 00000000000000001671      IPv6 Pkt Out : 00000000000000001675
UP Count : 1                            UPTIME : 00:06:05

Protocol Client Info:
OSPF6-> Client ID: 5    Flags: 4
```

Table 1-232 explains the output fields.

Table 1-232: show BFD session fields

Entry	Description
Session Interface Index	ID number of the Interface.
Session Index	ID number for this BFD session.
Lower Layer	The lower layer protocol on which BFD is carried (IPv4 or IPv6).
Session State	The state of the session: Init: session is initializing Up: session is up. Down: session is down AdminDown: session has been administratively shutdown indefinitely
Session Type	Whether the session is Single Hop or Multiple Hop
Local Discriminator	A unique value generated by the transmitting device used to demultiplex multiple BFD sessions between the same pair of devices.
Remote Discriminator	The discriminator received from the corresponding remote device. This field is zero if the value is unknown.

© 2021 IP Infusion Inc. Proprietary

Table 1-232: show BFD session fields

Entry	Description
Local Address	Local address of the transmitting device.
Remote Address	Remote address of the receiving device.
Local Port	UDP port number of the transmitting device.
Remote Port	UDP port number of the receiving device.
Min Tx	Minimum transmit interval in milliseconds.
Min Rx	Minimum receive interval in milliseconds.
Min echo Tx	Minimum transmit interval for echo packets
Min echo Rx	minimum receive interval for echo packets
Neg echo intrvl	The negotiated
Storage type	Indicates the storage type: 1 = other 2 = volatile 3 = nonvolatile 4 = permanent 5 = read only
Sess down time	How long the session was down
Sess Down Reason	Reason for Session being down
Bfd GTSM	Whether Generalized TTL Security Mechanism (GTSM) is enabled or disabled on the connection.
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving system in asynchronous mode.
UP Count	Number of times the BFD session has been in up state.
UPTIME	Length of time this BFD session has been in the up state.
Bfd Authentication	If authentication is used, if yes, the type authentication: simple password, MD5, and so on.
Pkt In	Number of Packets received on the BFD session
Pkt Out	Number of packets transmitted on the BFD session
Pkts Drop	Number of packets dropped on the session
Auth Pkts Drop	Number of Authentication packets dropped
Echo Out	Number of Transmitted BFD Echo Packets
IPv6 Echo Out	Number of transmitted BFD Ipv6 Echo packets
IPv6 Pkt In	Number of received IPv6 BFD packets
IPv6 Pkt Out	Number of transmitted IPV6 BFD packets
Protocol Client Info	Client ID and flags

show debugging bfd

Use this command to display debugging information for BFD processes.

Command Syntax

```
show debugging bfd
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show debugging bfd
BFD debugging status:
BFD events debugging is on
BFD packet debugging is on
BFD ipc-error debugging is on
BFD ipc-event debugging is on
BFD session debugging is on
BFD nsm debugging is on
#
```


© 2021 IP Infusion Inc. Proprietary

snmp restart bfd

Use this command to restart SNMP in Bidirectional Forwarding (BFD)

Command Syntax

```
snmp restart bfd
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart bfd
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Protocol Commands for BFD

The chapter describes the commands used to manage BFD functionality for OSPF, IS-IS and BGP.

- area virtual-link
- bfd all-interfaces
- debug bgp bfd
- debug isis bfd
- debug ospf bfd
- ip ospf bfd
- isis bfd

area virtual-link

Use this command to enable the BFD option for a specified virtual-link neighbor.

Use the `no` form of the command to disable BFD on a virtual-link neighbor.

Command Syntax

```
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}
```

Parameters

`A.B.C.D`	Indicate an area IP address
`<0-429467295>`	Indicate an area ID in integer format
`virtual-link`	Indicate a virtual link and its parameters
`A.B.C.D`	Indicate the IP address of the virtual link
`fall-over`	Indicate fall-over detection
`bfd`	Specify the Bidirectional Forwarding Detection (BFD)

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ospf
(config-router)#area 1 virtual-link 192.168.0.1 fall-over bfd
```


© 2021 IP Infusion Inc. Proprietary

bfd all-interfaces

Use this command to enable BFD for all neighbors maintained by an OSPF process or an ISIS instance.

Use the `no` form of the command to disable BFD.

Note: This command does not apply BFD to virtual-link neighbors.

Command Syntax

```
bfd all-interfaces
no bfd all-interfaces
```

Parameters

None

Default

By default, bfd all interface is disabled

Command Mode

Configure router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ospf
(config-router)#bfd all-interfaces

#configure terminal
(config)#router isis
(config-router)#bfd all-interfaces
```

debug bgp bfd

Use this command to debug BFD processes in BGP.

Use the `no` form of the command to stop debugging.

Command Syntax

```
debug bgp bfd
no debug bgp bfd
undebug bgp bfd
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug bgp bfd
```


© 2021 IP Infusion Inc. Proprietary

debug isis bfd

Use this command to debug BFD processes in IS-IS.

Use the `no` form of the command to stop debugging.

Command Syntax

```
debug isis bfd
no debug isis bfd
undebug isis bfd
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug isis bfd
```

debug ospf bfd

Use this command to debug BFD processes in OSPF.

Use the `no` form of the command to stop debugging.

Command Syntax

```
debug ospf bfd
no debug ospf bfd
undebug ospf bfd
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ospf bfd
```


© 2021 IP Infusion Inc. Proprietary

ip ospf bfd

Use this command to enable the BFD option for OSPF neighbors on an interface. Use the `no` form of the command to disable the BFD option for OSPF neighbors on an interface.

Note: When BFD monitoring is enabled for ospf session, protocol admin events like clear/ shutdown will cause BFD session to go to admin down.Due to this, neigbourship/adjacency down detection on peer will be according to the protocol configured dead interval and is not based on BFD interval.

Command Syntax

```
ip ospf bfd (disable|)
no ip ospf bfd (disable|)
```

Parameter

`disable`	Disable the BFD option for neighbors on an interface

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip ospf bfd
```

isis bfd

Use this command to enable the BFD option for IS-IS neighbors on an interface. Use the `no` form of the command to disable the BFD option for neighbors on an interface.

Note: When BFD monitoring is enabled for ISIS session, protocol admin events like clear/ shutdown will cause BFD session to go to admin down. Due to this, neigbourship/adjacency down detection on peer will be according to the protocol configured hello hold interval and is not based on BFD interval.

Command Syntax

```
isis bfd (disable|)
no isis bfd (disable|)
```

Parameter

`disable`	Used to disable the BFD option for neighbors on an interface

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis bfd disable
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 BFD Static Route Commands

Bidirectional Forwarding Detection (BFD) support for static routes can be configured on a static route basis, interface basis, or on a global level:

- When BFD is configured for an IPv4 or IPv6 static route, BFD provides the next-hop reachability detection for the given static route.
- When BFD is configured for an interface, BFD provides the data plane next-hop reachability information for any IPv4 or IPv6 static route configured through the given interface.
- When BFD is configured globally, BFD is applied on all interfaces with a single command. In all these cases, the BFD session update for NSM governs the state of the static routes.

This chapter includes the following commands:

- ip bfd static all-interfaces
- ip static fall-over-bfd
- ip static bfd
- ipv6 bfd static all-interfaces
- ipv6 static fall-over-bfd
- ipv6 static bfd

© 2021 IP Infusion Inc. Proprietary

ip bfd static all-interfaces

Use this command to enable BFD support for IPv4 static routes configured on all interfaces.

Use the `no` option with this command to disable BFD support for IPv4 static routes configured on all interfaces.

Command Syntax

```
ip bfd static all-interfaces
ip bfd vrf NAME static all-interfaces
no ip bfd static all-interfaces
no ip bfd vrf NAME static all-interfaces
```

Parameters

`NAME`	Enable/disable IPv4 static BFD on all interfaces bound to this user-defined Virtual Routing and Forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.5.

Example

```
#configure terminal
(config)#ip bfd static all-interfaces

#configure terminal
(config)#ip  bfd  vrf vrf1 static all-interfaces
```


© 2021 IP Infusion Inc. Proprietary

ip static fall-over-bfd

Use this command to enable BFD support for a specific IPv4 static route.

Use the `no` form of the command to disable the BFD support for a specific IPv4 static route.

Command Syntax

```
ip static A.B.C.D/M A.B.C.D fall-over-bfd (disable|enable)
no ip static A.B.C.D/M A.B.C.D
ip static vrf NAME A.B.C.D/M A.B.C.D fall-over-bfd (disable|enable)
no ip static vrf NAME A.B.C.D/M A.B.C.D
```

Parameters

`A.B.C.D/M`	The IPv4 destination prefix and mask length.
`A.B.C.D`	The IPv4 gateway address.
`disable`	Disable BFD.
`enable`	Enable BFD.
`NAME`	Enable/disable BFD for the IPv4 routes for this user-defined Virtual Routing and Forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.5.

Example

```
#configure terminal
(config)#ip static A.B.C.D/M A.B.C.D fall-over-bfd disable

#configure terminal
(config)# ip static vrf vrf1 A.B.C.D/M A.B.C.D fall-over-bfd enable
```

ip static bfd

Use this command to enable or disable BFD support for IPv4 static route(s) configured on an interface.

Use the `no` option with this command to reset BFD support for IPv4 static route(s) configured on an interface.

Command Syntax

```
ip static bfd (disable|enable)
no ip static bfd
```

Parameters

`disable`	Disable BFD
`enable`	Enable BFD

Command Mode

Interface mode

Default

By default, BFD static route support is disabled at all levels.

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip static bfd disable

(config)#interface eth1
(config-if)#ip static bfd enable
```


© 2021 IP Infusion Inc. Proprietary

ipv6 bfd static all-interfaces

Use this command to enable BFD support for IPv6 static routes on all interfaces.

Use the `no` option with this command to disable BFD support for IPv6 static routes on all interfaces.

Command Syntax

```
ipv6 bfd static all-interfaces
ipv6 bfd vrf NAME static all-interfaces
no ipv6 bfd static all-interfaces
no ipv6 bfd vrf NAME static all-interfaces
```

Parameters

`NAME`	Enable/disable IPv6 static BFD on all interfaces bound to this user-defined Virtual Routing and Forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.5.

Example

```
#configure terminal
(config)#ipv6 bfd static all-interfaces

#configure terminal
(config)#ipv6 bfd vrf vrf1 static all-interfaces
```

ipv6 static fall-over-bfd

Use this command to enable BFD support for a specific IPv6 static route.

Use the `no` option with this command to disable BFD support for a specific IPv6 static route.

Command Syntax

```
ipv6 static X:X::X:X/M X:X::X:X fall-over-bfd (disable|enable)
no ipv6 static X:X::X:X/M X:X::X:X
ipv6 static vrf NAME X:X::X:X/M X:X::X:X fall-over-bfd (disable|enable)
no ipv6 static vrf NAME X:X::X:X/M X:X::X:X
```

Parameters

`X:X::X:X/M`	The IPv6 destination prefix and mask length.
`X:X::X:X`	The IPv6 gateway address.
`NAME`	Enable/disable BFD for the IPv6 routes for this user-defined Virtual Routing and Forwarding instance name.
`disable`	Disable BFD.
`enable`	Enable BFD.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.5.

Examples

```
#configure terminal
(config)#ipv6 static X:X::X:X/M X:X::X:X fall-over-bfd disable

#configure terminal
(config)#ipv6 static X:X::X:X/M X:X::X:X fall-over-bfd enable

#configure terminal
(config)#ipv6 static vrf vrf1 X:X::X:X/M X:X::X:X fall-over-bfd disable
```


© 2021 IP Infusion Inc. Proprietary

ipv6 static bfd

Use this command to disable BFD support for IPv6 static route(s) configured on an interface.

Use the `no` option with this command to reset BFD support for IPv6 static route(s) configured on an interface.

Command Syntax

```
ipv6 static bfd (disable|enable)
no ipv6 static bfd
```

Parameters

`disable`	Disable BFD
`enable`	Enable BFD

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 static bfd disable
```

© 2021 IP Infusion Inc. Proprietary

SECTION 12 Quality of Service

Quality of Service Configuration Guide

Contents

This document contains these chapters.

- Chapter 1, *QoS Introduction*
- Chapter 2, *Dscp-to-queue Map Profile Configuration*
- Chapter 3, *Cos-to-queue Map Configuration*
- Chapter 4, *Queue-color-to-cos Map Profile Configuration*
- Chapter 5, *Queue-color-to-dscp Map Profile Configuration*
- Chapter 6, *Trust DSCP on Layer 2 Interface Configuration*
- Chapter 7, *Service based Queue Distribution Configuration*
- Chapter 8, *Weights for Queues Configuration*
- Chapter 9, *Marking/Remarking Configuration*
- Chapter 10, *Policing Configuration*
- Chapter 11, *Bandwidth Configuration*
- Chapter 12, *Shaping Configuration*
- Chapter 13, *Scheduling Configuration*
- Chapter 14, *WRED Configuration*
- Chapter 15, *Tail-Drop Configuration*
- Chapter 16, *Hierarchical Queuing Configuration*
- Chapter 17, *VXLAN Quality of Service*
- Chapter 18, *FP Rules Queuing Configuration*
- Chapter 19, *Explicit Congestion Notification (ECN) Configuration*
- Chapter 20, *Rate Limiting BUM Traffic*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 QoS Introduction

This chapter contains a general overview of QoS functionality and terminology.

QoS Functionality

Quality of Service (QoS) can be used to give certain traffic priority over other traffic. Without QoS, all traffic in a network has the same priority and chance of being delivered on time. If congestion occurs, all traffic has the same chance of being dropped. With QoS, specific network traffic can be prioritized to receive preferential treatment. In turn, a network performs more predictably, and utilizes bandwidth more effectively.

QoS is based on DiffServ architecture, which stipulates that individual packets be classified upon entry into a network. Classification information can be carried in the Layer-3 IP packet header or the Layer-2 frame. IP packet headers carry the information using 6-bits from the deprecated IP type of service (TOS) field. Layer-2 802.1Q frames carry the information using a 2-byte Tag Control Information field. All switches and routers accessing the Internet depend on class information to give the same forwarding treatment to packets with the same class information, and give different treatment to packets with different class information. A packet can be assigned class information, as follows:

- End hosts or switches along a path, based on a configured policy
- Detailed packet examination, expected to occur nearer to the network edge, to prevent overloading core switches and routers
- A combination of the above two techniques

Class information can be used by switches and routers along a path to limit the amount of allotted resources per traffic class. Per-hop behavior is an individual device's behavior when handling traffic in the DiffServ architecture. An end-to-end QoS solution can be created if all devices along a path have consistent per-hop behavior.

Terminology

Following is a brief description of terms and concepts used to describe QoS.

ACL

Access control lists (ACLs) classify traffic with the same characteristics. IP traffic is classified using IP standard or IP extended ACLs. The ACL can have multiple access control entries (ACEs), which are commands that match fields against the contents of the packet. It is not possible to match IP fragments against configured IP extended ACLs to enforce QoS, but it is possible to match IP options against configured IP extended ACLs to enforce QoS.

CoS Value

Class of Service (CoS) is a 3-bit value used to classify the priority of Layer-2 frames upon entry into a network. QoS classifies frames by assigning priority-indexed CoS values to them, and gives preference to higher-priority traffic. Layer-2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, called the User Priority bits. On interfaces configured as Layer-2 802.1Q trunks, all traffic is in 802.1Q frames, except for traffic in the native VLAN. Other frame types cannot carry Layer-2 CoS values. CoS values range from zero to seven, seven being the highest priority.

© 2021 IP Infusion Inc. Proprietary

DSCP Value

Differentiated Services Code Point (DSCP) is a 6-bit value used to classify the priority of Layer-3 packets upon entry into a network. DSCP values range from 0 to 63, 63 being the highest priority, 0 being best-effort traffic.

Classification

Classification distinguishes one kind of traffic from another by examining the fields in the packet. The process generates an internal DSCP for a packet, which identifies all future QoS actions to be taken on the packet. Each packet is classified upon entry into the network. At the ingress, the packet is inspected, and the DSCP is determined based on ACLs or the configuration. The Layer-2 CoS value is then mapped to a DSCP value. The classification is carried in the IP packet header using 6 bits from the deprecated IP TOS field to carry the classification information. Classification can also occur in the Layer-2 frame. Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, thus, no classification occurs. Classification occurs on an ingress physical port, but not at the switch virtual interface level. Classification can be based on QoS ACLs, or class maps and policy maps.

Policing

Policing determines whether a packet is in or out of profile by comparing the internal DSCP to the configured policer. Policer limits the bandwidth consumed by a traffic flow with the results given to the marker. The two types of policers:

- Individual: QoS applies the bandwidth limits specified in the policer, separately, to each matched traffic class. An individual policer is configured within a policy map.
- Aggregate: QoS applies the bandwidth limits specified in an aggregate policer, cumulatively, to all matched traffic flows. An aggregate policer is configured by specifying the policer name within a policy map. The bandwidth limits of the policer are specified. In this way, multiple classes of traffic across policy map share the aggregate policer.

Policing and policers have the following attributes:

- Policers can occur only on a physical port basis.
- Policing can occur on ingress interfaces.
- Only one policer can be applied to a packet per direction.

Marking

Marking determines how to handle a packet when it is out of profile. It assesses the policer and the configuration data to determine the action required for the packet, and then handles the packet using one of the following methods:

- Let the packet through without modification
- Drop the packet

Marking can occur on ingress and egress interfaces.

Queuing

Queuing maps packets to a CoS queue. Each egress port can accommodate up 8 CoS queues, prioritized as 0 lowest and 7 highest. The tagged packet incoming priority can be mapped to one of the 8 queues obtained from the filtering mechanism result. The untagged packet CoS priority is also obtained from the filtering mechanism result. After the packets are mapped to a CoS queue, they are scheduled.

© 2021 IP Infusion Inc. Proprietary

Bandwidth Reservation

Bandwidth reservation is the minimum guaranteed bandwidth allocated per queue. Total guaranteed bandwidth of all the queues belonging to a particular port should not exceed the interface Bandwidth. In case if no Bandwidth reservation is done for the queue, minimum guaranteed per each queue will be 1% of the parent node [scheduling node or interface]

Scheduling

Scheduling forwards or conditions packets using one of the following methods:

- Strict Priority-Based (SP), in which any high-priority packets are first transmitted. Lower-priority packets are transmitted only when the higher-priority queues are empty. A problem may occur when too many lower-priority packets are not transmitted. Strict Priority will be operating on the remaining bandwith available for the Port
- Weighted Round Robin (WRR), in which each queue is assigned a weight to control the number of packets relatively sent from each queue.The weights assigned for the queues will be in the ratio of bandwidth reservation of those queues
- Combination of WRR and SP, the Remaining Bandwidth will be scheduled in the strict order for the SP Queues. The Remaining Bandwidth will be scheduled in the WRR mode for WRR Queues.

Class Map

A class map names and isolates specific traffic from other traffic. The class map defines the criteria used to match against a specific traffic flow to classify it further. The criteria can include:

- Matching the access group defined by the ACL
- Matching a specific list of DSCP values

If there is more than one type of traffic to be classified, another class map can be created under a different name. After a packet is matched against the class-map criteria, it is further classified using a policy map.

Policy Map

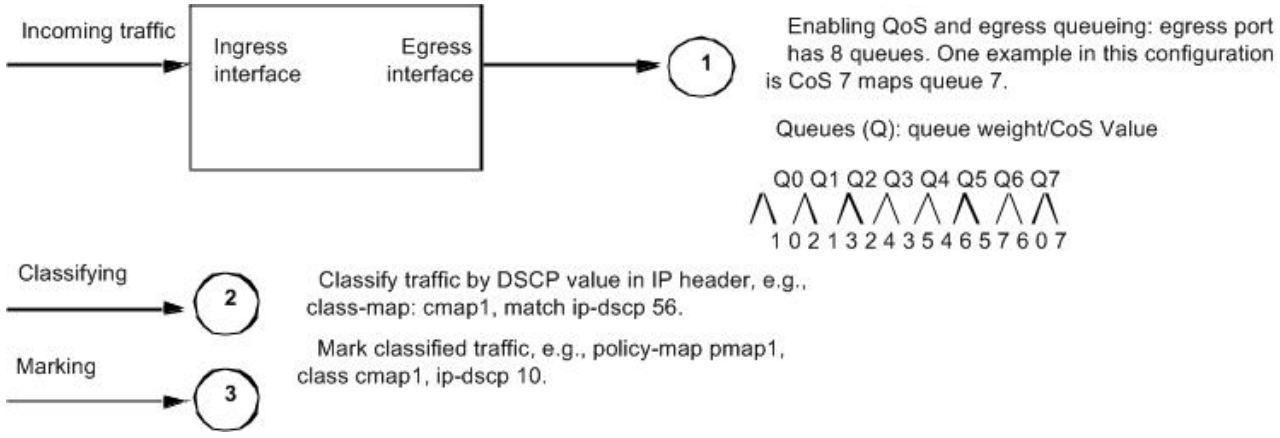
A policy map specifies on which traffic class to act. This can be implemented as follows:

- Set a specific CoS or DSCP value in the traffic class.
- Specify the traffic bandwidth limitations for each matched traffic class (policer) and the action to take (marking) when the traffic is out of profile.

Policy maps have the following attributes:

- A policy map can contain multiple class statements, each with different match criteria and policers.
- A separate policy-map class can exist for each type of traffic received through an interface.
- There can be only one policy map per interface per direction. The same policy map can be applied to multiple interfaces and directions.
- Before a policy map can be effective, it must be attached to an interface.

© 2021 IP Infusion Inc. Proprietary



Enable/Disable Configuration

Topology



Figure 1-50: Simple configuration of QoS

Enabling QoS

The following steps describe how to enable QoS.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable (H)QoS on configuration mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
!
```

Disabling QoS

The following steps disable QoS.

© 2021 IP Infusion Inc. Proprietary

`#configure terminal`	Enter configure mode.
`(config)#qos disable`	Disable (H)QoS on configuration mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
% QoS is not enabled globally
```

QoS Statistics Configuration

This section show how to enable QoS statistics.

Topology



Figure 1-51: Simple configuration of QoS

Enabling QoS Statistics

The following steps describe how to enable QoS Statistics.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics on configuration mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
!
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Dscp-to-queue Map Profile Configuration

This chapter contains a complete sample of configuring Dscp-to-queue map profile.

Topology

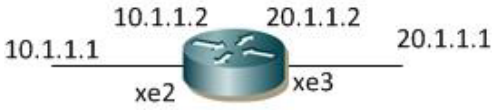


Figure 2-52: Simple configuration of Dscp-to-queue map

Configuration of dcsp-to-queue Map Profile on configuration mode

The following steps describe how to configure dscp-to-queue map on configuration mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#qos profile dscp-to-queue Profile1`	Enter Dscp to queue map profile configuration mode
`(config)#qos profile dscp-to-queue Dscp2queue`	Enter dscp-to-queue profile configuration mode
`(config-ingress-dscp-map)#dscp 10 queue 5`	Map dscp 10 to queue 5
`(config-ingress-dscp-map)#exit`	Exit dscp-to-queue profile configure mode.
`(config)#qos profile dscp-to-queue Profile3`	Enter Dscp to queue map profile configuration mode
`(config-ingress-dscp-map)#dscp 24 queue 6 color green`	Map dscp 24 to queue 6 for green packets
`(config-ingress-dscp-map)#exit`	Exit dscp-to-queue profile configure mode
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
!
qos profile dscp-to-queue Profile1
 dscp 10 queue 5
!
qos profile dscp-to-queue Profile3
 dscp 24 queue 6 color green
```

Configuration of dscp-to-queue Map Profile on Interface mode

The following steps describe how to configure dscp-to-queue map profile on interface mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#qos map-profile dscp-to-queue Profile1`	Map dscp-to-queue profile to the interface
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.
`(config)#interface xe3`	Enter interface mode,
`(config-if)#qos map-profile dscp-to-queue Profile3`	Map dscp-to-queue profile to the interface
`(config-if)#exit`	Exit interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
!
qos profile dscp-to-queue Profile1
 dscp 10 queue 5
!
!
!
interface xe2
 qos map-profile dscp-to-queue Profile1
!
interface xe3
 qos map-profile dscp-to-queue Profile3
!
```

```
#show qos-profile type dscp-to-queue Profile1
profile name: Profile1
profile type: dscp-to-queue
profile attached to 1 instances
configured mapping:
 dscp 10 queue 5
Detailed mapping:
 Ingress map for dscp to queue-color
 -------+----------------- | -------+----------------- | -------+----------------- | -------+-----------------
  INPUT |     OUTPUT       |  INPUT |     OUTPUT       |  INPUT |     OUTPUT       |  INPUT |     OUTPUT
 -------+-----------------+ -------+-----------------+ -------+-----------------+ -------+-----------------
  DSCP  | Queue | Color    |  DSCP  | Queue | Color    |  DSCP  | Queue | Color    |  DSCP  | Queue | Color
 -------+-------+--------- | -------+-------+--------- | -------+-------+--------- | -------+-------+---------
  0       0       green    |  16      2       green    |  32      4       green    |  48      6       green
  1       0       green    |  17      2       green    |  33      4       green    |  49      6       green
  2       0       green    |  18      2       green    |  34      4       green    |  50      6       green
  3       0       green    |  19      2       green    |  35      4       green    |  51      6       green
```


© 2021 IP Infusion Inc. Proprietary

```
4       0       green   |  20      2       yellow  |  36      4       yellow  |  52      6       green
5       0       green   |  21      2       green   |  37      4       green   |  53      6       green
6       0       green   |  22      2       red     |  38      4       red     |  54      6       green
7       0       green   |  23      2       green   |  39      4       green   |  55      6       green
8       1       green   |  24      3       green   |  40      5       green   |  56      7       green
9       1       green   |  25      3       green   |  41      5       green   |  57      7       green
10      5       green   |  26      3       green   |  42      5       green   |  58      7       green
11      1       green   |  27      3       green   |  43      5       green   |  59      7       green
12      1       yellow  |  28      3       yellow  |  44      5       green   |  60      7       green
13      1       green   |  29      3       green   |  45      5       green   |  61      7       green
14      1       red     |  30      3       red     |  46      5       green   |  62      7       green
15      1       green   |  31      3       green   |  47      5       green   |  63      7       green
```

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 Cos-to-queue Map Configuration

This chapter contains a complete sample of configuring Cos-to-queue map.

Topology



Figure 3-53: Simple configuration of CoS

Configuration of Cos-to-queue Map on configuration mode

The following steps describe how to configure Cos-to-queue map on configuration mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#qos profile cos-to-queue Profile2`	Enter cos-to-queue profile configuration mode
`(config-ingress-cos-map)#cos 2 queue 4`	Map cos 2 to queue 4 under cos-to-queue profile configuration mode
`(config-ingress-cos-map)#exit`	Exit configure mode.
`(config)#qos profile cos-to-queue Profile4`	Enter cos-to-queue profile configuration mode
`(config-ingress-cos-map)#cos 3 queue 4 color yellow`	Map cos 3 to queue 4 for yellow packets
`(config-ingress-cos-map)#exit`	Exit cos-to-queue map profile configuration
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos qos enable
qos statistics
!
qos profile cos-to-queue Profile2
 cos 2 dei all queue 4
qos map cos 2 queue 4
!
qos profile cos-to-queue Profile4
 cos 3 dei all queue 4 color yellow
!
```

Configuration of Cos-to-queue Map Profile on Interface mode

The following steps describe how to configure Cos-to-queue map profile on interface mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure the port as switchport
`(config-if)#qos map-profile cos-to-queue Profile2`	Map cos-to-queue profile on the interface
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure the port as switchport
`(config-if)#qos map-profile cos-to-queue Profile4`	Map cos-to-queue profile on the interface
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
!
qos profile cos-to-queue Profile2
 cos 2 dei all queue 4
!
!
!
interface ce3/1
 qos map-profile cos-to-queue Profile2
!
qos profile cos-to-queue Profile4
 cos 3 dei all queue 4 color yellow
!
!
#show qos-profile type cos-to-queue Profile4
profile name: Profile4
profile type: cos-to-queue
profile attached to 0 instances
configured mapping:
 cos 3 dei all queue 4 color yellow
Detailed mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
```


© 2021 IP Infusion Inc. Proprietary

```
2       0       2       green    |  2       1       2       yellow
3       0       4       yellow   |  3       1       4       yellow
4       0       4       green    |  4       1       4       yellow
5       0       5       green    |  5       1       5       yellow
6       0       6       green    |  6       1       6       yellow
7       0       7       green    |  7       1       7       yellow
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 Queue-color-to-cos Map Profile Configuration

This chapter contains a complete sample of configuring queue-color-to-cos map profile.

Topology

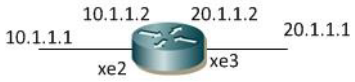


Figure 4-54: Queue color-to-cos map profile configuration

Configuration queue-color-to-qos map profile

The following steps describe how to configure queue-color-to-cos map profile on configuration mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#qos profile queue-color-to-cos Profile5`	Enter queue-color-to-cos profile configuration mode
`(config-ingress-cos-map)#queue 2 color all cos 7`	Map queue 2 to cos 7 for all colors under cos-to-queue profile configuration mode
`(config-egress-cos-map)#exit`	Exit queue-color-to-cos configuration mode
`(config)#qos profile queue-color-to-cos default`	Enter queue-color-to-cos default map profile configuration mode
`(config-egress-cos-map)#queue 3 cos 5`	Map queue 3 frames to cos 5
`(config-egress-cos-map)#exit`	Exit queue-color-to-cos
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
!
qos profile queue-color-to-cos default
 queue 3 color all cos 5
!
qos profile queue-color-to-cos Profile5
 queue 2 color all cos 7
!
```

Configuration of Queue-color-to-cos Map Profile on Interface mode

The following steps describe how to configure Queue-color-to-cos map profile on interface mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure the port as switchport
`(config-if)#qos map-profile queue-color-to-cos Profile5`	map queue-color-to-cos profile on the interface
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
# show running-config qos
qos enable
qos statistics
!
qos profile queue-color-to-cos default
 queue 3 color all cos 5
!
qos profile queue-color-to-cos Profile5
 queue 2 color all cos 7
!
!
!
interface xe2
 qos map-profile queue-color-to-cos Profile5
!
```

```
#show qos-profile type queue-color-to-cos Profile5
profile name: Profile5
profile type: queue-color-to-cos
profile attached to 1 instances
configured mapping:
 queue 2 color all cos 7
Detailed mapping:
 ----------------+-------- | ----------------+-------- | ----------------+--------
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      | OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+--------
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+--------
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    7       |  2       yellow   7       |  2       red      7
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 Queue-color-to-dscp Map Profile Configuration

This chapter contains a complete sample of configuring queue-color-to-dscp map profile.

Topology

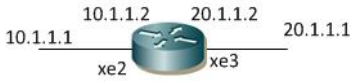


Figure 5-55: Queue color-to-dscp map profile configuration

Configuration queue-color-to-dscp map profile

The following steps describe how to configure queue-color-to-dscp map profile on configuration mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#qos profile queue-color-to-dscp Profile6`	Enter queue-color-to-dscp profile configuration mode
`(config-egress-dscp-map)#queue 3 color green dscp 48`	Map queue 3 to dscp 48 for green color traffic under queue-color-to-dscp profile configuration mode
`(config-egress-dscp-map)#exit`	Exit queue-color-to-dscp map configuration mode
`(config)#qos profile queue-color-to-dscp default`	Enter queue-color-to-dscp default map profile configuration mode
`(config-egress-dscp-map)#queue 5 dscp 32`	Map queue 5 frames to dscp 32
`(config-egress-cos-map)#exit`	Exit queue-color-to-dscp configuration mode
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
!
qos profile queue-color-to-dscp default
 queue 5 color all dscp 32
!
qos profile queue-color-to-dscp Profile6
 queue 3 color green dscp 48
! ?
```

Configuration of Queue-color-to-dscp Map Profile on Interface mode

The following steps describe how to configure Queue-color-to-dscp map profile on interface mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure the port as switchport
`(config-if)#qos map-profile queue-color-to-dscp Profile6`	map queue-color-to-dscp profile on the interface
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
# show running-config qos
qos enable
qos statistics
!
qos profile queue-color-to-dscp default
 queue 5 color all dscp 32
!
qos profile queue-color-to-dscp Profile6
 queue 3 color green dscp 48
!
!
!
interface xe2
 qos map-profile queue-color-to-dscp Profile6
!
```

```
#show qos-profile type queue-color-to-dscp Profile6
profile name: Profile6
profile type: queue-color-to-dscp
profile attached to 1 instances
configured mapping:
 queue 3 color green dscp 48
Detailed mapping:
 ----------------+-------- | ----------------+-------- | ----------------+--------
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      | OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+--------
  Queue | Color  | DSCP    |  Queue | Color  | DSCP    |  Queue | Color  | DSCP
 -------+--------+-------- | -------+--------+-------- | -------+--------+--------
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    10      |  1       yellow   12      |  1       red      14
  2       green    18      |  2       yellow   20      |  2       red      22
  3       green    48      |  3       yellow   28      |  3       red      30
  4       green    34      |  4       yellow   36      |  4       red      38
  5       green    40      |  5       yellow   40      |  5       red      40
  6       green    48      |  6       yellow   48      |  6       red      48
  7       green    56      |  7       yellow   56      |  7       red      56
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 6 Trust DSCP on Layer 2 Interface Configuration

This chapter contains a complete sample of configuring trust DSCP on Layer 2 interface.

Topology

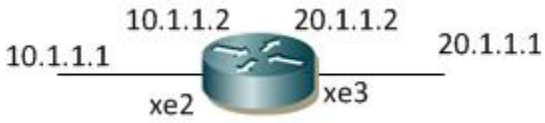


Figure 6-56: Simple configuration of trust DSCP

Configuration Trust DSCP on Interface mode

The following steps describe how to configure trust DSCP on Layer 2 interface.By default, Layer 2 interface will be trust CoS and layer3 interface will be trust DSCP.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#trust dscp`	Configure trust DSCP on the interface xe2.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
qos statistics
!
!
interface xe2
 trust dscp
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 7 Service based Queue Distribution Configuration

This chapter describes configuring queue distribution based on type of service such as Precedence or DSCP on Layer 3 interface. Prior to this feature support, only one type of configuration was possibile either precedence or DSCP.

Using the most significant three bits of the DSCP such as Class Selector bits which provides backward compatibility with ip precedence, user can set Precedence. For example when user configure Precedence as 101 in CLI, convert this value to DSCPs(101000 ~ 101111), then set the DSCP.

In the configuration section, new precedence profiles are introduced as qos map-profile based on the existing DHCP profiles.

The configuration procedures given below are similar to DHCP, however, both configurations are supported based on requirements.

Service based Queue configuration

There are 2 Qos-map Precedence profiles used in the configuration procedure.

Precedence-to-queue:

This is an ingress profile similar to dhcp-to-queue. This profile will map precedence value 0-7 to queue 0-7

Topology



Figure 7-57: Precedence-to-queue topology

`#configure terminal`	Enter configure mode
`(config)#enable qos`	Enable Qos
`(config)#exit`	Exit configure mode
`(config)# qos profile precedence-to-queue Prec1_que1`	Configure qos-map profile precedence-to-queue with
`Profile name as Prece1_que1`	
`(config-ingress-prec-map)# precedence 1 queue 2`	Configure mapping of prece 1 to queue 2, so that traffic with precedence 1 should take queue as q2
`(config)#exit`	Exit configure mode
`(config)# interface xe1`	Configure ingress interface xe1

(config-if)#qos map-profile precedence-to-queue Prec1_que1	Map the profile Prec1_que1 to interface xe1 so that ingress traffic hitting the xe1 interface with prece as 1 should take queue q2
(config)#commit	Commit the configuration
(config)#end	

Validation

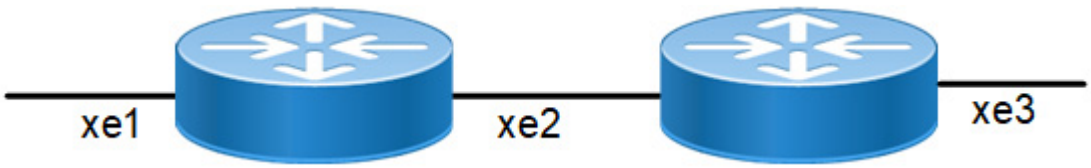
```
#show run int xe1
!
interface xe1
 qos map-profile precedence-to-queue Prec1_que1
!

#show qos-profile type precedence-to-queue
profile name: Prec1_que1
profile type: precedence-to-queue
profile attached to 1 instances
configured mapping:
 precedence 1 queue 2
 Detailed mapping:
 -------+------------------
  INPUT |    OUTPUT
 -------+------------------
  PREC  | Queue | Out PREC
 -------+-------+----------
  0       0       0
  1       1       2
  2       2       0
  3       3       0
  4       4       0
  5       5       0
  6       6       0
  7       7       0


R1#show run qos
qos enable
!
qos profile precedence-to-queue Prec1_que1
 precedence 1 queue 2
!
interface xe1
 qos map-profile precedence-to-queue Prec1_que1
```

Queue-to-precedence:

This is egress profile similar to queue-to-dscp. This qos-map profile maps default or corresponding queue to new precedence value that enables the user to see queue corresponding to new precedence mentioned in this profile on the next node egress interface.

 © 2021 IP Infusion Inc. Proprietary

Topology



#configure terminal	Enter configure mode
(config)#enable qos	Enable Qos
(config)#exit	Exit configure mode
(config)# qos profile queue-to-precedence queeue_prece1	Configure qos-map profile queue-to-precedence with Profile name as queeue_prece1
(config-ingress-prec-map)# queue 2 precedence 5	Configure mapping of queue 2 to precedence 5, so that traffic with precedence 1 should take queue as q2
(config)#exit	Exit configure mode
(config)# interface xe2	Configure egress interface xe2 of 1st node
(config-if)#qos map-profile queue-to-precedence queeue_prece1	Map the profile queeue_prece1 to interface xe2 so that egress traffic from xe2 can be remarked with new precedence value 5 and on next node can verify this on egress interface xe3
(config)#commit	Commit the configuration
(config)#end	

Validation

```
#show run int ce50
!
interface ce50
 qos map-profile queue-to-precedence queue_prece1
!
#
```

```
R1#show run qos
qos enable
qos statistics
qos remark dscp
!
!
qos profile queue-to-precedence queeue_prece1
```

```
 queue 2 precedence 5
!
!
!
interface ce50
 qos map-profile queue-to-precedence queeue_prece1
!
#



#show qos-profile queeue_prece1
profile name: queeue_prece1
profile type: queue-to-precedence
profile attached to 1 instances
configured mapping:
 queue 2 precedence 5
Detailed mapping:
 -------+--------
  INPUT | OUTPUT
 -------+--------
  Queue | PREC
 -------+--------
  0       0
  1       1
  2       5
  3       3
  4       4
  5       5
  6       6
  7       7
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 8 Weights for Queues Configuration

This chapter contains a complete sample of configuring WRR weights for queues.

Topology



Figure 8-58: Simple configuration of QoS

Configuring WRR Weights for Queues

Do the following to configure WRR weights for queues.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map cmap1`	Enter class-map mode
`(config-cmap-qos)#match cos 2`	Configure match criteria as cos 2
`(config-cmap-qos)#exit`	Exit out of class-map mode
`(config)#class-map cmap2`	Enter class-map mode
`(config-cmap-qos)#match cos 3`	Configure match criteria as cos 3
`(config-cmap-qos)#exit`	Exit out of class-map mode
`(config)#policy-map pmap1`	Enter policy-map mode.
`(config-pmap-qos)#class cmap1`	Assign class cmap1.
`(config-pmap-c-qos)#set qos-group 1`	Remark matched traffic to qos-group 1
`(config-pmap-c-qos)#exit`	Exit out of pmap-c mode
`(config-pmap-qos)#exit`	Exit pmap mode.
`(config)#policy-map pmap1`	Enter policy-map mode.
`(config-pmap-qos)#class cmap2`	Assign class cmap2.
`(config-pmap-c-qos)#set qos-group 2`	Remark matched traffic to qos-group 2
`(config-pmap-c-qos)#exit`	Exit out of pmap-c mode
`(config-pmap-qos)#exit`	Exit pmap mode.
`(config)#class-map type queuing cq1`	Configure class-map of type queuing with name cq1, and enter into class-map mode
`(config-cmap-que)#match qos-group 1`	Configure match criteria as qos-group 1
`(config-cmap-que)#exit`	Exit out of class-map mode.
`(config)#class-map type queuing cq2`	Configure class-map of type queuing with name cq2, and enter into class-map mode.
`(config-cmap-que)#match qos-group 2`	Configure match criteria as qos-group 2.
`(config-cmap-que)#exit`	Exit out of class-map mode.

© 2021 IP Infusion Inc. Proprietary

(config)#policy-map type queuing pq1	Configure policy-map of type queuing with name pq1, and enter into policy-map mode.
(config-pmap-que)#class cq1	Attach class cq1 to Policy-map pq1.
(config-pmap-c-que)#wrr-queue weight 2	Configure WRR Weight of 2.
(config-pmap-c-que)#exit	Exit from pmap-c mode.
(config-pmap-que)#class cq2	Assign class (queue) cq2 to pq1.
(config-pmap-c-que)#wrr-queue weight 4	Configure WRR weight of 4.
(config-pmap-c-que)#exit	Exit from pmap-c mode.
(config-pmap-que)#exit	Exit from pmap mode.
(config)#interface xe2	Enter into interface xe2.
(config-if)#service-policy type queuing output pq1	Assign service policy pq1 of type queueing on out direction.
(config-if)#exit	Exit interface mode
(config)#exit	Exit configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)# service-policy type qos input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit the interface mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
```


© 2021 IP Infusion Inc. Proprietary

```
!
class-map cmap1
 match cos 2
!
class-map cmap2
 match cos 3
!
class-map type queuing match-any cq1
 match qos-group 1
!
class-map type queuing match-any cq2
 match qos-group 2
!
policy-map pmap1
 class cmap1
  set qos-group 1
  exit
 class cmap2
  set qos-group 2
  exit
!
!
policy-map type queuing pq1
 class type queuing cq1
  wrr-queue weight 2
  exit
 class type queuing cq2
  wrr-queue weight 4
  exit
!
!
interface xe2
 service-policy type queuing output pq1
!
interface xe3
 service-policy type qos input pmap1
!


#show policy-map

Type qos policy-maps
====================

policy-map pmap1
 class cmap1
  set qos-group 1
  exit
 class cmap2
  set qos-group 2
```

```
  exit


Type queuing policy-maps
========================

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 1
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 1
  exit
 class type queuing default q3
  priority level 1
  exit
 class type queuing default q4
  priority level 1
  exit
 class type queuing default q5
  priority level 1
  exit
 class type queuing default q6
  priority level 1
  exit
 class type queuing default q7
  priority level 1
  exit

policy-map type queuing pq1
 class type queuing cq1
  wrr-queue weight 2
  exit
 class type queuing cq2
  wrr-queue weight 4
  exit


#show class-map

  Type qos class-maps
  ===================
      class-map type qos match-any class-default

      class-map cmap1
         match cos 2
```


© 2021 IP Infusion Inc. Proprietary

```
      class-map cmap2
         match cos 3


  Type queuing class-maps
  =======================
      class-map type queuing match-any cq1
         match qos-group 1

      class-map type queuing match-any cq2
         match qos-group 2

      class-map match-any q0

      class-map match-any q1

      class-map match-any q2

      class-map match-any q3

      class-map match-any q4

      class-map match-any q5

      class-map match-any q6

      class-map match-any q7


  Type Vlan-Queuing class-maps
  ============================

#show policy-map interface xe2
Interface xe2
Global statistics status : enabled

Service-policy (queuing) output: pq1
---------------------------------
Class-map (queuing): cq1
 match qos-group 1
 wrr-queue weight 2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): cq2
 match qos-group 2
 wrr-queue weight 4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```

```
Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets

#show policy-map interface xe3

Interface xe3
Global statistics status : enabled

Service-policy (qos) input     : pmap1
--------------------------------
Class-map (qos): cmap1 (match all)
 match cos 2
 set qos-group 1
      matched      : 209681694 packets, 15097081968 bytes
      transmitted  : 209681694 packets, 15097081968 bytes

Class-map (qos): cmap2 (match all)
 match cos 3
 set qos-group 2
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes
```

```
Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 11789 packets, 754820 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 1460 packets, 93914 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 39311112 packets, 2830400048 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```

 © 2021 IP Infusion Inc. Proprietary

```
Class-map (queuing): mc-q2
      output       : 78930334 packets, 5051541376 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 21 packets, 1428 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 9 Marking/Remarking Configuration

This chapter contains a complete sample of configuring Marking/Remarking.

Topology

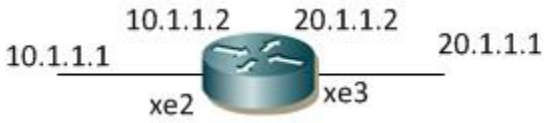


Figure 9-59: Simple configuration of Marking/Remarking

L2 Interface

The following steps describe how to configure Marking/Remarking.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol rstp vlan-bridge`	Configure bridge 1 as RSTP-VLAN aware.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe2 interface.
`(config-if)#exit`	Exit the xe2 interface mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type qos cmap1`	Enter Class-map mode
`(config-cmap-qos)#match cos 2`	Configure match criteria as CoS with Value 2
`(config-cmap-qos)#exit`	Exit Class-map mode
`(config)#policy-map type qos pmap1`	Enter policy-map mode
`(config-pmap-qos)#class type qos cmap1`	Assign Class cmap1 to Policy-map pmap1
`(config-pmap-c-qos)#set cos 5`	Remark cos from cos 2 to cos 5
`(config-pmap-c-qos)#exit`	Exit out of policy-class-map mode
`(config-pmap-qos)#exit`	Exit out of Policy-map mode
`(config)#interface xe2`	Enter xe2 interface
`(config-if)#service-policy type qos input pmap1`	Assign service-policy to interface on in-direction
`(config-if)#exit`	Exit the xe2 interface mode.

(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate bridge to an interface.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the xe3 interface mode.
(config)#class-map type qos cmap2	Enter Class-map mode
(config-cmap-qos)#match protocol arp	Configure match criteria as protocol with arp
(config-cmap-qos)#exit	Exit Class-map mode
(config)#policy-map type qos pmap2	Enter policy-map mode
(config-pmap-qos)#class type qos cmap2	Assign Class cmap2 to Policy-map pmap2
(config-pmap-c-qos)#set cos 6	Remark all frame with ethertype as arp to cos 6
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#exit	Exit out of Policy-map mode
(config)#interface xe3	Enter xe3 interface
(config-if)#service-policy type qos input pmap2	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.2/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.3	Enter interface mode.
(config-if)# ip address 20.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
!
class-map type qos cmap1
 match cos 2
!
class-map type qos cmap2
 match protocol arp
```


© 2021 IP Infusion Inc. Proprietary

```
!
policy-map type qos pmap1
 class type qos cmap1
  set cos 5
  exit
!
policy-map type qos pmap2
 class type qos cmap2
  set cos 6
  exit
!
!
!
interface xe2
 service-policy type qos input pmap1
!
interface xe3
 service-policy type qos input pmap2
!

#show class-map cmap1

  Type qos class-maps
  ===================

      class-map type qos cmap1
         match cos 2


#show policy-map

Type qos policy-maps
====================

policy-map type qos pmap1
 class type qos cmap1
  set cos 5
  exit

policy-map type qos pmap2
 class type qos cmap2
  set cos 6
  exit


Type queuing policy-maps
========================

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority
  exit
 class type queuing default q1
  priority
  exit
 class type queuing default q2
  priority
```

```
  exit
 class type queuing default q3
  priority
  exit
 class type queuing default q4
  priority
  exit
 class type queuing default q5
  priority
  exit
 class type queuing default q6
  priority
  exit
 class type queuing default q7
  priority
  exit

#show policy-map interface xe2

Interface xe2
Global statistics status : enabled

Class-map (qos): cmap1 (match all)
 match cos 2
 set cos 5
      matched      : 8 packets, 680 bytes
      transmitted  : 8 packets, 680 bytes


Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority
      output       : 12 packets, 1416 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
```

 © 2021 IP Infusion Inc. Proprietary

```
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority
      output       : 589 packets, 37876 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 7 packets, 448 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 12 packets, 852 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets


OcNOS#show policy-map interface xe3

Interface xe3
Type QoS statistics status : enabled
```

```
Class-map (qos): cmap2 (match all)
 match protocol arp
 set cos 6

      matched      : 7 packets, 448 bytes
      transmitted  : 7 packets, 448 bytes


Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority
      output       : 699 packets, 59550 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 1 packets, 64 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 2 packets, 136 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

L3 Interface

`#configure terminal`	Enter configure mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#ip address 10.1.1.1/24`	Assign IP Address on interface to 10.1.1.2 with mask 255.255.255.0
`(config-if)#exit`	Exit out of interface mode
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type qos cmap3`	Configure class-map of type qos with name cmap3 and enter into Class-map mode
`(config-cmap-qos)#match dscp 10`	Configure match criteria as dscp with a value of 10.
`(config-cmap-qos)#exit`	Exit Class-map mode
`(config)#policy-map type qos pmap3`	Enter policy-map mode

(config-pmap-qos)#class type qos cmap3	Assign Class cmap3 to Policy-map pmap3
(config-pmap-c-qos)#set dscp ef	Remark frames with dscp value 10 to dscp 46
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#exit	Exit out of Policy-map mode
(config)#interface xe3	Enter xe3 interface
(config-if)#service-policy type qos input pmap3	Assign service-policy pmap3 to interface xe3 on in-direction
(config-if)#exit	Exit out of interface mode
(config)#ip access-list 101	Configure access-list 101 with action as permit for tcp traffic with destination port as ftp port
(config-ip-acl)#permit tcp any any eq ftp	Permit for tcp traffic with destination port as ftp port.
(config-ip-acl)#exit	Exit access list mode
(config)#class-map type qos match-any cmap4	Enter Class-map mode
(config-cmap-qos)#match access-group 101	Configure access-group 101 as match criteria
(config-cmap-qos)#exit	Exit class-map mode
(config)#policy-map type qos pmap4	Enter policy map mode
(config-pmap-qos)#class cmap4	Assign Class cmap4 to Policy-map pmap4
(config-pmap-c-qos)#set precedence 7	Remark frames matching access-group 101 to precedence 7
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#exit	Exit out of Policy-map mode
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 20.1.1.1/24	Assign IP Address on interface to 20.1.1.1 with mask 255.255.255.0
(config-if)#service-policy type qos input pmap4	Assign service-policy to interface on in-direction

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
!
class-map type qos cmap3
 match dscp af11
```


© 2021 IP Infusion Inc. Proprietary

```
!
class-map type qos match-any cmap4
 match access-group 101
!
policy-map type qos pmap3
 class type qos cmap3
  set dscp ef
  exit
policy-map type qos pmap4
 class type qos cmap4
  set precedence network
  exit
!
interface xe2
 service-policy type qos input pmap4
!
interface xe3
 service-policy type qos input pmap3


#show class-map type qos

  Type qos class-maps
  ===================
      class-map type qos match-any class-default

      class-map type qos cmap3
         match dscp af11

      class-map type qos match-any cmap4
         match access-group 101



#show policy-map

Type qos policy-maps
====================

policy-map type qos pmap3
 class type qos cmap3
  set dscp ef

policy-map type qos pmap4
 class type qos cmap4
  set precedence network


Type queuing policy-maps
========================
```

```
policy-map type queuing default default-out-policy
 class type queuing default q0
  priority
 class type queuing default q1
  priority
 class type queuing default q2
  priority
 class type queuing default q3
  priority
 class type queuing default q4
  priority
 class type queuing default q5
  priority
 class type queuing default q6
  priority
 class type queuing default q7
priority

#show policy-map interface xe2


Interface xe2
Type Qos statistics status : enabled
--------------------------------
 Class-map (qos): cmap4 (match any)
 match access-group 101
 set precedence 7
      matched    : 375594046 packets, 25540397168 bytes

Service-policy (queuing) output: default-out-policy
--------------------------------
 Class-map (queuing): q0
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q2
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes
```

 © 2021 IP Infusion Inc. Proprietary

```
 Class-map (queuing): q3
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q4
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q5
 priority
      output     : 391282612 packets, 25042086656 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q6
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7
 priority
      output     : 4 packets, 256 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q4
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets

#show policy-map interface xe3


Interface xe3
Global statistics status : enabled
--------------------------------
 Class-map (qos): cmap3 (match all)
 match dscp af11
 set dscp 46
      matched    : 401497149 packets, 25695819008 bytes


Service-policy (queuing) output: default-out-policy
--------------------------------
 Class-map (queuing): q0
 priority level 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes
```

 © 2021 IP Infusion Inc. Proprietary

```
 Class-map (queuing): q2
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q3
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q4
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q5
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q6
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7
 priority
      output     : 382211720 packets, 25990396484 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2
      output     : 0 packets, 0 bytes
```

```
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q4
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

 © 2021 IP Infusion Inc. Proprietary

CHAPTER 10 Policing Configuration

Topology

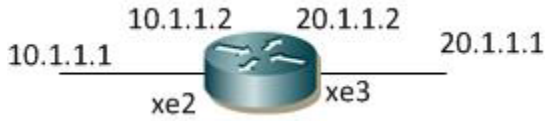


Figure 10-60: Simple configuration of Policing

L2 Interface

Do the following to configure policing on an L2 interface.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Configure bridge 1 as mstp aware.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe2 interface.
`(config-if)#exit`	Exit the xe2 interface mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type qos 1234`	Enter Class-map mode
`(config-cmap-qos)#match cos 3`	Configure match criteria as CoS with Value 3
`(config-cmap-qos)#exit`	Exit Class-map mode
`(config)#policy-map type qos 1234`	Enter policy-map mode
`(config-pmap-qos)#class type qos 1234`	Assign Class 1234 to Policy-map 1234
`(config-pmap-c-qos))# police cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform transmit exceed set-cos-transmit 1 violate drop`	Police access-list 102 frames @ Committed information rate 2 mbps, committed bust 2 mbyte, peak information rate 3 mbps, peak burst 2 mbytes when traffic is > CIR and <= PIR then Set the class of service (CoS) field to 1, if traffic violate the action then drop the frames.
`(config-pmap-c-qos)#exit`	Exit out of policy-class-map mode
`(config-pmap-qos)#exit`	Exit out of Policy-map mode
`(config)#interface xe2`	Enter xe2 interface
`(config-if)#service-policy type qos input 1234`	Assign service-policy to interface on in-direction
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe3 as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.

© 2021 IP Infusion Inc. Proprietary

(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the xe3 interface mode.
(config)#mac access-list 102	Configure mac access-list with action
(config-mac-acl)#permit host 0000.0101.1010 host 0000.0202.2020	Permit when frames matches Source mac address 00:00:01:01:10:10 and destination mac address 00:00:02:02:20:20
(config-mac-acl)#exit	Exit mac access-list mode
(config)#class-map type qos match-any 2345	Enter Class-map mode
(cmap-qos-match-any-mode)#match access-group 102	Configure match criteria as access-group 102
(cmap-qos-match-any-mode)#exit	Exit Class-map mode
(config)#policy-map type qos 2345	Enter policy-map mode
(config-pmap-qos)#class type qos 2345	Assign Class 2345 to Policy-map 2345
(config-pmap-c-qos))# police cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform transmit exceed set-cos-transmit 1 violate drop	Police access-list 102 frames @ Committed information rate 2 mbps, committed bust 2 mbytes, peak information rate 3 mbps, peak burst 2 mbytes when traffic is > CIR and <= PIR, then set the class of service (CoS) field to 1, if traffic violate the action, then drop the frames.
(config-pmap-qos)#exit	Exit Policy-class mode
(config-pmap-qos)#exit	Exit Policy-map mode
(config)#interface xe3	Enter interface mode.
(config-if)#service-policy type qos input 2345	Assign service-policy 2345 to interface on in-direction
(config-if)#exit	Exit interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
!
class-map type qos 1234
 match cos 2
!
class-map type qos match-any 2345
 match access-group 102
!
policy-map type qos 1234
 class type qos 1234
  police cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform transmit exceed set-cos-transmit 1 violate drop
  exit
policy-map type qos 2345
```


© 2021 IP Infusion Inc. Proprietary

```
 class type qos 2345
  police cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform transmit exceed set-cos-
transmit 1 violate drop
  exit
!
interface xe2
 service-policy type qos input 1234
!
interface xe3
 service-policy type qos input 2345
#show class-map type qos

  Type qos class-maps
  ===================
      class-map type qos 1234
         match cos 2

      class-map type qos match-any 2345
         match access-group 102

      class-map type qos match-any class-default

#show policy-map type qos

Type qos policy-maps
====================

policy-map type qos 1234
 class type qos 1234
  police colour-aware cir 1 mbps bc 1 mbytes conform set-cos-transmit 5 violate
drop
  exit

policy-map type qos 2345
 class type qos 2345
  police colour-aware cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform tran
smit exceed set-cos-transmit 1 violate drop
  exit
#
#show policy-map interface xe2


Interface xe2
Global statistics status : enabled


Service-policy (qos) input     : 1234
--------------------------------
 Class-map (qos): 1234 (match all)
 match cos 3
```

```
 police cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform transmit exceed set-cos-
transmit 1 violate drop
      matched    : 7419394 packets, 504519132 bytes
      dropped    : 7409793 packets, 503866264 bytes


Service-policy (queuing) output: default-out-policy
--------------------------------
 Class-map (queuing): q0
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
 priority
      output     : 7222 packets, 491096 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q2
 priority
      output     : 14444 packets, 982192 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q3
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q4
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q5
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q6
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7
```

 © 2021 IP Infusion Inc. Proprietary

```
 priority
      output     : 2 packets, 246 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q4
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

```
#show policy-map interface xe3


Interface xe3
Global statistics status : enabled


Service-policy (qos) input     : 2345
--------------------------------
 Class-map (qos): 2345 (match any)
 match access-group 102
 police colour-aware cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform trans
mit exceed set-cos-transmit 1 violate drop
      matched    : 16218780 packets, 1102879420 bytes


Service-policy (queuing) output: default-out-policy
--------------------------------
 Class-map (queuing): q0
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q2
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q3
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q4
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
 Class-map (queuing): q5
 priority
      output     : 18527 packets, 1259836 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q6
 priority
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7
 priority
      output     : 5 packets, 615 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q4
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6
      output     : 0 packets, 0 bytes
```

```
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 11 Bandwidth Configuration

This chapter contains a complete sample of configuring Bandwidth.

Topology

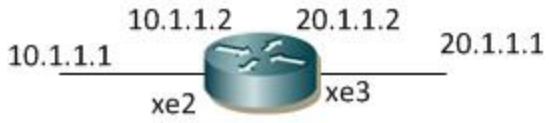


Figure 11-61: Simple configuration of Bandwidth

L2/L3 Interface

The following steps describe how to configure bandwidth.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#policy-map type queuing default P1`	Configure policy-map of type queuing as default with name P1, and enter into policy-map mode
`(config-pmap-que)#class type queuing default q2`	Configure class-map of type queuing as default for q0 and enter into class-map mode
`(config-pmap-c-que)#bandwidth percent 70`	Configure minimum bandwidth as 70 percent of total bandwidth available on interface
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#class type queuing default q3`	Attach class q3 to Policy-map P1
`(config-pmap-c-que)#bandwidth percent 30`	Configure minimum bandwidth as 30 percent of remaining bandwidth available on interface after all allocations are done.
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#exit`	Exit out of Policy-map mode
`(config)#class-map type qos c1`	Enter Class-map mode
`(config-cmap-qos)#match dscp 10`	Configure match criteria as dscp 10
`(config-cmap-qos)#match cos 3`	Configure match criteria as cos 3
`(config-cmap-qos)#exit`	Exit out of class-map mode
`(config)#class-map type qos c2`	Enter Class-map mode
`(config-cmap-qos)#match dscp 22`	Configure match criteria as dscp 22
`(config-cmap-qos)#match cos 4`	Configure match criteria as cos 4
`(config-cmap-qos)#exit`	Exit out of class-map mode
`(config)#policy-map type qos pmap1`	Configure policy-map with name pmap1 and enter policy-map mode

© 2021 IP Infusion Inc. Proprietary

(config-pmap-qos)#class type qos c1	Assign Class c1 to Policy-map pmap1
(config-pmap-c-qos)#set precedence 2	Set precedence to value 2
(config-pmap-c-qos)#exit	Exit out of pmap-c mode
(config-pmap-qos)#class type qos c2	Assign Class c2 to Policy-map pmap1
(config-pmap-c-qos)#set cos 2	Set cos to value 2
(config-pmap-c-qos)#exit	Exit out of pmap-c mode
(config)#interface xe3	Enter interface mode
(config-if)#service-policy type queuing output P1	Attach service-policy P1 of type queuing on out direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe2	Enter interface mode
(config-if)#service-policy type qos input pmap1	Attach service-policy pmap1 of type qos on in direction
(config-if)#exit	Exit out of interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.2/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.3	Enter interface mode.
(config-if)# ip address 20.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos
```


© 2021 IP Infusion Inc. Proprietary

```
qos enable
!
qos statistics
!
class-map type qos c1
 match dscp af11
 match cos 2
!
class-map type qos c2
 match dscp af23
 match cos 4
!
policy-map type qos pmap1
 class type qos c1
  set precedence
  immediate
  exit
 class type qos
  c2
   set cos 2
   exit

!
policy-map type queuing default P1
class type queuing default q1
priority
  bandwidth percent 70
  exit
 class type queuing q2
priority
  bandwidth percent 30
  exit
!
!
!
interface xe2
 service-policy type qos input pmap1
!
interface xe3
 service-policy type queuing output P1
!

#show policy-map interface xe2

Interface xe2

Type QoS statistics status : enabled

Class-map (qos): c1 (match all)
 match dscp af11
```

```
 match cos 3
 set precedence 2

Class-map (qos): c2 (match all)
 match dscp af23
 match cos 4
 set cos 2


Type Queuing policy-map : default-out-policy

Class-map (queuing): q0
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q1
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q2
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q3
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q4
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q5
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q6
 priority
      output              : 6 packets, 724 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q7
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 1 packets, 90 bytes
      dropped      : 0 packets, 0 bytes

Wred/Tail Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets


#show policy-map interface xe3

Interface xe3
Type Queuing policy-map : P1

Class-map (queuing): q0
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes
```

```
Class-map (queuing): q1
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q2
 priority
 bandwidth percent 70
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q3
 priority
 bandwidth percent 30
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q4
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q5
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q6
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q7
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
```

 © 2021 IP Infusion Inc. Proprietary

```
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Wred/Tail Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 12 Shaping Configuration

This chapter contains a complete sample of configuring Shaping.

Topology

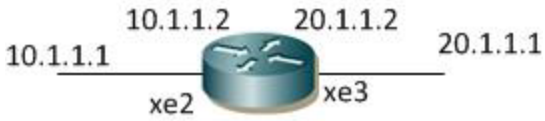


Figure 12-62: Simple configuration of Shaping

L2/L3 Interface

The following steps describe how to configure Shaping.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#policy-map type queuing default P1`	Configure policy-map of type queuing with name P1, and enter into policy-map mode
`(config-pmap-que)#class type queuing default q0`	Configure class type queuing of type default and enter into class map configuration mode
`(config-pmap-c-que)#shape 200 mbps`	Configure shaping to 200 mbps
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#exit`	Exit out of Policy-map mode
`(config)#class-map type qos c1`	Enter Class-map mode
`(config-cmap-qos)#match dscp 10`	Configure match criteria as dscp 10
`(config-cmap-qos)#match cos 3`	Configure match criteria as cos 3
`(config-cmap-qos)#exit`	Exit out of class-map mode
`(config)#class-map type qos c2`	Enter Class-map mode
`(config-cmap-qos)#match dscp 22`	Configure match criteria as dscp 22
`(config-cmap-qos)#match cos 4`	Configure match criteria as cos 4
`(config-cmap-qos)#exit`	Exit out of class-map mode
`(config)#policy-map type qos pmap1`	Configure policy-map with name pmap1 and enter policy-map mode
`(config-pmap-qos)#class type qos c1`	Assign Class c1 to Policy-map pmap1
`(config-pmap-c-qos)#set queue 2`	Set queue 2 for frames with either cos 3 or dscp 10
`(config-pmap-c-qos)#exit`	Exit out of pmap-c mode
`(config-pmap-qos)#class type qos c2`	Assign Class c2 to Policy-map pmap1
`(config-pmap-c-qos)#set queue 3`	Set queue 3 for frames with either cos 4 or dscp 22
`(config-pmap-c-qos)#exit`	Exit out of pmap-c mode

© 2021 IP Infusion Inc. Proprietary

(config-pmap-qos)#exit	Exit policy-map mode
(config)#interface xe3	Enter interface mode
(config-if)#service-policy type queuing output P1	Attach service-policy P1 of type queuing on out direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe2	Enter interface mode
(config-if)#service-policy type qos input pmap1	Attach service-policy pmap1 of type qos on in direction
(config-if)#exit	Exit out of interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.2/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.3	Enter interface mode.
(config-if)# ip address 20.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show policy-map type queuing

Type queuing policy-maps
========================

policy-map type queuing default P1
 class type queuing default q0
```


© 2021 IP Infusion Inc. Proprietary

```
  shape 200 mbps
  priority
 class type queuing default q1
  priority
 class type queuing default q2
  priority
 class type queuing default q3
  priority
 class type queuing default q4
  priority
 class type queuing default q5
  priority
 class type queuing default q6
  priority
 class type queuing default q7
  priority

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority
  exit
 class type queuing default q1
  priority
  exit
 class type queuing default q2
  priority
  exit
 class type queuing default q3
  priority
  exit
 class type queuing default q4
  priority
  exit
 class type queuing default q5
  priority
  exit
 class type queuing default q6
  priority
  exit
 class type queuing default q7
  priority
  exit


#show policy-map type qos
Type qos policy-maps
====================

policy-map type qos pmap1
  class type qos c1
```

```
    set queue 2
    exit
  class type qos c2
    set queue 3
    exit

#show class-map type queuing

  Type queuing class-maps
  =======================
     class-map type queuing q0

  class-map type queuing q1

  class-map type queuing q2

  class-map type queuing q3

  class-map type queuing q4

  class-map type queuing q5

  class-map type queuing q6

      class-map type queuing q7

#show class-map type qos
  Type qos class-maps
   ====================
   class-map type qos match-all c1
    match cos 3
    match dscp af11

   class-map type qos match-all c2
    match cos 4
    match dscp af23

#show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]
-------------------------------------------------------------------------------------
-------------
L0             L1             L2             Group  PrioLevel   Shape          Bandwidth
-------------------------------------------------------------------------------------
-------------
q0                                              -      High        200 mbps       -
q1                                              -      High        -              -
q2                                              -      High        -              -
q3                                              -      High        -              -
q4                                              -      High        -              -
q5                                              -      High        -              -
```

 © 2021 IP Infusion Inc. Proprietary

```
q6                                                  -      High        -              -
q7                                                  -      High        -              -

#show queuing interface xe3

Egress Queuing for Ethernet xe3 [System]
------------------------------------------------------------------------------------------
L0             L1             L2             Group  PrioLevel   Shape          Bandwidth
------------------------------------------------------------------------------------------
q0                                                  -      High        -              -
q1                                                  -      High        -              -
q2                                                  -      High        -              -
q3                                                  -      High        -              -
q4                                                  -      High        -              -
q5                                                  -      High        -              -
q6                                                  -      High        -              -
q7                                                  -      High        -              -

#show policy-map interface xe3

Interface xe3
Type QoS statistics status : enabled

Class-map (qos): c1 (match all)
 match dscp af11
 match cos 3
 set queue 2

Class-map (qos): c2 (match all)
 match dscp af23
 match cos 4
 set queue 3


Type Queuing policy-map : default-out-policy

Class-map (queuing): q0
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q1
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q2
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes
```

```
Class-map (queuing): q3
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q4
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q5
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q6
 priority
      output              : 6 packets, 724 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q7
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 1 packets, 90 bytes
      dropped      : 0 packets, 0 bytes

Wred/Tail Drop Statistics :
-----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 13 Scheduling Configuration

This chapter contains a complete sample of configuring weight, strict priority on queues and weight between uc and mc queue.

Topology

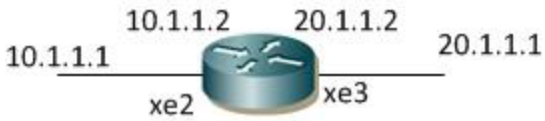


Figure 13-63: Simple configuration of Priority

Configuring Weight on L2 /L3 Interface

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#policy-map type queuing default default-out-policy`	Enter policy-map type queueing default.
`(config-pmap-que-def)#class type queuing default q0`	Enter policy-class-map mode.
`(config-pmap-c-que-def)#wrr-queue weight 2`	Modify strict queue to wrr-queue with weight 2.
`(config-pmap-c-que-def)#exit`	Exit from policy-class-map mode.
`(config-pmap-que-def)#exit`	Exit from policy-map mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show policy-map type queuing

Type queuing policy-maps
========================

policy-map type queuing default default-out-policy
 class type queuing default q0
  wrr-queue weight 2
 class type queuing default q1
  priority
 class type queuing default q2
  priority
 class type queuing default q3
  priority
```

```
     class type queuing default q4
      priority
     class type queuing default q5
      priority
     class type queuing default q6
      priority
     class type queuing default q7
      priority
```

Configuring Strict priority on L2 /L3 Interface

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#policy-map type queuing default p3`	Enter policy-map type queueing default.
`(config-pmap-que-def)#class type queuing default q0`	Enter policy-class-map mode.
`(config-pmap-c-que-def)#priority`	Configure priority for q0.
`(config-pmap-c-que-def)#exit`	Exit from policy-class-map mode.
`(config-pmap-que-def)#exit`	Exit from policy-map mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#service-policy type queuing output p3`	Attach policy-map of type queuing on egress interface
`(config)#exit`	Exit configure mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
# show running-config qos
qos enable
qos statistics
!
!
policy-map type queuing default p3
 class type queuing default q0
  priority
  exit
!
interface xe2
 service-policy type queuing output p3
!

# show policy-map type queuing

Type queuing policy-maps
========================
```


© 2021 IP Infusion Inc. Proprietary

```
policy-map type queuing default default-out-policy
 class type queuing default q0
  priority
 class type queuing default q1
  priority
 class type queuing default q2
  priority
 class type queuing default q3
  priority
 class type queuing default q4
  priority
 class type queuing default q5
  priority
 class type queuing default q6
  priority
 class type queuing default q7
  priority

policy-map type queuing default p3
 class type queuing default q0
  priority
 class type queuing default q1
  priority
 class type queuing default q2
  priority
 class type queuing default q3
  priority
 class type queuing default q4
  priority
 class type queuing default q5
  priority
 class type queuing default q6
  priority
 class type queuing default q7
  priority

OcNOS#
```

Configuring weight between unicast and multicast queues

Use the following configuration to set weights between unicast and multicast traffic of same traffic class.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)# set qos wrr uc 3 non-uc 1`	Schedule unicast and multicast traffic in 3:1
`(config)#exit`	Exit configure mode.

Note: Unicast weight should be always higher than multicast weight. Between unicast and multicast traffic of different traffic class, scheduling will be as per configuration given in the queueing policy-map attached on the interface.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#sh run qos
qos enable
qos statistics
set qos wrr uc 3 non-uc 1
!

#show int cou queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
 * indicates monitor is active
+-------------+--------------------+--------+-----------------+-------------------+----
-------------+--------------------+
|  Interface  |   Queue/Class-map  | Q-Size |     Tx pkts     |      Tx bytes     |
Dropped pkts   |   Dropped bytes   |
+-------------+--------------------+--------+-----------------+-------------------+----
-------------+--------------------+
 ce1/1       q1             (E) 373152   1256           1256000           15245
15241000
 ce1/1       mc-q1          (E) 92352    418            418000            16048
16045000
 ce24/1      pg-q0          (I) 419536   NA             NA                NA
NA
 ce24/1      pg-q1          (I) 468000   NA             NA                NA
NA

Validation
Enter the commands listed in the sections below to confirm the configurations.
#show policy-map type queuingdefault default-out-policy Type queuing policy-maps
========================

policy-map type queuing default default-out-policy class type queuing default q0
wrr-queue weight 2
bandwidth percent 1 exit
class type queuing default q1 priority level 1
bandwidth percent 1 exit
class type queuing default q2 priority level 1


bandwidth percent 1 exit
class type queuing default q3 priority level 1
bandwidth percent 1 exit
class type queuing default q4 priority level 1
bandwidth percent 1 exit
class type queuing default q5 priority level 1
bandwidth percent 1 exit
class type queuing default q6 priority level 1
bandwidth percent 1 exit
class type queuing default q7 priority level 1
bandwidth percent 1 exit
```


© 2021 IP Infusion Inc. Proprietary

```
#show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]

L0  L1  L2  GroupPrioLevelShape Bandwidth


q0  -   -   -
-
q1  -   High-
-
q2  -   High-
-
q3  -   High-
-
q4  -   High-
-
q5  -   High-
-
q6  -   High-
-
q7  -   High-
-
#
```

Note: Unicast weight should be always higher than multicast weight. Between unicast and multicast traffic of different traffic class, scheduling will be as per configuration given in the queueing policy-map attached on the interface.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)# set qos wrr uc 1 non-uc 1`	Schedule unicast and multicast traffic in 1:1
`(config)#exit`	Exit configure mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-configuration qos
qos enable
qos statistics
set qos wrr uc 1 non-uc 1
!

#show policy-map

Type queuing policy-maps
========================
```

```
policy-map type queuing default default-out-policy
 class type queuing default q0
  priority
 class type queuing default q1
  priority
 class type queuing default q2
  priority
 class type queuing default q3
  priority
 class type queuing default q4
  priority
 class type queuing default q5
  priority
 class type queuing default q6
  priority
 class type queuing default q7
  priority
#show interface counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
 * indicates monitor is active
+-------------+--------------------+--------+-----------------+-------------------+----
-------------+-------------------+
|  Interface  |   Queue/Class-map  | Q-Size |     Tx pkts     |      Tx bytes     |
Dropped pkts   |   Dropped bytes   |
+-------------+--------------------+--------+-----------------+-------------------+----
-------------+-------------------+
 cpu          bpdu            (E) 0       1               68                0
0
 ce1/1        q1              (E) 424320   0              0                16817
16814000
 ce1/1        q7              (E) 0       1               64                0
0
 ce1/1        mc-q2           (E) 102336   1710           1710000           15059
15055000
 ce24/1       q7              (E) 0       1               64                0
0
 ce24/1       pg-q1           (I) 509600   NA             NA                NA
NA
 ce24/1       pg-q2           (I) 103584   NA             NA                NA
NA
By default, default-out-policy with priority on all queues is applied on ce1/1, hence
receiving only q2 multicast traffic

#show interface counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
 * indicates monitor is active
+-------------+--------------------+--------+-----------------+-------------------+----
-------------+-------------------+
|  Interface  |   Queue/Class-map  | Q-Size |     Tx pkts     |      Tx bytes     |
Dropped pkts   |   Dropped bytes   |
+-------------+--------------------+--------+-----------------+-------------------+----
-------------+-------------------+
```


© 2021 IP Infusion Inc. Proprietary

```
 cpu          bpdu            (E) 0       1              68              0
0
 ce1/1        q1             (E) 424320   816            816000          15279
15276000
 ce1/1        q7              (E) 0       1              64              0
0
 ce1/1        mc-q1          (E) 106080   816            816000          15229
15226000
 ce24/1       q7              (E) 0       1              64              0
0
 ce24/1       pg-q1           (I) 513344   NA             NA              NA
NA
```

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#policy-map type queuing default default-out-policy`	Enter policy-map type queueing default.
`(config-pmap-que-def)#class type queuing default q0`	Enter policy-class-map mode.
`(config-pmap-c-que-def)#wrr-queue weight 2`	Modify strict queue to wrr-queue with weight 2.
`(config-pmap-c-que-def)# class type queuing default q1`	
`(config-pmap-c-que-def)# wrr-queue weight 2`	
`(config-pmap-c-que-def)# class type queuing default q2`	
`(config-pmap-c-que-def)#wrr-queue weight 4`	
`(config-pmap-c-que-def)#exit`	Exit from policy-class-map mode.
`(config-pmap-que-def)#exit`	Exit from policy-map mode.
`(config)#exit`	Exit configure mode.

Validation

```
#show policy-map

Type queuing policy-maps
========================

policy-map type queuing default default-out-policy
 class type queuing default q0
wrr-queue weight 2
 class type queuing default q1
wrr-queue weight 2
 class type queuing default q2
wrr-queue weight 4
 class type queuing default q3
  priority
 class type queuing default q4
```

```
  priority
 class type queuing default q5
  priority
 class type queuing default q6
  priority
 class type queuing default q7
  priority

#show interface counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
 * indicates monitor is active
+-------------+--------------------+--------+-----------------+-------------------+----
-------------+--------------------+
|  Interface  |   Queue/Class-map  | Q-Size |     Tx pkts     |      Tx bytes     |
Dropped pkts   |   Dropped bytes   |
+-------------+--------------------+--------+-----------------+-------------------+----
-------------+--------------------+
 cpu          bpdu            (E) 0       1               68                0
0
 ce1/1        q1             (E) 421824   312             312000            8957
8954000
 ce1/1        q7              (E) 0       1               64                0
0
 ce1/1        mc-q2          (E) 106080   624             624000            8607
8592000
 ce24/1       q7              (E) 0       1               64                0
0
 ce24/1       pg-q1           (I) 411008   NA              NA                NA
NA
 ce24/1       pg-q2           (I) 106080   NA              NA                NA
NA
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 14 WRED Configuration

This chapter contains a complete sample of configuring WRED.

Topology

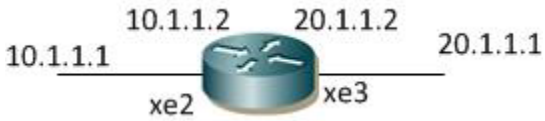


Figure 14-64: Simple configuration of WRED

L2/L3 Interface

The following steps describe how to configure WRED.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type qos match-all C1`	Configure class-map of type qos with name C1, and enter into class-map mode
`(config-cmap-que)#match cos 1`	Configure match cos value 1
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#policy-map type qos p1`	Configure plicy-map of type qos with name p1, and enter into policy-map mode
`(config-cmap-que)#class type qos C1`	Enter class-map configuration mode
`(config-cmap-que)# police cir 100 mbps pir 200 mbpsexit`	Configure police rate of cir 100 mbps and pir 200 mbpsExit out of class-map mode
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-qos)#exi`	Exit out of policy-class mode
`(config)#policy-map type queuing default p3`	Configure policy-map of type queuing with name p3, and enter into policy-map mode
`(config-cmap-que)#class type queuing default q0`	Enter class type of type queuing default configuration mode for q0
`(config-pmap-c-que-def)#wrr-queue weight 10`	Configure WRR weight of 10
`(config-pmap-c-que-def)#random-detect min-threshold 50 max-threshold 80 kbytes`	Configure WRED for minimum threshold of 50 kbytest and maximum threshold of 80 kbytes of queue size.
`(config-pmap-c-que-def)#exit`	Exit out of class configuration mode
`(config)#interface xe3`	Enter interface mode
`(config-if)#service-policy type queuing output P3`	Attach service-policy p3 of type queuing on out direction
`(config-if)#exit`	Exit out of interface mode
`(config)#interface xe2`	Enter interface mode
`(config-if)#service-policy type qos input p1`	Attach service-policy p1 of type qos on in direction

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit out of interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.2/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.3	Enter interface mode.
(config-if)# ip address 20.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
os enable
qos statistics
!
class-map type qos match-all 1
!
class-map type qos match-all C1
 match cos 1
!
policy-map type qos p1
 class type qos C1
  police cir 100 mbps pir 200 mbps
  exit
!
!
policy-map type queuing default p3
```


© 2021 IP Infusion Inc. Proprietary

```
 class type queuing default q0
  wrr-queue weight 10
  random-detect min-threshold 50 max-threshold 80 kbytes drop-probability 80
  exit
!
interface xe2
 service-policy type qos input p1
!
interface xe3
service-policy type queuing output p3

#show policy-map interface xe2

Interface xe2
Type QoS statistics status : enabled
Class-map (qos): C1 (match all)
 match cos 1
 police cir 100 mbps pir 200 mbps


Type Queuing policy-map : default-out-policy

Class-map (queuing): q0
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q1
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q2
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q3
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q4
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q5
 priority
      output              : 0 packets, 0 bytes
```

```
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q6
 priority
      output              : 6 packets, 724 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q7
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 1 packets, 90 bytes
      dropped      : 0 packets, 0 bytes

Wred/Tail Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```


© 2021 IP Infusion Inc. Proprietary

```
#show policy-map interface xe3

Interface xe3
Type Queuing policy-map : p3
Class-map (queuing): q0
 wrr-queue weight 10
 random-detect min-threshold 50 kbytes max-threshold 80 kbytes drop-probability 80
weight 8
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q1
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q2
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q3
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q4
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q5
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q6
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q7
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes
Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Wred/Tail Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets

#show queuing interface xe1/2

Egress Queuing for Ethernet ce2/1 [System]
------------------------------------------------------------------------------------
L0             L1             L2             Group  PrioLevel   Shape          Bandwidth
------------------------------------------------------------------------------------
q0                                              -      High        -              -
q1                                              -      High        -              -
q2                                              -      High        -              -
q3                                              -      High        -              -
q4                                              -      High        -              -
q5                                              -      High        -              -
q6                                              -      High        -              -
q7                                              -      High        -              -
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 15 Tail-Drop Configuration

Topology

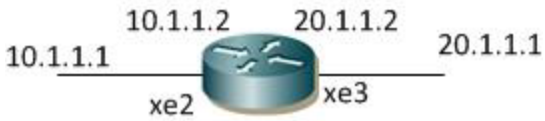


Figure 15-65: Simple configuration of Tail-Drop

Configuring Tail-Drop

The following steps describe how to configure Tail-Drop.

Configuration on L2/L3 Interfaces

Do the following to configure Tail-Drop on a queue.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type qos match-all C1`	Configure class-map of type qos with name C1, and enter into class-map mode
`(config-cmap-que)#match cos 1`	match cos value 1
`(OcNOS(config-cmap-qos)#exit`	Exit out of class-map
`(config)#policy-map type qos p1`	Enter policy-map configuration mode of type qos
`(config-cmap-que)#class type qos C1`	Enter class-map configuration mode
`(config-cmap-que)# police cir 100 mbps pir 200 mbps`	Configure police rate of cir 100 mbps and pir 200 mbps
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-qos)#exit`	Exit out of policy-class mode
`(config)#policy-map type queuing default p3`	Configure policy-map of type queuing with name p3 and enter into policy-map mode
`(config-cmap-que)#class type queuing default q1`	Enter class type of type queuing default configuration mode for q1
`(config-pmap-c-que)#shape percent 20`	Configure shaping to 20 percent of bandwidth available on interface
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#class type queuing default q2`	Enter class type of type queuing default configuration mode for q2
`(config-pmap-c-que)#bandwidth 25000 kbps`	Configure bandwidth to 25000 kbps
`(config-pmap-c-que)#queue-limit 99 packets`	Configure tail-drop to 99 packets
`(config-pmap-c-que)#exit`	Exit out of policy-class mode

© 2021 IP Infusion Inc. Proprietary

(config-pmap-que)#class type queuing default q3	Enter class type of type queuing default configuration mode for q3
(config-pmap-c-que)#queue-limit 101 packets	Configure tail-drop to 101 packets
(config-pmap-c-que)#exit	Exit out of policy-class mode
(config-pmap-que)#exit	Exit out of policy-map mode
(config)#interface xe2	Enter interface mode
(config-if)#service-policy type queuing output p3	Attach service-policy p3 of type queuing on out direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter interface mode
(config-if)#service-policy type qos input p1	Attach service-policy p1 of type qos on in direction
(config-if)#exit	Exit out of interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.2/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.3	Enter interface mode.
(config-if)# ip address 20.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable
!
qos statistics
```


© 2021 IP Infusion Inc. Proprietary

```
!
class-map type qos match-all C1
 match cos 1
!
policy-map type qos p1
 class type qos C1
  police cir 100 mbps pir 200 mbps
  exit
!
!
policy-map type queuing default p3
 class type queuing default q1
  shape percent 20
  priority
  exit
 class type queuing default q2
  priority
  queue-limit 99 packets
  bandwidth 25000 kbps
  exit
 class type queuing default q3
  priority
  queue-limit 101 packets
  exit

#show class-map
Type qos class-maps
  ===================
      class-map type qos match-all C1
         match cos 1

      class-map type qos match-any class-default


  Type queuing class-maps
  =======================
      class-map type queuing q0

      class-map type queuing q1

      class-map type queuing q2

      class-map type queuing q3

      class-map type queuing q4

      class-map type queuing q5

      class-map type queuing q6
```

```
      class-map type queuing q7


  Type Vlan-Queuing class-maps


#show policy-map

Type qos policy-maps
====================

policy-map type qos p1
 class type qos C1
  police cir 100 mbps pir 200 mbps


Type queuing policy-maps
========================

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority
 class type queuing default q1
  priority
 class type queuing default q2
  priority
 class type queuing default q3
  priority
 class type queuing default q4
  priority
 class type queuing default q5
  priority
 class type queuing default q6
  priority
 class type queuing default q7
  priority

policy-map type queuing default p3
 class type queuing default q0
  priority
 class type queuing default q1
  shape percent 20
  priority
 class type queuing default q2
  priority
  queue-limit 99 packets
  bandwidth 25000 kbps
 class type queuing default q3
  priority
  queue-limit 101 packets
```


© 2021 IP Infusion Inc. Proprietary

```
 class type queuing default q4
  priority
 class type queuing default q5
  priority
 class type queuing default q6
  priority
 class type queuing default q7
  priority

#show policy-map interface xe2

QoS statistics status : enabled

Class-map (qos): C1 (match all)
 match cos 1
 police cir 100 mbps pir 200 mbps


Type Queuing policy-map : default-out-policy

Class-map (queuing): q0
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q1
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q2
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q3
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q4
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q5
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes
```

```
Class-map (queuing): q6
 priority
      output              : 6 packets, 724 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q7
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 1 packets, 90 bytes
      dropped      : 0 packets, 0 bytes

Wred/Tail Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets

#show policy-map interface xe3
```


© 2021 IP Infusion Inc. Proprietary

```
Type Queuing policy-map : p3

Class-map (queuing): q0
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q1
 shape percent 20
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q2
 priority
 queue-limit 99 packets
 bandwidth 25000 kbps
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q3
 priority
 queue-limit 101 packets
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q4
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q5
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q6
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): q7
 priority
      output              : 0 packets, 0 bytes
      dropped             : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Wred/Tail Drop Statistics :
-----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets

OcNOS#show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]
L0             L1             L2             Group  PrioLevel   Shape          Bandwidth
-------------------------------------------------------------------------------------------
-------------
q0                                               -      High        -              -
q1                                               -      High        -              -
q2                                               -      High        -              -
q3                                               -      High        -              -
q4                                               -      High        -              -
q5                                               -      High        -              -
q6                                               -      High        -              -
q7                                               -      High        -              -

OcNOS#show queuing interface xe3
```


© 2021 IP Infusion Inc. Proprietary

```
Egress Queuing for Ethernet xe3 [System]
-----------------------------------------------------------------------------------------
L0              L1              L2              Group  PrioLevel   Shape          Bandwidth
-----------------------------------------------------------------------------------------
q0                                              -      High        -              -
q1                                              -      High        20 percent     -
q2                                                 -      High        -              25000 kbps
q3                                              -      High        -              -
q4                                              -      High        -              -
q5                                              -      High        -              -
q6                                              -      High        -              -
q7                                              -      High        -              -
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 16 Hierarchical Queuing Configuration

This chapter contains a complete sample of configuring hierarchical queuing.

Topology



Figure 16-66: Simple configuration of Hierarchical Queuing

Configuring Hierarchical Queuing

Do the following to configure 3-level hierarchical queuing on an interface.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type qos match-any C_QOS1`	Configure class-map C_QOS1 of type qos and enter into class-map mode
`(config-cmap-qos)#match cos 0`	Configure match criteria as cos 0
`(config-cmap-qos)#match dscp 0-7`	Configure match criteria as dscp 0-7
`(config-cmap-qos)#exit`	Exit out of cmap mode
`(config)#class-map type qos match-any C_QOS2`	Configure class-map C_QOS2 of type qos and enter into class-map mode
`(config-cmap-qos)#match cos 1`	Configure match criteria as cos 1
`(config-cmap-qos)#match dscp 8-15`	Configure match criteria as dscp 8-15
`(config-cmap-qos)#exit`	Exit out of cmap mode
`(config)#class-map type qos match-any C_QOS3`	Configure class-map C_QOS3 of type qos and enter into class-map mode
`(config-cmap-qos)#match cos 2`	Configure match criteria as cos 2
`(config-cmap-qos)#match dscp 16-23`	Configure match criteria as dscp 16-23
`(config-cmap-qos)#exit`	Exit out of cmap mode
`(config)#class-map type qos match-any C_QOS4`	Configure class-map C_QOS4 of type qos and enter into class-map mode
`(config-cmap-qos)#match cos 3`	Configure match criteria as cos 3
`(config-cmap-qos)#match dscp 24-31`	Configure match criteria as dscp 24-31
`(config-cmap-qos)#exit`	Exit out of cmap mode
`(config)#class-map type qos match-any C_QOS5`	Configure class-map C_QOS5 of type qos and enter into class-map mode
`(config-cmap-qos)#match cos 4`	Configure match criteria as cos 4
`(config-cmap-qos)#match dscp 32-39`	Configure match criteria as dscp 32-39

© 2021 IP Infusion Inc. Proprietary

(config-cmap-qos)#exit	Exit out of cmap mode
(config)#class-map type qos match-any C_QOS6	Configure class-map C_QOS6 of type qos and enter into class-map mode
(config-cmap-qos)#match cos 5	Configure match criteria as cos 5
(config-cmap-qos)#match dscp 40-47	Configure match criteria as dscp 40-47
(config-cmap-qos)#exit	Exit out of cmap mode
(config)#class-map type qos match-any C_QOS7	Configure class-map C_QOS7 of type qos and enter into class-map mode
(config-cmap-qos)#match cos 6	Configure match criteria as cos 6
(config-cmap-qos)#match dscp 48-55	Configure match criteria as dscp 48-55
(config-cmap-qos)#exit	Exit out of cmap mode
(config)#class-map type qos match-any C_QOS8	Configure class-map C_QOS8 of type qos and enter into class-map mode
(config-cmap-qos)#match cos 7	Configure match criteria as cos 7
(config-cmap-qos)#match dscp 56-63	Configure match criteria as dscp 56-63
(config-cmap-qos)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any cq1	Configure class-map cq1 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 1	Configure match criteria as qos-group 1
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#class-map type queuing match-any cq2	Configure class-map cq2 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 2	Configure match criteria as qos-group 2
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#class-map type queuing match-any cq3	Configure class-map cq3 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 3	Configure match criteria as qos-group 3
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#class-map type queuing match-any cq4	Configure class-map cq4 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 4	Configure match criteria as qos-group 4
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#class-map type queuing match-any cq5	Configure class-map cq5 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 5	Configure match criteria as qos-group 5
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#class-map type queuing match-any cq6	Configure class-map cq6 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 6	Configure match criteria as qos-group 6
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#class-map type queuing match-any cq7	Configure class-map cq7 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 7	Configure match criteria as qos-group 7
(config-cmap-que)#exit	Exit out of cmap mode.

© 2021 IP Infusion Inc. Proprietary

(config)#class-map type queuing match-any cq8	Configure class-map cq8 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 8	Configure match criteria as qos-group 8
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#policy-map type qos pmap1	Configure policy-map pmap1 og type qos and enter into policy-map mode.
(config-pmap-qos)#class type qos C_QOS1	Assign class C-QOS1 to pmap1 and enter into policy-class-map mode.
(config-pmap-c-qos)#set qos-group 1	Remark matched traffic to qos-group 1
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS2	Assign class C-QOS2 to pmap1 and enter into policy-class-map mode.
(config-pmap-c-qos)#set qos-group 2	Remark matched traffic to qos-group 2
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS3	Assign class C-QOS3 to pmap1 and enter into policy-class-map mode.
(config-pmap-c-qos)#set qos-group 3	Remark matched traffic to qos-group 3
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS4	Assign class C-QOS4 to pmap1 and enter into policy-class-map mode.
(config-pmap-c-qos)#set qos-group 4	Remark matched traffic to qos-group 4
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS5	Assign class C-QOS5 to pmap1 and enter into policy-class-map mode.
(config-pmap-c-qos)#set qos-group 5	Remark matched traffic to qos-group 5
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS6	Assign class C-QOS6 to pmap1 and enter into policy-class-map mode.
(config-pmap-c-qos)#set qos-group 6	Remark matched traffic to qos-group 6
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS7	Assign class C-QOS7 to pmap1 and enter into policy-class-map mode.
(config-pmap-c-qos)#set qos-group 7	Remark matched traffic to qos-group 7
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS8	Assign class C-QOS8 to pmap1 and enter into policy-class-map mode.
(config-pmap-c-qos)#set qos-group 8	Remark matched traffic to qos-group 8
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#exit	Exit out of policy-map mode
(config)#policy-map type queuing P1P1	Configure policy-map of type queuing P1P1 and enter into policy-map mode.
(config-pmap-que)#class type queuing cq1	Assign class cq1 to policy-map P1 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 20	Shape the matched traffic to percent 20
(config-pmap-c-que)#queue-limit 70 packets	Configure tail-drop on q1 to 70 packets.

(config-pmap-c-que)#bandwidth percent 18	Configure minimum bandwidth to 18 percent on q1.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing cq2	Assign class cq2 to policy-map P1 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 80	Shape the matched traffic to percent 80
(config-pmap-c-que)#queue-limit 70 packets	Configure tail-drop on q2 to 70 packets.
(config-pmap-c-que)#bandwidth percent 75	Configure minimum bandwidth to 75 percent on q2.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#policy-map type queuing P2	Configure policy-map of type queuing P2 and enter into policy-map mode.
(config-pmap-que)#class type queuing cq3	Assign class cq3 to policy-map P2 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 25	Shape the matched traffic to percent 25
(config-pmap-c-que)#random-detect minimum-threshold 50 maximum-threshold 75 kbytes	Configure WRED on q3 to minimum threshold 50 and maximum threshold 75 packets.
(config-pmap-c-que)#bandwidth percent 20	Configure minimum bandwidth to 20 percent on q3.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing cq4	Assign class cq4 to policy-map P2 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 75	Shape the matched traffic to percent 75
(config-pmap-c-que)#random-detect minimum-threshold 50 maximum-threshold 75 kbytes	Configure WRED on q4 to minimum threshold 50 and maximum threshold 75 kbytes.
(config-pmap-c-que)#bandwidth percent 65	Configure minimum bandwidth to 65 percent on q4.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#policy-map type queuing P3	Configure policy-map of type queuing P3 and enter into policy-map mode.
(config-pmap-que)#class type queuing cq5	Assign class cq5 to policy-map P3 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 40	Shape the matched traffic to percent 40
(config-pmap-c-que)#queue-limit 100 packets	Configure Tail-Drop on q5 to 100 packets.
(config-pmap-c-que)#bandwidth percent 35	Configure minimum bandwidth to 35 percent on q5.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing cq6	Assign class cq6 to policy-map P3 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 60	Shape the matched traffic to percent 60
(config-pmap-c-que)#queue-limit 100 packets	Configure Tail-Drop on q6 to 100 packets.
(config-pmap-c-que)#bandwidth percent 55	Configure minimum bandwidth to 55 percent on q6.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#policy-map type queuing P4	Configure policy-map of type queuing P4 and enter into policy-map mode.
(config-pmap-que)#class type queuing cq7	Assign class cq7 to policy-map P4 and enter into policy-class-map mode.

© 2021 IP Infusion Inc. Proprietary

(config-pmap-c-que)#shape average percent 40	Shape the matched traffic to percent 40
(config-pmap-c-que)#random-detect minimum-threshold 80 packets maximum-threshold 100 packets	Configure WRED on q7 to maximum threshold of 80 packets and maximum threshold of 100 packets..
(config-pmap-c-que)#bandwidth percent 35	Configure minimum bandwidth to 35 percent on q7.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing cq8	Assign class cq8 to policy-map P4 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 60	Shape the matched traffic to percent 60
(config-pmap-c-que)#random-detect minimum-threshold 80 packets maximum-threshold 100 packets	Configure WRED on q8 to minimum threshold of 80 packets and maximum threshold of 100 packets..
(config-pmap-c-que)#bandwidth percent 55	Configure minimum bandwidth to 55 percent on q8.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#class-map type queuing match-any empty1	Configure class-map of type queuing empty1
(config-cmap-que)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any empty2	Configure class-map of type queuing empty2
(config-cmap-que)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any empty3	Configure class-map of type queuing empty3
(config-cmap-que)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any empty4	Configure class-map of type queuing empty4
(config-cmap-que)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any empty5	Configure class-map of type queuing empty5
(config-cmap-que)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any empty6	Configure class-map of type queuing empty6
(config-cmap-que)#exit	Exit out of cmap mode
(config)#policy-map type queuing P1P2	Configure policy-map of type queuing P1P2 and enter into policy-map mode.
(config-pmap-que)#class type queuing empty1	Assign class-map of type queuing empty1 to P1P2 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 40	Shape the matched traffic to 40 percent
(config-pmap-c-que)#bandwidth percent 30	Configure minimum bandwidth to 30 percent on empty1.
(config-pmap-c-que)#service-policy P1P1	Assign service-policy P1P1
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing empty2	Assign class-map of type queuing empty2 to P1P2 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 60	Shape the matched traffic to 60 percent
(config-pmap-c-que)#bandwidth percent 55	Configure minimum bandwidth to 55 percent on empty2.
(config-pmap-c-que)#service-policy P2	Assign service-policy P2

(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#policy-map type queuing P3P4	Configure policy-map of type queuing P3P4 and enter into policy-map mode.
(config-pmap-que)#class type queuing empty3	Assign class-map of type queuing empty3 to P3P4 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 40	Shape the matched traffic to 40 percent
(config-pmap-c-que)#bandwidth percent 35	Configure minimum bandwidth to 35 percent on empty3.
(config-pmap-c-que)#service-policy P3	Assign service-policy P3
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing empty4	Assign class-map of type queuing empty4 to P3P4 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 60	Shape the matched traffic to 60 percent
(config-pmap-c-que)#bandwidth percent 50	Configure minimum bandwidth to 50 percent on empty4.
(config-pmap-c-que)#service-policy P4	Assign service-policy P4
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#policy-map type queuing Pend	Configure policy-map of type queuing Pend and enter into policy-map mode.
(config-pmap-que)#class type queuing empty5	Assign class-map of type queuing empty5 to Pend and enter into policy-class-map mode.
(config-pmap-c-que)#shape average 400 mbps	Shape the matched traffic to 400 mbps
(config-pmap-c-que)#bandwidth 350 mbps	Configure minimum bandwidth to 350 mbps.
(config-pmap-c-que)#service-policy P1P1	Assign service-policy P1P1
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing empty6	Assign class-map of type queuing empty6 to Pend and enter into policy-class-map mode.
(config-pmap-c-que)#shape average 500 mbps	Shape the matched traffic to 500 mbps
(config-pmap-c-que)#bandwidth 450 mbps	Configure minimum bandwidth to 450 mbps.
(config-pmap-c-que)#service-policy P3P4	Assign service-policy P3P4
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#interface xe2	Enter into interface mode
(config-if)#service-policy type qos input pmap1	Assign service-policy of type qos policy-map1.
(config-if)#exit	Exit out of intf mode
(config)#interface xe3	Enter into interface mode
(config-if)#service-policy type queuing output Pend	Assign service-policy of type queing pend on out direction.
(config-if)#exit	Exit out of interface mode.

Configuring one of the scheduler modes implicitly un-configures other modes, only one scheduler mode can be configured at a time.

(config)#set qos wrr uc 1 non-uc 2	Schedule unicast and multicast traffic in 1:2

© 2021 IP Infusion Inc. Proprietary

(config)#set qos sp	Set strict priority between unicast and multicast traffic, with higher priority to multicast traffic
(config)#interface xe49/2	Enter interface mode
(config-if)#exit	Exit interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Specify VLAN for bridge 1.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2-3 bridge 1 state enable	Enable VLAN (2-3) on bridge 1. Specifying the enable state.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface vlan1.2	Enter interface mode.
(config-if)# ip address 10.1.1.2/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.3	Enter interface mode.
(config-if)# ip address 20.1.1.1/24	Configure the IP address.
(config-if)#exit	Exit the interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure xe2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the interface mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos
qos enable
!
set qos wrr uc 1 non-uc 2
qos statistics
!
class-map type qos match-any C_QOS1
 match dscp 0-7
 match cos 0
!
class-map type qos match-any C_QOS2
 match dscp 8-15
 match cos 1
```

```
!
class-map type qos match-any C_QOS3
 match dscp 16-23
 match cos 2
!
class-map type qos match-any C_QOS4
 match dscp 24-31
 match cos 3
!
class-map type qos match-any C_QOS5
 match dscp 32-39
 match cos 4
!
class-map type qos match-any C_QOS6
 match dscp 40-47
 match cos 5
!
class-map type qos match-any C_QOS7
 match dscp 48-55
 match cos 6
!
class-map type qos match-any C_QOS8
 match dscp 56-63
 match cos 7
!
class-map type queuing match-any cq1
 match qos-group 1
!
class-map type queuing match-any cq2
 match qos-group 2
!
class-map type queuing match-any cq3
 match qos-group 3
!
class-map type queuing match-any cq4
 match qos-group 4
!
class-map type queuing match-any cq5
!
class-map type queuing match-any cq6
 match qos-group 6
!
class-map type queuing match-any cq7
 match qos-group 7
!
class-map type queuing match-any cq8
 match qos-group 8
!
class-map type queuing match-any empty1
!
```


© 2021 IP Infusion Inc. Proprietary

```
class-map type queuing match-any empty2
!
class-map type queuing match-any empty3
!
class-map type queuing match-any empty4
!
class-map type queuing match-any empty5
!
class-map type queuing match-any empty6
!
policy-map type qos pmap1
 class type qos C_QOS1
  set qos-group 1
  exit
 class type qos C_QOS2
  set qos-group 2
  exit
 class type qos C_QOS3
  set qos-group 3
  exit
 class type qos C_QOS4
  set qos-group 4
  exit
 class type qos C_QOS5
  set qos-group 5
  exit
 class type qos C_QOS6
  set qos-group 6
  exit
 class type qos C_QOS7
  set qos-group 7
  exit
 class type qos C_QOS8
  set qos-group 8
  exit
!
policy-map type queuing P1P1
 class type queuing cq1
  shape average percent 20
  wrr-queue weight 1
  queue-limit 70 packets
  bandwidth percent 18
  exit
 class type queuing cq2
  shape average percent 80
  wrr-queue weight 1
  queue-limit 70 packets
  bandwidth percent 75
  exit
!
```

```
policy-map type queuing P2
 class type queuing cq3
  shape average percent 25
  wrr-queue weight 1
  random-detect minimum-threshold 50 maximum-threshold 75 kbytes
  bandwidth percent 20
  exit
 class type queuing cq4
  shape average percent 75
  wrr-queue weight 1
  random-detect minimum-threshold 50 maximum-threshold 75 kbytes
  bandwidth percent 65
  exit
!
policy-map type queuing P3
 class type queuing cq5
  shape average percent 40
  wrr-queue weight 1
  queue-limit 100 packets
  bandwidth percent 35
  exit
 class type queuing cq6
  shape average percent 60
  wrr-queue weight 1
  queue-limit 100 packets
  bandwidth percent 55
  exit
!
policy-map type queuing P4
 class type queuing cq7
  shape average percent 40
  wrr-queue weight 1
  random-detect minimum-threshold 80 maximum-threshold 100 packets
  bandwidth percent 35
  exit
 class type queuing cq8
  shape average percent 60
  wrr-queue weight 1
  random-detect minimum-threshold 80 maximum-threshold 100 packets
  bandwidth percent 55
  exit
!
!
policy-map type queuing P3P4
 class type queuing empty3
  shape average percent 40
  wrr-queue weight 1
  bandwidth percent 35
  service-policy P3
  exit
```


© 2021 IP Infusion Inc. Proprietary

```
 class type queuing empty4
  shape average percent 60
  wrr-queue weight 1
  bandwidth percent 50
  service-policy P4
  exit
!
policy-map type queuing P1P2
 class type queuing empty1
  shape average percent 40
  wrr-queue weight 1
  bandwidth percent 30
  service-policy P1P1
  exit
 class type queuing empty2
  shape average percent 60
  wrr-queue weight 1
  bandwidth percent 55
  service-policy P2
  exit
!
policy-map type queuing Pend
 class type queuing empty5
  shape average 400 mbps
  wrr-queue weight 1
  bandwidth 350 mbps
  service-policy P1P1
  exit
 class type queuing empty6
  shape average 500 mbps
  wrr-queue weight 1
  bandwidth 450 mbps
  service-policy P3P4
  exit
!
!
interface xe2
 service-policy type qos input pmap1
!
interface xe3
 service-policy type queuing output Pend
!



#sh class-map

  Type qos class-maps
  ===================
      class-map type qos match-any C_QOS1
```

```
        match cos 0
        match dscp 0-7

    class-map type qos match-any C_QOS2
        match cos 1
        match dscp 8-15

    class-map type qos match-any C_QOS3
        match cos 2
        match dscp 16-23

    class-map type qos match-any C_QOS4
        match cos 3
        match dscp 24-31

    class-map type qos match-any C_QOS5
        match cos 4
        match dscp 32-39

    class-map type qos match-any C_QOS6
        match cos 5
        match dscp 40-47

    class-map type qos match-any C_QOS7
        match cos 6
        match dscp 48-55

    class-map type qos match-any C_QOS8
        match cos 7
        match dscp 56-63

    class-map type qos match-any class-default


Type queuing class-maps
=======================
    class-map type queuing match-any cq1
        match qos-group 1

    class-map type queuing match-any cq2
        match qos-group 2

    class-map type queuing match-any cq3
        match qos-group 3

    class-map type queuing match-any cq4
        match qos-group 4

    class-map type queuing match-any cq5
```


© 2021 IP Infusion Inc. Proprietary

```
      class-map type queuing match-any cq6
         match qos-group 6

      class-map type queuing match-any cq7
         match qos-group 7

      class-map type queuing match-any cq8
         match qos-group 8

      class-map type queuing match-any empty1

      class-map type queuing match-any empty2

      class-map type queuing match-any empty3

      class-map type queuing match-any empty4

      class-map type queuing match-any empty5

      class-map type queuing match-any empty6

      class-map match-any q0

      class-map match-any q1

      class-map match-any q2

      class-map match-any q3

      class-map match-any q4

      class-map match-any q5

      class-map match-any q6

      class-map match-any q7


  Type Vlan-Queuing class-maps
  ============================

#show policy-map

Type qos policy-maps
====================

policy-map type qos pmap1
 class type qos C_QOS1
  set qos-group 1
  exit
```

```
 class type qos C_QOS2
  set qos-group 2
  exit
 class type qos C_QOS3
  set qos-group 3
  exit
 class type qos C_QOS4
  set qos-group 4
  exit
 class type qos C_QOS5
  set qos-group 5
  exit
 class type qos C_QOS6
  set qos-group 6
  exit
 class type qos C_QOS7
  set qos-group 7
  exit
 class type qos C_QOS8
  set qos-group 8
  exit


Type queuing policy-maps
========================

policy-map type queuing P1P1
 class type queuing cq1
  shape average percent 20
  wrr-queue weight 1
  queue-limit 70 packets
  bandwidth percent 18
  exit
 class type queuing cq2
  shape average percent 80
  wrr-queue weight 1
  queue-limit 70 packets
  bandwidth percent 75
  exit

policy-map type queuing P1P2
 class type queuing empty1
  shape average percent 40
  wrr-queue weight 1
  bandwidth percent 30
  service-policy P1P1
  exit
 class type queuing empty2
  shape average percent 60
  wrr-queue weight 1
```


© 2021 IP Infusion Inc. Proprietary

```
  bandwidth percent 55
  service-policy P2
  exit

policy-map type queuing P2
 class type queuing cq3
  shape average percent 25
  wrr-queue weight 1
  random-detect minimum-threshold 50 maximum-threshold 75 kbytes
  bandwidth percent 20
  exit
 class type queuing cq4
  shape average percent 75
  wrr-queue weight 1
  random-detect minimum-threshold 50 maximum-threshold 75 kbytes
  bandwidth percent 65
  exit

policy-map type queuing P3
 class type queuing cq5
  shape average percent 40
  wrr-queue weight 1
  queue-limit 100 packets
  bandwidth percent 35
  exit
 class type queuing cq6
  shape average percent 60
  wrr-queue weight 1
  queue-limit 100 packets
  bandwidth percent 55
  exit

policy-map type queuing P3P4
 class type queuing empty3
  shape average percent 40
  wrr-queue weight 1
  bandwidth percent 35
  service-policy P3
  exit
 class type queuing empty4
  shape average percent 60
  wrr-queue weight 1
  bandwidth percent 50
  service-policy P4
  exit

policy-map type queuing P4
 class type queuing cq7
  shape average percent 40
  wrr-queue weight 1
```

```
  random-detect minimum-threshold 80 maximum-threshold 100 packets
  bandwidth percent 35
  exit
 class type queuing cq8
  shape average percent 60
  wrr-queue weight 1
  random-detect minimum-threshold 80 maximum-threshold 100 packets
  bandwidth percent 55
  exit

policy-map type queuing Pend
 class type queuing empty5
  shape average 400 mbps
  wrr-queue weight 1
  bandwidth 350 mbps
  service-policy P1P1
  exit
 class type queuing empty6
  shape average 500 mbps
  wrr-queue weight 1
  bandwidth 450 mbps
  service-policy P3P4
  exit

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 1
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 1
  exit
 class type queuing default q3
  priority level 1
  exit
 class type queuing default q4
  priority level 1
  exit
 class type queuing default q5
  priority level 1
  exit
 class type queuing default q6
  priority level 1
  exit
 class type queuing default q7
  priority level 1
  exit
```


© 2021 IP Infusion Inc. Proprietary

```
#show policy-map interface xe2

Interface xe2
Global statistics status : enabled

Service-policy (qos) input     : pmap1
--------------------------------
Class-map (qos): C_QOS1 (match any)
 match dscp 0-7
 match cos 0
 set qos-group 1
      matched      : 2 packets, 128 bytes
      transmitted  : 2 packets, 128 bytes

Class-map (qos): C_QOS2 (match any)
 match dscp 8-15
 match cos 1
 set qos-group 2
      matched      : 23751790 packets, 1520114560 bytes
      transmitted  : 23751790 packets, 1520114560 bytes

Class-map (qos): C_QOS3 (match any)
 match dscp 16-23
 match cos 2
 set qos-group 3
      matched      : 5412521 packets, 346401344 bytes
      transmitted  : 5412521 packets, 346401344 bytes

Class-map (qos): C_QOS4 (match any)
 match dscp 24-31
 match cos 3
 set qos-group 4
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS5 (match any)
 match dscp 32-39
 match cos 4
 set qos-group 5
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS6 (match any)
 match dscp 40-47
 match cos 5
 set qos-group 6
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes
```

```
Class-map (qos): C_QOS7 (match any)
 match dscp 48-55
 match cos 6
 set qos-group 7
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS8 (match any)
 match dscp 56-63
 match cos 7
 set qos-group 8
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes


Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 1 packets, 64 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 2058 packets, 131912 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 4 packets, 272 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets


#show policy-map interface xe3

Interface xe3
Global statistics status : enabled
```

```
Service-policy (queuing) output: Pend
-----------------------------------
Class-map (queuing): empty5
 shape average 400 mbps
 wrr-queue weight 1
 bandwidth 350 mbps

     Service-policy (queuing) output: P1P1
     -----------------------------------
     Class-map (queuing): cq1
      match qos-group 1
      shape percent 20
 wrr-queue weight 1
      queue-limit 70 packets
      bandwidth percent 18
           output       : 1 packets, 64 bytes
           dropped      : 0 packets, 0 bytes

     Class-map (queuing): cq2
      match qos-group 2
      shape percent 80
 wrr-queue weight 1
      queue-limit 70 packets
      bandwidth percent 75
           output       : 10290336 packets, 658581504 bytes
           dropped      : 13382099 packets, 856454336 bytes

Class-map (queuing): empty6
 shape average 500 mbps
 wrr-queue weight 1
 bandwidth 450 mbps

     Service-policy (queuing) output: P3P4
     -----------------------------------
     Class-map (queuing): empty3
      shape percent 40
 wrr-queue weight 1
      bandwidth percent 35

          Service-policy (queuing) output: P3
          -----------------------------------
          Class-map (queuing): cq5
           shape percent 40
 wrr-queue weight 1
           queue-limit 100 packets
           bandwidth percent 35
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
          Class-map (queuing): cq6
           match qos-group 6
           shape percent 60
 wrr-queue weight 1
           queue-limit 100 packets
           bandwidth percent 55
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

     Class-map (queuing): empty4
      shape percent 60
 wrr-queue weight 1
      bandwidth percent 50

          Service-policy (queuing) output: P4
          -----------------------------------
          Class-map (queuing): cq7
           match qos-group 7
           shape percent 40
 wrr-queue weight 1
           random-detect minimum-threshold 80 maximum-threshold 100 packets
bytes
kbytes
percent
           bandwidth percent 35
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

          Class-map (queuing): cq8
           match qos-group 8
           shape percent 60
 wrr-queue weight 1
           random-detect minimum-threshold 80 maximum-threshold 100 packets
bytes
kbytes
percent
           bandwidth percent 55
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 2011 packets, 128964 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 11 packets, 748 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 13382099 packets
 yellow : 0 packets
 red    : 0 packets


#show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]
------------------------------------------------------------------------------
L0              L1              L2              Group  PrioLevel   Shape
  Bandwidth
------------------------------------------------------------------------------
q0                                              -      High        -
  -
q1                                              -      High        -
  -
q2                                              -      High        -
  -
q3                                              -      High        -
  -
q4                                              -      High        -
  -
q5                                              -      High        -
  -
q6                                              -      High        -
  -
q7                                              -      High        -


#show queuing interface xe3

Egress Queuing for Ethernet xe3 [System]
------------------------------------------------------------------------------
L0              L1              L2              Group  PrioLevel   Shape
```

```
  Bandwidth
-------------------------------------------------------------------------------
empty5                                      -      -           400 mbps
  350 mbps
               cq1                          1      -           20 percent
  18 percent
               cq2                          2      -           80 percent
  75 percent
empty6                                      -      -           500 mbps
  450 mbps
               empty3                       -      -           40 percent
  35 percent
                              cq5           -      -           40 percent
  35 percent
                              cq6           6      -           60 percent
  55 percent
               empty4                       -      -           60 percent
  50 percent
                              cq7           7      -           40 percent
  35 percent
                              cq8           8      -           60 percent
  55 percent


(config)#set qos wrr uc 1 non-uc 127
(config)#exit

#show policy-map interface xe2

Interface xe2
Global statistics status : enabled

Service-policy (qos) input     : pmap1
--------------------------------
Class-map (qos): C_QOS1 (match any)
 match dscp 0-7
 match cos 0
 set qos-group 1
      matched      : 2 packets, 128 bytes
      transmitted  : 2 packets, 128 bytes

Class-map (qos): C_QOS2 (match any)
 match dscp 8-15
 match cos 1
 set qos-group 2
      matched      : 24126931 packets, 1544123584 bytes
      transmitted  : 24126931 packets, 1544123584 bytes

Class-map (qos): C_QOS3 (match any)
 match dscp 16-23
```


© 2021 IP Infusion Inc. Proprietary

```
 match cos 2
 set qos-group 3
      matched      : 5412521 packets, 346401344 bytes
      transmitted  : 5412521 packets, 346401344 bytes

Class-map (qos): C_QOS4 (match any)
 match dscp 24-31
 match cos 3
 set qos-group 4
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS5 (match any)
 match dscp 32-39
 match cos 4
 set qos-group 5
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS6 (match any)
 match dscp 40-47
 match cos 5
 set qos-group 6
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS7 (match any)
 match dscp 48-55
 match cos 6
 set qos-group 7
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS8 (match any)
 match dscp 56-63
 match cos 7
 set qos-group 8
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes


Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
```

```
      output       : 1 packets, 64 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 2245 packets, 143880 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
```


© 2021 IP Infusion Inc. Proprietary

```
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 4 packets, 272 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets


#show policy-map interface xe3

Interface xe3
Global statistics status : enabled

Service-policy (queuing) output: Pend
-----------------------------------
Class-map (queuing): empty5
 shape average 400 mbps
 wrr-queue weight 1
 bandwidth 350 mbps

     Service-policy (queuing) output: P1P1
     ----------------------------------
     Class-map (queuing): cq1
      match qos-group 1
      shape percent 20
 wrr-queue weight 1
      queue-limit 70 packets
      bandwidth percent 18
           output       : 1 packets, 64 bytes
           dropped      : 0 packets, 0 bytes

     Class-map (queuing): cq2
      match qos-group 2
      shape percent 80
 wrr-queue weight 1
      queue-limit 70 packets
```

```
      bandwidth percent 75
           output       : 10761532 packets, 688738048 bytes
           dropped      : 13382100 packets, 856454400 bytes

Class-map (queuing): empty6
 shape average 500 mbps
 wrr-queue weight 1
 bandwidth 450 mbps

     Service-policy (queuing) output: P3P4
     -----------------------------------
     Class-map (queuing): empty3
      shape percent 40
 wrr-queue weight 1
      bandwidth percent 35

          Service-policy (queuing) output: P3
          -----------------------------------
          Class-map (queuing): cq5
           shape percent 40
 wrr-queue weight 1
           queue-limit 100 packets
           bandwidth percent 35
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

          Class-map (queuing): cq6
           match qos-group 6
           shape percent 60
 wrr-queue weight 1
           queue-limit 100 packets
           bandwidth percent 55
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

     Class-map (queuing): empty4
      shape percent 60
 wrr-queue weight 1
      bandwidth percent 50

          Service-policy (queuing) output: P4
          -----------------------------------
          Class-map (queuing): cq7
           match qos-group 7
           shape percent 40
 wrr-queue weight 1
           random-detect minimum-threshold 80 maximum-threshold 100 packets
bytes
kbytes
percent
```


© 2021 IP Infusion Inc. Proprietary

```
           bandwidth percent 35
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

          Class-map (queuing): cq8
           match qos-group 8
           shape percent 60
 wrr-queue weight 1
           random-detect minimum-threshold 80 maximum-threshold 100 packets
bytes
kbytes
percent
           bandwidth percent 55
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
```

```
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 2246 packets, 144004 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 12 packets, 816 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 13382099 packets
 yellow : 0 packets
 red    : 0 packets


(config)#set qos wrr uc 1 non-uc 2
(config)#exit
```


© 2021 IP Infusion Inc. Proprietary

```
#show policy-map interface xe2

Interface xe2
Global statistics status : enabled

Service-policy (qos) input     : pmap1
--------------------------------
Class-map (qos): C_QOS1 (match any)
 match dscp 0-7
 match cos 0
 set qos-group 1
      matched      : 2 packets, 128 bytes
      transmitted  : 2 packets, 128 bytes

Class-map (qos): C_QOS2 (match any)
 match dscp 8-15
 match cos 1
 set qos-group 2
      matched      : 24459636 packets, 1565416704 bytes
      transmitted  : 24459636 packets, 1565416704 bytes

Class-map (qos): C_QOS3 (match any)
 match dscp 16-23
 match cos 2
 set qos-group 3
      matched      : 5412521 packets, 346401344 bytes
      transmitted  : 5412521 packets, 346401344 bytes

Class-map (qos): C_QOS4 (match any)
 match dscp 24-31
 match cos 3
 set qos-group 4
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS5 (match any)
 match dscp 32-39
 match cos 4
 set qos-group 5
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS6 (match any)
 match dscp 40-47
 match cos 5
 set qos-group 6
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS7 (match any)
```

```
 match dscp 48-55
 match cos 6
 set qos-group 7
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS8 (match any)
 match dscp 56-63
 match cos 7
 set qos-group 8
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes


Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 1 packets, 64 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
Class-map (queuing): q7
 priority level 1
      output       : 2412 packets, 154568 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 4 packets, 272 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets


#show policy-map interface xe3

Interface xe3
Global statistics status : enabled
```

```
Service-policy (queuing) output: Pend
-----------------------------------
Class-map (queuing): empty5
 shape average 400 mbps
 wrr-queue weight 1
 bandwidth 350 mbps

     Service-policy (queuing) output: P1P1
     -----------------------------------
     Class-map (queuing): cq1
      match qos-group 1
      shape percent 20
 wrr-queue weight 1
      queue-limit 70 packets
      bandwidth percent 18
           output       : 1 packets, 64 bytes
           dropped      : 0 packets, 0 bytes

     Class-map (queuing): cq2
      match qos-group 2
      shape percent 80
 wrr-queue weight 1
      queue-limit 70 packets
      bandwidth percent 75
           output       : 10871860 packets, 695799040 bytes
           dropped      : 13598654 packets, 870313856 bytes

Class-map (queuing): empty6
 shape average 500 mbps
 wrr-queue weight 1
 bandwidth 450 mbps

     Service-policy (queuing) output: P3P4
     -----------------------------------
     Class-map (queuing): empty3
      shape percent 40
 wrr-queue weight 1
      bandwidth percent 35

          Service-policy (queuing) output: P3
          -----------------------------------
          Class-map (queuing): cq5
           shape percent 40
 wrr-queue weight 1
           queue-limit 100 packets
           bandwidth percent 35
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

          Class-map (queuing): cq6
```


© 2021 IP Infusion Inc. Proprietary

```
           match qos-group 6
           shape percent 60
 wrr-queue weight 1
           queue-limit 100 packets
           bandwidth percent 55
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

     Class-map (queuing): empty4
      shape percent 60
 wrr-queue weight 1
      bandwidth percent 50

          Service-policy (queuing) output: P4
          -----------------------------------
          Class-map (queuing): cq7
           match qos-group 7
           shape percent 40
 wrr-queue weight 1
           random-detect minimum-threshold 80 maximum-threshold 100 packets
bytes
kbytes
percent
           bandwidth percent 35
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

          Class-map (queuing): cq8
           match qos-group 8
           shape percent 60
 wrr-queue weight 1
           random-detect minimum-threshold 80 maximum-threshold 100 packets
bytes
kbytes
percent
           bandwidth percent 55
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```

```
Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 2410 packets, 154500 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 13 packets, 884 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 13598643 packets
 yellow : 0 packets
 red    : 0 packets


(config)#set qos sp
(config)#exit


#show policy-map interface xe2

Interface xe2
Global statistics status : enabled

Service-policy (qos) input     : pmap1
--------------------------------
Class-map (qos): C_QOS1 (match any)
 match dscp 0-7
 match cos 0
 set qos-group 1
      matched      : 2 packets, 128 bytes
      transmitted  : 2 packets, 128 bytes

Class-map (qos): C_QOS2 (match any)
 match dscp 8-15
 match cos 1
 set qos-group 2
      matched      : 24622849 packets, 1575862336 bytes
      transmitted  : 24622849 packets, 1575862336 bytes

Class-map (qos): C_QOS3 (match any)
 match dscp 16-23
 match cos 2
 set qos-group 3
      matched      : 5412521 packets, 346401344 bytes
```

```
      transmitted  : 5412521 packets, 346401344 bytes

Class-map (qos): C_QOS4 (match any)
 match dscp 24-31
 match cos 3
 set qos-group 4
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS5 (match any)
 match dscp 32-39
 match cos 4
 set qos-group 5
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS6 (match any)
 match dscp 40-47
 match cos 5
 set qos-group 6
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS7 (match any)
 match dscp 48-55
 match cos 6
 set qos-group 7
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes

Class-map (qos): C_QOS8 (match any)
 match dscp 56-63
 match cos 7
 set qos-group 8
      matched      : 0 packets, 0 bytes
      transmitted  : 0 packets, 0 bytes


Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 1 packets, 64 bytes
      dropped      : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 2493 packets, 159752 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 4 packets, 272 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets


#show policy-map interface xe3

Interface xe3
Global statistics status : enabled

Service-policy (queuing) output: Pend
-----------------------------------
Class-map (queuing): empty5
 shape average 400 mbps
 wrr-queue weight 1
 bandwidth 350 mbps

     Service-policy (queuing) output: P1P1
     ----------------------------------
     Class-map (queuing): cq1
      match qos-group 1
      shape percent 20
 wrr-queue weight 1
      queue-limit 70 packets
      bandwidth percent 18
           output       : 1 packets, 64 bytes
           dropped      : 0 packets, 0 bytes

     Class-map (queuing): cq2
      match qos-group 2
      shape percent 80
 wrr-queue weight 1
      queue-limit 70 packets
      bandwidth percent 75
           output       : 10871860 packets, 695799040 bytes
           dropped      : 13743831 packets, 879605184 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
Class-map (queuing): empty6
 shape average 500 mbps
 wrr-queue weight 1
 bandwidth 450 mbps

     Service-policy (queuing) output: P3P4
     -------------------------------------
     Class-map (queuing): empty3
      shape percent 40
 wrr-queue weight 1
      bandwidth percent 35

          Service-policy (queuing) output: P3
          -----------------------------------
          Class-map (queuing): cq5
           shape percent 40
 wrr-queue weight 1
           queue-limit 100 packets
           bandwidth percent 35
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

          Class-map (queuing): cq6
           match qos-group 6
           shape percent 60
 wrr-queue weight 1
           queue-limit 100 packets
           bandwidth percent 55
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

     Class-map (queuing): empty4
      shape percent 60
 wrr-queue weight 1
      bandwidth percent 50

          Service-policy (queuing) output: P4
          -----------------------------------
          Class-map (queuing): cq7
           match qos-group 7
           shape percent 40
 wrr-queue weight 1
           random-detect minimum-threshold 80 maximum-threshold 100 packets
bytes
kbytes
percent
           bandwidth percent 35
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes
```

```
          Class-map (queuing): cq8
           match qos-group 8
           shape percent 60
 wrr-queue weight 1
           random-detect minimum-threshold 80 maximum-threshold 100 packets
bytes
kbytes
percent
           bandwidth percent 55
                output       : 0 packets, 0 bytes
                dropped      : 0 packets, 0 bytes

Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
Class-map (queuing): q7
 priority level 1
      output       : 2488 packets, 159492 bytes
      dropped      : 3 packets, 192 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 13 packets, 884 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 13743818 packets
 yellow : 0 packets
 red    : 0 packets
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 17 VXLAN Quality of Service

For VXLAN Quality-of-Service configuration procedures, see the Virtual eXtensible Local Area Network Configuration Guide.

© 2021 IP Infusion Inc. Proprietary

CHAPTER 18 FP Rules Queuing Configuration

This chapter contains basic information about cpu-queue properties and complete sample configuration for cpu-queue properties.

DUT has many CPU queues for management/classification of control traffic and provides rate limiters for control plane protection. Different types of CPU port bound packets are queued in different cpu-queues each with different properties like rate, queue-limit, monitoring status and drop status.

Topology



Figure 18-67: Simple configuration of CPU Queuing

Default Values

```
R1#show cpu-queue details
* - Can not configure the parameter
Cpu queue       Rate In PPS             Lossy Status           Monitor Status
Name      Configured  Default     Configured  Default     Configured  Default
========= ==========  =======     ==========  ==========  ==========
===========
sflow          -       32000          -       *lossy          -        monitor
bgp            -       1500           -        lossless       -        monitor
vrrp           -       500            -        lossless       -        monitor
ldp-rsvp       -       500            -        lossless       -        monitor
rip            -       500            -        lossless       -        monitor
ospf           -       2000           -        lossless       -        monitor
dhcp           -       100            -        lossy          -        no-
monitor
nd             -       6000           -        lossless       -        monitor
mpls           -       500            -        lossy          -        no-
monitor
pim            -       4000           -       *lossy          -       *no-
monitor
arp            -       6000           -        lossless       -        monitor
igmp           -       4000           -       *lossy          -       *no-
monitor
bpdu           -       10000          -        lossless       -        monitor
ccm            -       500            -        lossy          -        no-
monitor
bfd            -       2000           -        lossy          -        no-
monitor
ptp            -       1000           -        lossy          -        no-
monitor
isis           -       500            -        lossless       -        monitor
trill-isis     -       1000           -        lossless       -        monitor
acl            -       200            -       *lossy          -       *no-
monitor
vxlan          -       500            -        lossy          -        monitor
```

Note: Enable feature before validating cpu-queue for that protocol.

Monitor option will generate operational log, if it reaches above 90%. Log generation will stop, when it goes below 90%.

1. 2001 Jan 07 22:29:03.345 : R1 : HSL : NOTIF : [CPU_RATE_HIGH_4]: Average CPU queue rate for bpdu is 90% (540 pkts/sec).
2. 2001 Jan 07 22:29:08.346 : R1 : HSL : NOTIF : [CPU_QUEUE_RECOVERED_4]: CPU queue rate for bpdu is back to normal. Current average rate is 89%.

Lossless option will drop the traffic at ingress interface. We can use "show interface counters indiscard-stats" to verify the drop. Packets will be incremented in IBP Discards column.

Lossy option will drop the traffic at cpu. We can use “show interface cpu counters queue-stats`” to verify the drop.

“disable l3-protocols-cpu vxlan” command is used, when sending traffic to vxlan interface. In Vxlan, arp and nd traffic will go to vxlan queue. Remaining traffics are considered as data traffic.

Configuring CPU Queuing Lossless

Do the following to configure CPU queuing on an interface.

`#configure terminal`	
`(config)#bridge 1 protocol rstp`	Configure Bridge 1
`(config)#int xe52/2`	
`(config)#switchport`	Configure interface as L2
`(config-cmap-qos)#bridge-group 1`	Configure bridge 1 in interface
`(config-cmap-qos)#int xe52/3`	
`(config-cmap-qos)#switchport`	Configure interface as L2
`(config)#bridge-group 1`	Configure bridge 1 in interface
`(config-cmap-qos)#exit`	
`(config)#cpu-queue bpdu rate 600 lossless no-monitor`	Configure bpdu cpu-queue with rate of 600 pps and lossless and no-monitor option

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
R1(config)#do show running-config | inc cpu
cpu-queue bpdu rate 600 lossless no-monitor
R1(config)#
R1(config)#do show cpu-queue details
* - Can not configure the parameter
Cpu queue       Rate In PPS             Lossy Status            Monitor Status
Name      Configured  Default     Configured  Default     Configured  Default
========= ==========  =======     ==========  ==========  ==========
===========
sflow         -       32000           -       *lossy          -        monitor
bgp           -       1500            -        lossless       -        monitor
```

 © 2021 IP Infusion Inc. Proprietary

```
vrrp            -       500             -       lossless        -       monitor
ldp-rsvp        -       500             -       lossless        -       monitor
rip             -       500             -       lossless        -       monitor
ospf            -       2000            -       lossless        -       monitor
dhcp            -       100             -       lossy           -       no-
monitor
nd              -       6000            -       lossless        -       monitor
mpls            -       500             -       lossy           -       no-
monitor
pim             -       4000            -      *lossy           -      *no-
monitor
arp             -       6000            -       lossless        -       monitor
igmp            -       4000            -      *lossy           -      *no-
monitor
bpdu      600           10000       lossless    lossless   no-monitor   monitor
ccm             -       500             -       lossy           -       no-
monitor
bfd             -       2000            -       lossy           -       no-
monitor
ptp             -       1000            -       lossy           -       no-
monitor
isis            -       500             -       lossless        -       monitor
trill-isis      -       1000            -       lossless        -       monitor
acl             -       200             -      *lossy           -      *no-
monitor
vxlan           -       500             -       lossy           -       monitor
R1(config)#do clear interface cpu counters
R1(config)#do clear interface counters

R1(config)#do show interface counters rate
+------------------+-------------+------------+-------------+------------
+
|     Interface    |    Rx bps   |    Rx pps  |    Tx bps   |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 po1                436           0            2980          5
 po2                768714        1372         769045        1373
 xe52/1             0             0            44            0
 xe52/2             0             0            263           0
 xe52/3             669424827     99971        263           0
 xe53/1             33            0            788           1
 xe53/2             33            0            719           1
 xe53/3             336           0            702           1
 xe53/4             33            0            769           1
 xe54/1             192176        343          192014        342
 xe54/2             192166        343          192292        343
 xe54/3             192150        343          192348        343
 xe54/4             192204        343          192390        343
R1(config)#do show interface cpu counters rate
Load interval: 30 second
+------------------+-------------+------------+-------------+------------
+
|    CPU Queue(%)  |    Rx bps   |    Rx pps  |    Tx bps   |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 hw-bfd       ( N/A) -             -            101679        1374
 bpdu         (100%) -             -            436856        600
```

```
 ospf          (  0%) -              -             84             0
 bgp           (  0%) -              -             44             0
R1(config)#do show interface cpu counters rate
Load interval: 30 second
+------------------+-------------+------------+-------------+------------
+
|    CPU Queue(%)   |    Rx bps    |    Rx pps   |    Tx bps    |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 hw-bfd        ( N/A) -              -             101574         1372
 bpdu          ( 99%) -              -             433465         599
 ospf          (  0%) -              -             39             0
 bgp           (  0%) -              -             44             0

R1(config)#do show interface cpu counters queue-sta
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+----------------+------------------+---------
--------+--------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts     |     Tx bytes      |  Dropped
pkts   |   Dropped bytes   |
+--------------------+--------+----------------+------------------+---------
--------+--------------------+
hw-bfd           (E) 0       130582           9663068           0
0
bpdu            (E) 2706080  57086            41576707          0
0
arp             (E) 0       2                136               0
0
ospf            (E) 0       35               4658              0
0
bgp             (E) 0       95               7030              0
0


R1(config)#do show interface counters indiscard-stats
+-------------+-----------------+--------------+--------------+-----------
-----+-----------------+-------------+--------------------+
|  Interface  | Port Block Drops | Vlan Discards | ACL/QOS Drops | Policy
Discards | EGR Port Unavail | IBP Discards |   Total Discards   |
+-------------+-----------------+--------------+--------------+-----------
-----+-----------------+-------------+--------------------+
 xe52/3       0                0              0              0
0                 13080579       13080579

Configuring cpu-queue with lossy
============================
```

Configuring CPU Queuing Lossy

Do the following to configure CPU queuing on an interface.

`#configure terminal`	
`R1(config)#cpu-queue  bpdu rate 500 lossy no-monitor`	Configure bpdu cpu-queue with rate of 500 pps and lossy and no-monitor option
`R1(config-if)#exit`	

© 2021 IP Infusion Inc. Proprietary

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
R1(config)#do clear interface cpu counters
R1(config)#do clear interface  counters
R1(config)#do show running-config | inc cpu
cpu-queue bpdu rate 500 lossy no-monitor
disable l3-protocols-cpu vxlan
R1(config)#do show cpu-queue details
* - Can not configure the parameter
Cpu queue       Rate In PPS             Lossy Status            Monitor Status
Name      Configured  Default     Configured  Default     Configured  Default
========= ==========  =======     ==========  ==========  ==========
===========
sflow         -       32000           -       *lossy          -        monitor
bgp           -       1500            -        lossless       -        monitor
vrrp          -       500             -        lossless       -        monitor
ldp-rsvp      -       500             -        lossless       -        monitor
rip           -       500             -        lossless       -        monitor
ospf          -       2000            -        lossless       -        monitor
dhcp          -       100             -        lossy          -        no-
monitor
nd            -       6000            -        lossless       -        monitor
mpls          -       500             -        lossy          -        no-
monitor
pim           -       4000            -       *lossy          -       *no-
monitor
arp           -       6000            -        lossless       -        monitor
igmp          -       4000            -       *lossy          -       *no-
monitor
bpdu      500         10000       lossy        lossless   no-monitor   monitor
ccm           -       500             -        lossy          -        no-
monitor
bfd           -       2000            -        lossy          -        no-
monitor
ptp           -       1000            -        lossy          -        no-
monitor
isis          -       500             -        lossless       -        monitor
trill-isis    -       1000            -        lossless       -        monitor
acl           -       200             -       *lossy          -       *no-
monitor
vxlan         -       500             -        lossy          -        monitor
R1(config)#do show interface counters rate
+------------------+-------------+------------+-------------+------------
+
|     Interface    |    Rx bps   |    Rx pps  |    Tx bps   |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 po1                780           0            2974          5
 po2                769353        1373         769260        1373
 xe52/1             0             0            11            0
 xe52/2             0             0            248           0
 xe52/3             669564071     100000       248           0
```

```
 xe53/1              98             0             871            1
 xe53/2              98             0             692            1
 xe53/3              485            0             699            1
 xe53/4              98             0             710            1
 xe54/1              192647         343           192322         343
 xe54/2              191965         342           192280         343
 xe54/3              192466         343           192278         343
 xe54/4              192295         343           192416         343
R1(config)#do show interface cpu counters rate
Load interval: 30 second
+------------------+-------------+------------+-------------+------------
+
|    CPU Queue(%)   |    Rx bps    |    Rx pps   |    Tx bps    |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 hw-bfd       ( N/A) -              -             101505         1371
 bpdu         ( 99%) -              -             345547         499
 ospf         (  0%) -              -             74             0
 bgp          (  0%) -              -             44             0
R1(config)#do show interface cpu counters rate
Load interval: 30 second
+------------------+-------------+------------+-------------+------------
+
|    CPU Queue(%)   |    Rx bps    |    Rx pps   |    Tx bps    |    Tx pps
|
+------------------+-------------+------------+-------------+------------
+
 hw-bfd       ( N/A) -              -             101505         1371
 bpdu         ( 99%) -              -             345547         499
 ospf         (  0%) -              -             74             0
 bgp          (  0%) -              -             44             0
R1(config)#do show cpu-queue details
cpu-queue bpdu rate 500 lossy no-monitor
disable l3-protocols-cpu vxlan
R1(config)#
R1(config)#
R1(config)#do show interface cpu counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+-----------------+-------------------+---------
--------+--------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts     |     Tx bytes      |  Dropped
pkts   |   Dropped bytes   |
+--------------------+--------+-----------------+-------------------+---------
--------+--------------------+
hw-bfd           (E) 0       78216           5787984           0
0
bpdu            (E) 978848   39290           27124511          7818876
6550244016
arp              (E) 0       2               136               0
0
ospf             (E) 0       21              3070              0
0
bgp              (E) 0       55              4070              0
0

R1(config)#do show interface counters indiscard-stats
+-------------+-----------------+--------------+--------------+-----------
-----+-----------------+--------------+--------------------+
```


© 2021 IP Infusion Inc. Proprietary

```
|  Interface  | Port Block Drops | Vlan Discards | ACL/QOS Drops | Policy
Discards | EGR Port Unavail | IBP Discards |   Total Discards   |
+-------------+------------------+---------------+---------------+------------
-----+------------------+--------------+--------------------+
 xe53/3        4                  0               0               0
4                    0              4
 xe54/1        3                  0               0               0
3                    0              3
 xe54/2        2                  0               0               0
2                    0              2
 xe54/3        1                  0               0               0
1                    0              1
 xe54/4        3                  0               0               0
3                    0              3
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 19 Explicit Congestion Notification (ECN) Configuration

Explicit congestion notification (ECN) enables end-to-end congestion notification between two endpoints on TCP/IP based networks. The two endpoints are an ECN-enabled sender and an ECN-enabled receiver. ECN must be enabled on both endpoints and on all of the intermediate devices between the endpoints for ECN to work properly. Any device in the transmission path that does not support ECN breaks the end-to-end ECN functionality.

WRED drops packets, based on the average queue length exceeding a specific threshold value, to indicate congestion. ECN is an extension to WRED in that ECN marks packets instead of dropping them when the average queue length exceeds a specific threshold value. When configured with the WRED -- Explicit Congestion Notification feature, routers and end hosts would use this marking as a signal that the network is congested and slow down sending packets.

ECN requires an ECN-specific field that has two bits--the ECN-capable Transport (ECT) bit and the CE (Congestion Experienced) bit--in the IP header. The ECT bit and the CE bit can be used to make four ECN field combinations of 00 to 11. The first number is the ECT bit and the second number is the CE bit. The table below lists each of the ECT and CE bit combination settings in the ECN field and what the combinations indicate.

Table 19-233 explains the output fields.

Table 19-233: show bfd fields

ECT Bit	CE Bit	Combination Indicates
0	0	Not- ECN capable
0	1	Endpoints of the transport protocol are ECN capable
1	0	Endpoints of the transport protocol
1	1	Congestion experienced

The ECN field combination 00 indicates that a packet is not using ECN. The ECN field combinations of 01 and 10 called as ECT(1) and ECT(0) respectively. This sets by the data sender to indicate that the endpoints of the transport protocol are ECN-capable. Routers treat those two field combinations identically. Data senders can use either one or both of these two combinations.

ECN is Enabled

If the number of packets in the queue is below the minimum threshold, packets are transmitted. This happens whether or not ECN is enabled, and this treatment is identical to the treatment a packet receives when WRED only is being used on the network.

If the number of packets in the queue is between the minimum threshold and the maximum threshold, one of the following three scenarios can occur:

If the ECN field on the packet indicates that the endpoints are ECN-capable (that is, the ECT bit is set to 1 and the CE bit is set to 0, or the ECT bit is set to 0 and the CE bit is set to 1)--and the WRED algorithm determines that the packet should have been dropped based on the drop probability--the ECT and CE bits for the packet are changed to 1, and the packet is transmitted. This happens because ECN is enabled and the packet gets marked instead of dropped.

If the ECN field on the packet indicates that neither endpoint is ECN-capable (that is, the ECT bit is set to 0 and the CE bit is set to 0), the packet might be dropped based on the WRED drop probability. This is the identical treatment that a packet receives when WRED is enabled without ECN configured on the router.

If the ECN field on the packet indicates that the network is experiencing congestion (that is, both the ECT bit and the CE bit are set to 1), the packet is transmitted. No further marking is required.

If the number of packets in the queue is above the maximum threshold, packets are dropped based on the drop probability. This is the identical treatment a packet receives when WRED is enabled without ECN configured on the router.

Topology



Figure 19-68: Simple configuration of ECN

Configuring ECN on L3 Interface

Do the following to configure ECN on anL3 interface.

`#configure terminal`	Enter inside configure mode
`(config)#qos enable`	Enable QoS on configuration mode.
`(config)#qos statisticsEnable`	QoS statistics on configuration mode.
`(config)#class-map match-any cmap`	Enter Class-map mode
`(cmap-qos-match-any-mode)#match precedence 3`	Configure match criteria as precedence with Value 3
`(config-pmap-qos)#policy-map pmap`	Enter policy-map mode
`(config-pmap-qos)#class cmap`	Assign Class cmap to Policy-map pmap
`(cmap-qos-match-any-mode)#match precedence 3`	Configure match criteria as precedence with Value 3
`(config-pmap-qos)#policy-map pmap`	Enter policy-map mode
`(config-pmap-qos)#class cmap`	Assign Class cmap to Policy-map pmap
`(config-pmap-c-qos)# police cir 328 mbps pir 556 mbps conform transmit exceed transmit violate transmit`	Police Precedence 3 frames @ Committed information rate of 328 mbps and pir 556 mbps conform transmit exceed transmit violate transmit.
`(config-pmap-c-qos)#end`	Exit out of policy-class-map mode
`#configure terminal`	Enter inside configure mode
`(config)#interface xe29`	Enter interface mode
`(config-if)#service-policy type qos input pmap`	Assign service-policy to interface on in-direction
`(config-if)#exit`	Exit interface mode
`(config)#policy-map type queuing default xyz`	Enter policy-map queuing mode
`(config-pmap-que-def)#class type queuing default q3`	Enter class-map type queuing
`(config-pmap-c-que-def)#shape percent 80`	Configure shape percent 80 in q3

© 2021 IP Infusion Inc. Proprietary

`(config-pmap-c-que-def)# random-detect minimum-threshold 100 maximum-threshold 200 packets ecn`	Configure ECN with Random Early Detection which includes minimum and maximum threshold in packets
`#configure terminal`	Enter configure mode
`(config)#interface xe30`	Enter interface mode
`(config-if)#service-policy type queuing output xyz`	Attach policy on egress interface
`OcNOS(config-if)#exit`	Exit configure mode

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
OcNOS#show policy-map interface xe30
Interface xe30
Global statistics status : enabled
Service-policy (queuing) output: xyz
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q3
 shape percent 80
 priority level 1
 random-detect minimum-threshold 100 maximum-threshold 200 packets ecn
      output       : 44808 packets, 67210500 bytes
      dropped      : 10516 packets, 15774000 bytes
Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q7
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Wred Drop Statistics:
green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

Topology



Figure 19-69: Simple configuration of ECN

Configuring ECN on L2 Interface

Do the following to configure ECN on anL2 interface.

`#configure terminal`	Enter inside configure mode
`(config)#bridge 1 protocol mstp`	Configure bridge 1 as MSTP aware
`(config)#interface xe29`	Enter interface mode
`(config-if)#switchport`	Configure xe29 as a layer 2 port
`(config-if)#bridge-group 1`	Associate bridge to an interface
`(config-if)#switchport mode trunk`	Configure port as trunk
`(config-if)#switchport trunk allowed vlan all`	Allow all the vlan on the interface xe29
`(config-if)#exit`	Exit the xe29 interface mode
`(config)#interface xe30`	Enter interface mode

© 2021 IP Infusion Inc. Proprietary

(config-if)#switchport	Configure xe30 as a layer 2 port
(config-if)#bridge-group 1	Associate bridge to an interface
(config-if)#switchport mode trunk	Configure port as trunk
(config-if)#switchport trunk allowed vlan all	Allow all the vlan on the interface xe30
(config-if)#exit	Exit the xe30 interface mode
(config)#qos enable	Enable QoS on configuration mode
(config)#qos statistics	Enable QoS statistics on configuration mode
(config)#class-map match-any cmap	Enter Class-map mode
(cmap-qos-match-any-mode)#match precedence 3	Configure match criteria as precedence with Value 3
(config-pmap-qos)#policy-map pmap	Enter policy-map mode
(config-pmap-qos)#class cmap	Assign Class cmap to Policy-map pmap
(config-pmap-c-qos)# police cir 328 mbps pir 556 mbps conform transmit exceed transmit violate transmit	Police Precedence 3 frames @ Committed information rate of 328 mbps and pir 556 mbps conform transmit exceed transmit violate transmit.
(config-pmap-c-qos)#end	Exit out of policy-class-map mode
#configure terminal	Enter inside configure mode
(config)#interface xe29	Enter interface mode
(config-if)#trust dscp	Configure trust DSCP on the interface xe29
(config-if)#service-policy type qos input pmap	Assign service-policy to interface on in-direction
(config-if)#exit	Exit interface mode
(config)#policy-map type queuing default xyz	Enter policy-map queuing mode
(config-pmap-que-def)#class type queuing default q3	Enter class-map type queuing
(config-pmap-c-que-def)#shape average 900 mbps	Configure shape average 900 in q3
(config-pmap-c-que-def)#random-detect green 1000 2000 yellow 3000 4000 red 5000 6000 bytes ecn	Configure ECN with Random Early Detection which includes minimum and maximum threshold for green, yellow and red packets
(config-pmap-c-que-def)#end	Exit pmap mode
#configure terminal	Enter configure mode
(config)#interface xe30	Enter interface mode
(config-if)#service-policy type queuing output xyz	Attach policy on egress interface
OcNOS(config-if)#exit	Exit configure mode

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
 OcNOS#show policy-map interface xe30
Interface xe30
Global statistics status : enabled
Service-policy (queuing) output: xyz
---------------------------------
Class-map (queuing): q0
```

```
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q3
 shape average 900 mbps
 priority level 1
 random-detect green minimum-threshold 1000 maximum-threshold 2000 yellow
minimu
m-threshold 3000 maximum-threshold 4000 red minimum-threshold 5000 maximum-
thres
hold 6000 bytes ecn
      output       : 308318 packets, 462477000 bytes
      dropped      : 29774 packets, 44661000 bytes
Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): q7
 priority level 1
      output       : 3 packets, 369 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q6
```


© 2021 IP Infusion Inc. Proprietary

```
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Class-map (queuing): mc-q7
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes
Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 20 Rate Limiting BUM Traffic

To prevent the CPU from getting flooded with Broadcast, Unknown Unicast, and Multicast (BUM) traffic, rate limiting can be applied at the ingress interface. This configuration is called “storm control” and is independent of the QoS feature, and can be configured directly on the interface in the ingress direction.

Configuring per port rate limiting for BUM traffic

BUM rate limiting can be configured on the interface via following command:

```
storm-control (broadcast|multicast|dlf) (level LEVEL | <0-1000000000> (kbps|mbps|gbps))
(burst-size <32-128000>|)
```

The `broadcast` option is for broadcast traffic, `multicast` option is for multicast traffic and `dlf` (Destination Lookup Failure) option is for unknown unicast traffic.

There are two ways to configure the rate limiting information. One is in percentage and the other is in absolute values. Use the level option to configure in percentage format where the link speed is used for rate calculation. Percentage value can be configured with up to four fractional digits in order to support kbps level rate limiting on 100 gbps ports, and the Absolute configuration option uses the input rate in kbps, mbps, or gbps.

Burst-size is an optional parameter, if storm control is not configured with burst-size, default value is calculated as 5ms of configured rate to limit the traffic. Minimum of 32 Kbps burst will be allocated if the calculated value is below 32 Kbps.

An example of BUM rate limiting is shown below:

```
(config)#interface xe1
(config-if)#switchport
(config-if)#storm-control dlf 2 mbps
(config-if)#exit
```

In the configuration above, unknown unicast traffic received on `xe1` will be rate limited to 1.98 mbps. Burst-size is calculated as 32 Kbps.

Note: Minimum granularity for storm-control is 64kbps.

Note: Burst-range in XGS is 32-128000 Kbps.

Storm Detection Time

Rate-limit setting should take place immediately after detecting storm. With existing burst size, rate limit is happening after few seconds, if burst size should be changed to a lower value so that rate-limiting happens immediately on the switch. Also, user have a provision to change burst size through CLI.

An example of BUM rate limiting with Burst-size configuration is shown below:

```
(config)#interface xe1
(config-if)#switchport
(config-if)#storm-control broadcast 600 kbps burst-size 15
(config-if)#exit
```

In the configuration above, broadcast traffic received on xe1 will be rate limited to 576 kbps and Burst-size is configured as 40 Kbps. If traffic sent at 700 kbps. Time taken to detect the storm should be 0.32 Seconds.

© 2021 IP Infusion Inc. Proprietary

Storm Control Notifications

When storm control occurs in switch, there is no direct way for the user to identify the storm apart from discard counters with "show storm-control" CLI. So SNMP trap and syslog notifications are generated for the user to know about the storm control.

If storm-control occurs, based on the rate-limit discard counters, a Syslog notification and SNMP trap is generated. As the rate-limit packet discards stops, another syslog notification and SNMP trap is generated that storm packet discards are stopped.

Displaying BUM rate limit information

Use the following command to verify BUM rate limit configuration:

```
show storm-control (INTERFACE-NAME|)
```

```
show storm-control
*The hardware applicable value is displayed
Port          BcastLevel(burst)               McastLevel(burst)               DlfLevel(burst)               Discards
xe1         576.000 kbps(40 Kbps)           100.0000%(0 Kbps)               1.984 mbps(32 Kbps)             125411

2021 Sep 23 19:51:09.639 : OcNOS : HSL : NOTIF : [IF_STORM_DISCARDS_4]: Storm control discards started on interface xe1 total
discards 364173

2021 Sep 23 19:52:45.740 : OcNOS : HSL : NOTIF : [IF_STORM_DISCARDS_4]: Storm control discards stopped on interface xe1 total
discards 1272806
```


© 2021 IP Infusion Inc. Proprietary

Quality of Service Command Reference

Contents

This document contains this chapter:

- Chapter 1, *Quality of Service Commands*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Quality of Service Commands

This chapter is a reference for the ingress Quality of Service (QoS) and hierarchical QoS.

- bandwidth
- class-map type qos
- class-map type queuing
- class type qos
- class type queuing
- clear qos statistics
- cpu-queue
- egress cos map
- egress dscp map
- ingress cos map
- ingress dscp map
- ingress exp map
- match access-group
- match cos
- match cos inner
- match dscp
- match ip rtp
- match mac
- match precedence
- match protocol
- match qos-group
- match traffic-type
- match vlan
- match vlan inner
- police
- policy-map
- priority
- priority (queuing)
- qos (enable | disable)
- qos map-profile
- qos profile
- qos profile precedence-to-queue
- qos profile queue-to-precedence
- qos remark
- qos statistics

© 2021 IP Infusion Inc. Proprietary

- queue-limit
- random-detect
- service-policy
- service-policy type qos
- service-policy type queuing
- set bridge cos
- set bridge dscp
- set cos
- set dscp
- set mpls class
- set precedence
- set qos-group
- set qos queue scheduler
- set queue
- shape
- shape rate
- show class-map
- show cpu-queue details
- show policy-map
- show policy-map interface
- show qos-profile
- show qos-profile interface
- show queuing interface
- show running-config qos
- show running-config cpu-queue
- storm-control
- trust dscp
- wrr-queue weight

© 2021 IP Infusion Inc. Proprietary

bandwidth

Use this command to allocate a minimum percentage of the interface bandwidth to a queue.

Use the `no` command to remove a bandwidth configuration.

Command Syntax

```
bandwidth (<1-1000000000> (kbps|mbps|gbps) | percent <1-100>)
no bandwidth
```

Parameters

`<1-1000000000>`	Bandwidth value
`kbps`	Units in kilobits/sec.
`mbps`	Units in megabits/sec.
`gbps`	Units in gigabits/sec.
`percent`	Specify the percentage from 1 to 100.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map type queuing PQOS
(config-pmap-que)# class type queuing 1p7q4t-out-pq1
(config-pmap-c-que)# bandwidth 10 mbps
```

class-map type qos

Use this command to create a class-map of type qos.

Use the `no` command to remove a class-map.

Note: Class-map without any match qualification behaves similar to default class by matching all the packets on the interface it is attached via service policy.

In a class-map, adding or deleting match criteria with misconfiguration will have silent exit and will not proceed with operation.

Command Syntax

```
class-map (type qos|) (match-any|match-all|) NAME
no class-map (type qos|) (match-any|match-all|) NAME
```

Parameters

`NAME`	Specify the class map name (Max Size 32)
`match-any`	Match any parameter (boolean OR)
`match-all`	Match all parameters (boolean AND)

Default

By default, match type is match-all for any class-map

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)# class-map type qos C_QOS1
```


© 2021 IP Infusion Inc. Proprietary

class-map type queuing

Use this command to create a class-map of type queuing.

Use the `no` command to remove a class-map.

Note: Class-maps with no action are treated as incomplete configuration and don't take any effect until the action is added. Class-map deletion is not allowed if it is referenced by any policy-map.

Command Syntax

```
class-map type queuing (match-any|) NAME
no class-map type queuing (match-any|) NAME
```

Parameters

`NAME`	Specify the class map name (Max Size 32)
`match-any`	Match any parameter (boolean OR)

Default

By default, class-map type is match-any

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
#configure terminal
(config)# class-map type queuing C_QOS1
```

class type qos

Use this command to add a QoS class-map to a qos policy map.

Use the `no command` to remove a QoS class-map from the policy map.

Note: Implicit priority of the classes in a policy-map will be calculated based on the number of matches with VLAN match given lower weight-age over other matches. In case of classes with conflicting matches, it is not guaranteed which class the traffic would hit. Users are recommended to use priority in such cases.

Command Syntax

```
class (type qos|) (NAME|class-default)
no class (type qos|) (NAME|class-default)
```

Parameters

`NAME`	Specify the class map name

Default

By default, class is type qos

Command Mode

Policy-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#
(config)#policy-map type qos PP
(config-pmap-que)#class type qos C_PP_1
```


© 2021 IP Infusion Inc. Proprietary

class type queuing

Use this command to add a queuing class-map to a queuing policy map.

Use the `no` command to remove a queuing class-map from the policy map.

Command Syntax

```
class (type queuing ((default (q0|q1|q2|q3|q4|q5|q6|q7))|NAME) | NAME | queuing
  class-default)
no class (type queuing|) NAME
```

Parameters

`NAME`	Specify the class map name
`<q0-q7>`	Default queue name

Default

No default value is specified

Command Mode

Policy Map type queuing Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#
(config)#policy-map type queuing PP
(config-pmap-que)#class type queuing C_PP_1
```

clear qos statistics

Use this command to clear the quality of service (QoS) statistics.

Command Syntax

```
clear qos statistics  (interface IFNAME|) ((type all| type qos| type qos input| type
  qos output| type queuing)|)
```

Parameters

`NAME`	Specify which interface to clear.
`type all`	Clear all statistics from QoS and Queuing types.
`type qos`	Clear all statistics from QoS type.
`type qos input`	Clear all statistics from QoS input type.
`type qos output`	Clear all statistics from QoS output type.
`type queuing`	Clear all statistics from queuing type.

Default

By default, type QoS, type queuing class statistics on all interfaces will be cleared, if no parameters configured.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear qos statistics
```


© 2021 IP Infusion Inc. Proprietary

cpu-queue

Use this command to configure create a cpu queue for vxlan.

Use the `no` form of this command to remove a cpu queue.

Command Syntax

```
cpu-queue <queue-name> ( (rate <value>|)  (lossy|lossless|)  (monitor|no-monitor|)
  )
no cpu-queue <queue-name> ( (rate|)  (lossy|lossless|)  (monitor|no-monitor) |)
```

Parameters

`queue-name`	Name of the cpu queue
`rate`	When the packets are uplifted
`lossy`	If enabled, packets are dropped at cpu-queue when the cpu-queues congested
`loseless`	If enabled, packets are dropped at ingress port
`monitor`	Enable logging when cpu-queue discards packets
`no-monitor`	Disable logging

Default

Default value for vxlan cpu-queue command is 500.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.8

Example

```
#configure terminal
(config)#cpu-queue cpu rate 500
(config-dscp-queue)#exit
```

egress cos map

Use this command to map a queue value to the CoS value.

Use the `no` form of this command to remove the map.

Note: Egress CoS map will be taking effect only when remark CoS is enabled.

Note: Color is an optional parameter. If not provided, the same map will be set for all colors.

Note: If ingress qos policy-map is configured with set cos action on ingress interface, set action will take priority over egress cos map and packet will egress out with set cos value.

Command Syntax

```
queue <0-7> (color (green|yellow|red|all)|) cos <0-7>
no queue <0-7> (color (green|yellow|red|all)|)
```

Parameters

`<0-7>`	Identifying queue number
`color`	(green|yellow|red|all)
`<0-7>`	CoS value

Default

By default, CoS to queue mapping is one to one.

Command Mode

Egress cos map mode

Applicability

This command was introduced in OcNOS DC version 4.2.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Example

```
(config)#qos profile queue-color-to-cos default
(config-egress-cos-map)#queue 1 color green cos 5
(config-egress-cos-map)#queue 1 cos 6
```

Color is an optional parameter. So if users do not provide color, for all colors same CoS remarking will be set. If user provides color, then only for that specific color egress map will be changed. If user provides map for all colors as well as without color, map with color will take priority.

```
(config-egress-cos-map)#no queue 1 color green
(config-egress-cos-map)#no queue 1
```

If user want to remove all the mapping of queue (for all colors) no need to provide color, else can provide specific color to remove specific map .

 © 2021 IP Infusion Inc. Proprietary

egress dscp map

Use this command to map a queue to a DSCP value.

Use the `no` form of this command to remove the map.

Note: Egress DSCP map will be taking effect only when remark DSCP is enabled.

Note: Color is an optional parameter. If not provided, the same map will be set for all colors.

Note: If ingress qos policy-map is configured with set dscp/precedence action on ingress interface, set action will take priority over egress dscp map and packet will egress out with set scp/precedence value.

Command Syntax

```
queue <0-7> (color (green|yellow|red|all)|) dscp <0-63>
no queue <0-7> (color (green|yellow|red|all)|)
```

Parameters

`<0-7>`	Identifying queue number
`color`	(green|yellow|red|all)
`<0-63>`	DSCP value

Default

By default, 8 DSCP values are mapped to one queue.

For example: DSCP 0-7 queue 0, DSCP 8-15 queue 1.

Command Mode

Egress dscp map mode

Applicability

This command was introduced in OcNOS DC version 4.2

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Example

```
(config)#qos profile queue-color-to-dscp default
(config-egress-dscp-map)#queue 2 color yellow dscp 40
(config-egress-dscp-map)#queue 2 dscp 36
```

If user specifies color in map then map will be set for that specific color else for all colors same map will be set.

```
(config-egress-dscp-map)#no queue 2 color yellow
(config-egress-dscp-map)#no queue 2
```

If user want to remove all the mapping of dscp (for all colors) no need to provide color, else can provide specific color to remove specific map.

© 2021 IP Infusion Inc. Proprietary

ingress cos map

Use this command to map a CoS value to the queue.

Use the `no` form of this command to remove the map.

Command Syntax

```
cos <0-7> (dei (0|1|all)|) queue <0-7> (color (green|yellow|red)|)
no cos <0-7> (dei (0|1|all)|)
```

Parameters

`<0-7>`	CoS value
`dei`	Drop Eligible Indicator (0|1|all)
`<0-7>`	Identifying queue number
`color`	(green|yellow|red)

Default

By default, CoS to queue mapping is one to one, and DEI 0 will be mapped to color "green" and DEI 1 will be mapped to color "yellow”.

Command Mode

Ingress cos map mode

Applicability

This command was introduced in OcNOS DC version 4.2.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Example

```
(config)#qos profile cos-to-queue default
(config-ingress-cos-map)#cos 1 queue 2
```


© 2021 IP Infusion Inc. Proprietary

ingress dscp map

Use this command to map a DSCP value to the queue.

Use the `no` form of this command to remove the map.

Note: Color is an optional parameter. If not provided, it will be set as the default value. Please refer the Configuration Guide for the default value table.

Command Syntax

```
dscp <0-63> queue <0-7> (color (green|yellow|red)|)
no dscp <0-63>
```

Parameters

`<0-63>`	DSCP value
`<0-7>`	Identifying queue number
`color`	(green|yellow|red)

Default

By default, 8 DSCP values are mapped to one queue.

For example: DSCP 0-7 queue 0, DSCP 8-15 queue 1.

Command Mode

Ingress dscp map mode

Applicability

This command was introduced in OcNOS DC version 4.2.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Example

```
(config)#qos profile dscp-to-queue default
(config-ingress-dscp-map)#dscp 1 queue 2
```

ingress exp map

Use this command to map a exp value to the queue.

Use the `no` form of this command to remove the map.

Note: Color is an optional parameter. If not provided, color will be set to green.

Command Syntax

```
exp <0-7> queue <0-7> (color (green|yellow|red)|)
no exp <0-7>
```

Parameters

`<0-7>`	EXP value
`<0-7>`	Identifying queue number
`color`	(green|yellow|red)

Default

By default, EXP to queue mapping is one to one.

Command Mode

Ingress exp queue map mode

Applicability

This command was introduced in OcNOS DC version 4.2.

Example

```
(config)#qos profile exp-to-queue default
(config-ingress-exp-queue-map)#exp 1 queue 4 color green
(config-ingress-exp-queue-map)#exp 2 queue 3
```


© 2021 IP Infusion Inc. Proprietary

match access-group

Use this command to classify the group based on the access group.

Use the `no command` remove access group match criteria from a class map

Command Syntax

```
match access-group NAME
no match access-group NAME
```

Parameters

`NAME`	Specify the access group name

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)# class-map class_acl
(config-cmap-qos)# match access-group my_acl
```

match cos

Use this command to classify the traffic based on cos

Use the `no command` to remove the match configuration.

Note: The match commands which accept range have silent exit which makes removal of these match configurations easier. For example, classify the traffic based on cos using the command `match cos 2,4,6` and remove the match configuration using the command `no match cos 2-6`.

Command Syntax

```
match cos WORD
no match cos
```

Parameters

`WORD`	CoS value or list of specified CoS values. Valid values are from 0 to 7.
`all`	Delete all matched cos entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match cos 1
```


© 2021 IP Infusion Inc. Proprietary

match cos inner

Use this command to classify the traffic based on inner cos.

Use the `no` command to remove the match configuration.

Note: The match commands which accept range have silent exit which makes removal of these match configurations easier. For example, classify the traffic based on inner cos using the command `match cos inner 2,4,6` and remove the match configuration using the command `no match cos inner 2-6`.

Command Syntax

```
match cos inner WORD
no match cos inner
```

Parameters

`WORD`	Inner CoS value or list of specified CoS values. Valid values are from 0 to 7.
`all`	Delete all matched cos entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match cos inner 1
```

match dscp

Use this command to classify the traffic based on dscp.

Use the `no` command to remove the configured dscp value.

Note: The match commands which accept range have silent exit which makes removal of these match configurations easier. For example, classify the traffic based on dscp using the command `match dscp 2,4,6` and remove the match configuration using the command `no match dscp 2-6`.

Command Syntax

```
match dscp [WORD | af11 | af12 | af13 | af21 | af22 | af23 | af31| af32 | af33 |
  af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6| cs7 | default | ef]
no match dscp
```

Parameters

`WORD`	<0-63> List of DSCP values.
`af11`	AF11 dscp (001010).
`af12`	AF12 dscp (001100)
`af13`	AF13 dscp (001110)
`af21`	AF21 dscp (010010)
`af22`	AF22 dscp (010100)
`af23`	AF23 dscp (010110)
`af31`	AF31 dscp (011010)
`af32`	AF32 dscp (011100)
`af33`	AF33 dscp (011110)
`af41`	AF41 dscp (100010)
`af42`	AF42 dscp (100100)
`af43`	AF43 dscp (100110)
`cs1`	CS1(precedence 1) dscp (001000)
`cs2`	CS2(precedence 2) dscp (010000)
`cs3`	CS3(precedence 3) dscp (011000)
`cs4`	CS4(precedence 4) dscp (100000)
`cs5`	CS5(precedence 5) dscp (101000)
`cs6`	CS6(precedence 6) dscp (110000)
`cs7`	CS7(precedence 7) dscp (111000)
`default`	Default dscp (000000)
`ef`	EF dscp (101110)
`all`	Delete all matched DSCP values.

Default

No default value is specified

© 2021 IP Infusion Inc. Proprietary

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#class-map type qos C_QOS7
(config-cmap-qos)#match dscp 48-55
```

match ip rtp

Use this command to configure a class map to use the Real-Time Protocol (RTP) port as a match criteria.

Use the `no command` to remove the RTP port as a match criteria.

Note: The match commands which accept range have silent exit which makes removal of these match configurations easier. For example, classify the traffic based on RTP port using the command `match ip rtp 5000,7000, 9000` and remove the match configuration using the command `no match ip rtp 5000-9000`.

Command Syntax

```
match ip rtp WORD
no match ip rtp
```

Parameters

`WORD`	Specify User Datagram Protocol (UDP) or list of UDP ports that are using RTP. Valid values are from 2000 to 65535.
`all`	Delete all matched IP RTP values.

Default

No default value is specified

Command Mode

Class-map type qos

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)# class-map my_test
(config-cmap-qos)# match ip rtp 2300
```


© 2021 IP Infusion Inc. Proprietary

match mac

Use this command to classify based on the mac address (can be source or destination or both)

Use the `no` command to remove the match configuration.

Command Syntax

```
match mac (src |dest ) (XX:XX:XX:XX:XX:XX| XX-XX-XX-XX-XX-XX |XXXX.XXXX.XXXX)
no match mac (src |dest )
```

Parameters

`mac`	Ethernet mac address
`src`	specifies the source mac
`dest`	specifies the destination mac
`XX:XX:XX:XX:XX:XX`	MAC address option 1
`XX-XX-XX-XX-XX-XX`	MAC address option 2
`XXXX.XXXX.XXXX`	MAC address option 3

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match mac src 11:22:33:44:55:66
(config-cmap-qos)#match mac dest 3344.5566.7788
```

match precedence

Use this command to traffic classification based on precedence.

Use the `no` command to remove the match configuration.

Note: The match commands which accept range have silent exit which makes removal of these match configurations easier. For example, classify the traffic based on precedence using the command `match precedence 2,4,6` and remove the match configuration using the command `no match precedence 2-6`.

Command Syntax

```
match precedence [WORD | critical | flash | flash-override | immediate | internet |
  network | priority | routine | 0-7]
no match precedence
```

Parameters

`word`	IP precedence value
`critical`	Critical precedence
`flash`	Flash precedence
`flash-override`	Flash override precedence
`immediate`	Immediate precedence
`internet`	Internetwork control precedence
`network`	Network control precedence
`priority`	Priority precedence
`routine`	Routine precedence
`all`	Delete all matched IP precedence values.
`0-7`	Valid values are in range 0-7

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)# class-map my_test
(config-cmap-qos)# match precedence 7
```


© 2021 IP Infusion Inc. Proprietary

match protocol

Use this command to classify traffic based on protocol.

Use the `no command` to remove the specified protocol as a match criteria.

Command Syntax

```
match protocol (arp | bridging |cdp | clns | clns-is |clns-es | dhcp | isis | ldp|
  netbios )
no match protocol
```

Parameters

`arp`	Address Resolution Protocol (ARP)
`bridging`	Bridging
`cdp`	Cisco Discovery Protocol (CDP)
`clns`	Connection-less Network Service (CLNS)
`clns-is`	CLNS Intermediate System
`clns-es`	CLNS end System
`dhcp`	Dynamic Host Configuration (DHCP)
`isis`	Intermediate system to intermediate system (IS-IS)
`ldp`	Label Distribution Protocol (LDP)
`netbios`	NetBIOS Extended User Interface (NetBEUI)
`all`	Delete all matched protocols.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)# class-map my_test
(config-cmap-qos)# match protocol ldp
```

match qos-group

Use this command to match a QoS group in a type queuing class map.

Use the `no` to remove a QoS match on a queue number from a type queuing class map.

Command Syntax

```
match qos-group <1-2000>
no match qos-group <1-2000>
```

Parameters

`<1-2000>`	Specify qos group value or list of qos group values specified in bytes.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to Trident II and Trident II+ platforms.

Examples

```
(config)#
(config)#class-map type queuing match-any C_PP_1
(config-cmap-que)#match qos-group 1
```


© 2021 IP Infusion Inc. Proprietary

match traffic-type

Use this command to classify based on traffic-type

Use the `no` command to remove the match configuration.

Note: Class with match traffic type default will have lower priority over class with other traffic type match.

Command Syntax

```
match traffic-type (l2-uc|l2-uc-unknown|default)
no match traffic-type (l2-uc|l2-uc-unknown|default)
```

Parameters

`Traffic-type`	type of traffic to be matched
`l2-uc`	L2 Unicast traffic
`l2-uc-unknown`	Unknown L2 Unicast traffic
`default`	All other traffic-types

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match traffic-type l2-uc
```

match vlan

Use this command to classify the traffic based on a VLAN.

Use the `no` command to remove the match configuration.

Note: The match commands which accept range have silent exit which makes removal of these match configurations easier. For example, classify the traffic based on VLAN using the command `match vlan 2,4,6` and remove the match configuration using the command `no match vlan 2-6`.

Command Syntax

```
match vlan WORD
no match vlan (WORD|all)
```

Parameters

`not`	Match all except this.
`WORD`	Enter VLAN ID <1-4094> or range of VLAN ID's separated by commas. For example, 2 or 2,4-5 or 50,51,52 or 100-120,122-130 etc.
`all`	Delete all VLAN ID entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match vlan 1
```


© 2021 IP Infusion Inc. Proprietary

match vlan inner

Use this command to classify the traffic based on the inner VLAN.

Use the `no` command to remove the match configuration.

Note: The match commands which accept range have silent exit which makes removal of these match configurations easier. For example, classify the traffic based on the inner VLAN using the command `match vlan inner 2,4,6` and remove the match configuration using the command `no match vlan inner 2-6`.

Command Syntax

```
match vlan inner WORD
no match vlan inner (WORD|all)
```

Parameters

`not`	Match all except this.
`WORD`	Enter VLAN ID <1-4094> or list of VLAN ID's separated by commas. For example, 2,4 etc.
`all`	Delete all VLAN ID entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match vlan inner 1
```

police

Use this command to configure policing of the data rates for a particular class of traffic.

Use the `no` command to remove a policing configuration.

Note: Committed Information Rate (CIR) and Peak Information Rate (PIR) can only be whole numbers.

Command Syntax

```
police (colour-blind | colour-aware |) (cir) (<1-2000000000> (kbps|mbps|gbps) |
  percent <1-100>) ((pir (<1-2000000000> (kbps|mbps|gbps) | percent <1-100>)|)(bc)
  <1-256000> (kbytes|mbytes|ms|us)|)((be)<1-256000>
  (kbytes|mbytes|ms|us)|)((conform (transmit | set-prec-transmit <0-7> | set-dscp-
  transmit <0-63> | set-cos-transmit <0-7> | set-mpls-class <0-7> )) |)((exceed
  (drop | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit | set-mpls-
  class <0-7> ))|) ((violate (drop | set-dscp-transmit <0-63> | set-cos-transmit
  <0-7> | transmit | set-mpls-class <0-7> ))|))
no police
```

Parameters

`colour-blind`	Do not police on color.
`colour-aware`	Do police on color.
`cir <1-2000000000>`	Specify Committed information rate.
`pir <1-2000000000>`	Peak information rate.
`kbps`	Specify the units of kbps per second.
`mbps`	Specify the units of mbps per second.
`gbps`	Specify the units of gbps per second.
`Percent`	Specify the rate in percent.
`bc <1-256000>`	Burst rate committed.
`be <1-256000>`	Burst rate extended.
`transmit`	Specify the action of transmitting packets.
`set-prec-transmit`	Sets the IP precedence field to the specified value and transmits the packet.
`set-dscp-transmit`	Sets the Differentiated Service Code Point (DSCP) field to the specified value and transmits the packet.
`set-cos-transmit`	Sets the class of service (CoS) field to the specified value and transmits the packet.
`set-mpls-class`	Set the mpls class filed to the give value and tx the packet

© 2021 IP Infusion Inc. Proprietary

`drop`	Specify the action of dropping packets.
`conform`	Sets the action to take when the data rate is within bounds
`exceed`	Sets the action to take when the data rate is exceeded. Default is drop.
`violate`	Sets the action to take when the data rate violates the configured rate values. The default is drop.

Default

Table 1-234: Default values

Parameter	Default
policer-type	Color-Blind
`cir`	N/A
`pir`	0
`bc`	0
`be`	0
`conform`	Transmit
`exceed`	Drop
`violate`	Drop

Command Mode

Policy-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)# policy-map type qos 2345
(config-pmap-qos)#class type qos 2345
(config-pmap-c-qos)# police cir 2 mbps pir 4 mbps bc 2 mbytes be 4 mbytes conform
transmit exceed set-cos-transmit 1 violate drop
```

Usage

Traffic policing is based on the concept of *marking* IP packets, and then *metering* the packets in relation to how they are marked. This is called the “Two Rate Three Color Marker (trTCM)” process.

The Two Rate Three Color Marker (trTCM) meters an IP packet stream, and marks its packets as either green, yellow, or red. A packet is marked RED if it exceeds the *Peak Information Rate* (PIR). Otherwise it is marked either YELLOW or GREEN depending on whether it exceeds or does not exceed the Committed Information Rate (CIR). The trTCM is useful, for example, for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

The Meter meters each packet and passes the packet and the metering result to the Marker. The Meter operates in one of two modes – Color-Blind or Color-Aware. In the Color-Blind mode, the Meter assumes that the packet stream is

uncolored.In the Color-Aware mode, the Meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either GREEN, YELLOW, or RED.

The following describes the equations used to determine the BC an BE values:

Note: CIR, PIR, BC, and BE values are all in kbits/sec.

```
=================
BC = CIR * 5 / 1000;
Range check [64kbytes-256mbytes]
if (BC / 8) < 64)
then BC = 64 * 8;
else if (BC / 8) > 256000)
then BC = 256000 * 8;
=================
```

Same calculation for BE, as well.

Note: If the PIR value is not mentioned in the configuration, then the CIR value itself is considered for BE calculation.

```
=================
BE = PIR * 5 / 1000;
Range check [64kbytes-256mbytes]
if (BE / 8) < 64)
then BE = 64 * 8;
else if (BE / 8) > 256000)
then BE = 256000 * 8;
==================
```

For example:

```
Configure: police CIR 1 mbps
Hardware: CIR = 1000kbits/sec , BC = 512kbits, BE = 512kbits

Configure: police CIR 1 mbps PIR 200 mbps
Hardware: CIR = 1000kbits/sec, BC = 512kbits, PIR = 200000kbits/sec, BE = 1000kbits
```

For additional information regarding policing, see RFC 2697 and RFC 2698.

 © 2021 IP Infusion Inc. Proprietary

policy-map

Use this command to create a policy map and enter policy-map mode.

Use the `no` command to remove a policy map.

Note: You cannot delete a policy map if it is attached to an interface.

Command Syntax

```
policy-map {NAME | (type (qos|queuing (|default)) NAME)}
no policy-map {NAME |(type (qos|queuing (|default)) NAME)}
```

Parameters

`NAME`	Policy map name (maximum 32 characters)
`qos`	QoS policy map
`queuing`	Queuing policy map

Default

No default value is specified

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#
(config)#policy-map type qos PQOS
```

priority

Use this command to set the user priority for the class attached to this policy-map.
Use the `no` parameter with this command to unset the priority value.

Note: The higher the priority number, higher the priority for the class in a policy-map. User configured priority takes effect over default priority.

Command Syntax

```
priority <1-1000>
no priority
```

Parameters

`<1-1000>`	Priority value

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#priority 20
```


© 2021 IP Infusion Inc. Proprietary

priority (queuing)

Use this command to configure a single output queuing class as the priority queue.

Note: Priority can be set only on default queues (such as queues in the default queuing policy-map).

Command Syntax

```
priority
```

Parameters

None

Default

No default value is specified. Higher priority queue will have higher priority always when set.

Command Mode

Policy map-class type queuing mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
#configure terminal
(config)#policy-map type queuing default default-out-policy
(config-pmap-que)#class type queuing default q0
(config-pmap-c-que)#priority
```

qos (enable | disable)

Use this command to globally enable or disable Quality-of-Service (QoS).

Note: Enabling or disabling QoS is a disruptive operation, stopping all traffic on ports which causes traffic loss.

Command Syntax

```
qos (enable | disable)
```

Parameters

None

Default

By default, QoS is disabled

Command Mode

Configure

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)# qos enable

(config)#qos disable
```


© 2021 IP Infusion Inc. Proprietary

qos map-profile

Use this command to attach (map) a profile to an interface.

Use the no form of this command to remove a profile.

Note: By-default, "default" profiles are attached on their supported interfaces (cos-to-queue and queue-to-cos on L2 interfaces and DSCP-to-queue and queue-color-to-DSCP on L3 interfaces).

Note: You can create and attach your own profile to supported interfaces. After removing a user-defined profiles from an interface, the "default" profile is applied.

Command Syntax

```
qos map-profile (cos-to-queue | dscp-to-queue | queue-color-to-cos | queue-color-
  to-dscp | precedence-to-queue | queue-to-precedence) NAME
no qos map-profile (cos-to-queue | dscp-to-queue | queue-color-to-cos | queue-
  color-to-dscp| precedence-to-queue | queue-to-precedence) NAME
```

Parameters

`cos-to-queue`	Profile for CoS to queue map
`dscp-to-queue`	Profile for DSCP to queue map
`queue-color-to-cos`	Profile for queue color to CoS map
`queue-color-to-dscp`	Profile for queue color to DSCP map
`precedence-to-queue`	profile for precedence to queue map
`queue-to-precedence`	profile for queue to precedence map
`NAME`	Profile map name (maximum 32 characters)

Default

By default, the default cos-to-queue-profile is applied to an L2 interface, and the default DSCP-to-queue profile is attached to an L3 interface.

Command Mode

Interface modes

Applicability

This command was introduced in OcNOS DC version 4.2.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Example

```
(config-if)#qos map-profile cos-to-queue cos-map
(config-if)#qos map-profile dscp-to-queue dscp-map
(config-if)#qos map-profile queue-color-to-cos egress-cos-map
(config-if)#qos map-profile queue-color-to-dscp q-to-dscp-map
```

qos profile

Use this command to create new profiles or to update "default" profiles.

Use the no form of this command to remove the "user-defined" profiles, or to undo custom updates in "default" profiles.

Command Syntax

```
qos profile (cos-to-queue | dscp-to-queue | queue-color-to-cos | queue-color-to-
  dscp) (NAME|default)
no qos profile (cos-to-queue | dscp-to-queue | queue-color-to-cos | queue-color-to-
  dscp) (NAME|default)
```

Parameters

`cos-to-queue`	Profile for CoS to queue map
`dscp-to-queue`	Profile for DSCP to queue map
`queue-color-to-cos`	Profile for queue color to CoS map
`queue-color-to-dscp`	Profile for queue color to DSCP map
`NAME`	Profile map name (maximum 32 characters)

Default

By default, "default" profile is created for all the profile types. These profiles can only be updated by the user neither be created nor be destroyed.

Command Mode

Configure modes

Applicability

This command was introduced in OcNOS DC version 4.2.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Example

To create a new profile:

```
(config)#qos profile cos-to-queue cos-map
(config)#qos profile dscp-to-queue dscp-map
(config)#qos profile queue-color-to-cos egress-cos-map
(config)#qos profile queue-color-to-dscp q-to-dscp-map
```

To update the "default" profile:

```
(config)#qos profile cos-to-queue default
(config)#qos profile dscp-to-queue default
(config)#qos profile queue-color-to-cos default
```


© 2021 IP Infusion Inc. Proprietary

```
(config)#qos profile queue-color-to-dscp default
```

qos profile precedence-to-queue

Use this command to set the precedence to queue profile.

Use the no form of this command delete the profile.

Use show qos-profile to show the profile detail.

Use qos map-profile to map the profile on interface.

Command Syntax

```
qos profile precedence-to-queue (NAME|)
precedence <0-7> queue <0-7>
no qos profile precedence-to-queue (NAME|)
no precedence <0-7> queue <0-7>
```

Parameters

NAME	The profile name to be created
precedence <0-7>	Precedence value
queue <0-7>	The queue value

Command Mode

Configure modes

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#configure terminal
(config)#qos profile precedence-to-queue prec-map
(config-ingress-prec-map)#precedence 1 queue 1
(config)#interface xe1
(config-if)#qos map-profile precedence-to-queue prec-map
```


© 2021 IP Infusion Inc. Proprietary

qos profile queue-to-precedence

Use this command to set the queue to precedence profile.

Use the `no` form of this command delete the profile.

Use show qos-profile to show the profile detail.

Use qos map-profile to map the profile on interface.

Command Syntax

```
qos profile queue-to-precedence (NAME|)
queue <0-7> precedence <0-7>
no qos profile queue-to-precedence (NAME|)
no queue <0-7> precedence <0-7>
```

Parameters

`NAME`	The profile name to be created
`queue <0-7>`	The queue value
`precedence <0-7>`	Precedence value

Command Mode

Configure modes

Applicability

This command was introduced in OcNOS-SP version 5.0.

Example

```
#configure terminal
(config)#qos profile queue-to-precedence egress-prec-map
(config-egress-prec-map)#queue 1 precedence 0
(config)#interface xe2
(config-if)#qos map-profile queue-to-precedence egress-prec-map
```

© 2021 IP Infusion Inc. Proprietary

qos remark

Use this command to enable remarking of the Class of service (CoS) and Differentiated Services Control Protocol (DSCP) set by the egress map.

Use the `no` command to disable remarking of the CoS and DSCP.

Command Syntax

In Config mode :

```
qos remark (cos|dei|dscp)
no qos remark (cos|dei|dscp)
```

In interface mode:

```
qos remark (cos|dei|dscp)(enable|disable)
no qos remark (cos|dei|dscp)
```

Parameters

`type`	Remarking type. For example, CoS or DEI (Drop Eligible Indicator bit) or DSCP
`(enable|disable)`	Remarking action

Default

By default, remarking is disabled.

Command Mode

Configure mode, Interface mode

Applicability

This command was introduced in OcNOS DC version 4.2.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
((config)#qos remark cos
(config)#qos remark dscp
(config-if)# qos remark cos disable
(config-if)# qos remark cos enable
(config-if)# qos remark dscp disable
```

Interface remarking will take priority over global remarking configurations.

© 2021 IP Infusion Inc. Proprietary

qos statistics

Use this command to enable Quality of Service (QoS) statistics.

Use the `no` command to disable QoS statistics

Note: Class-map statistics is cleared whenever the match or action property of the class is modified dynamically.

Command Syntax

```
qos statistics
no qos statistics
```

Parameters

None

Default

By default, QoS statistics is disabled

Command Mode

Configure Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#qos statistics
(config)#
```

queue-limit

Use this command to configure tail drop by setting queue limits on egress queues.

Use the `no command` to remove a queue limit.

Command Syntax

```
queue-limit (<1-524288>) (packets | bytes | kbytes | percent)
no queue-limit
```

Parameters

`<1-524288>`	Specify queue-limit in packets, bytes, percent or Kilobytes. Max value for bytes is 524288 Max value for kilobytes is 512 Max value for packets is 600 Max value of percent is 100

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map type queuing P1
(config-pmap-que)#class type queuing q1
(config-pmap-c-que)# queue-limit percent 50
```


© 2021 IP Infusion Inc. Proprietary

random-detect

Use this command to configure weighted random early detection (WRED).

Use the `no command` to remove a WRED configuration.

Note: Explicit Congestion Notification (ECN) ECN-WRED is independent of WRED and max queue size parameters. With ECN, queue size can be reached until default max queue size is exceeded.

Command Syntax

```
random-detect green (min-threshold|)<1-524288> (max-threshold|)<1-524288> (drop-
  probability <1-100>|) yellow (min-threshold|)<1-524288> (max-threshold|)<1-
  524288> (drop-probability <1-100>|) red (min-threshold|)<1-524288> (max-
  threshold|)<1-524288>) (drop-probability <1-100>|) (packets | bytes |
  kbytes)(ecn|)
random-detect (min-threshold|)<1-524288> (max-threshold|)<1-524288> (packets |
  bytes | kbytes) (drop-probability <1-100>|) (ecn|)
random-detect weight <0-15>
no random-detect
no random-detect weight
```

Parameters

`min-threshold`	Specify the minimum threshold. In the range of <1-524288>
`max-threshold`	Specify the maximum threshold. In the range of <1-524288>
`drop-probability`	Specify the probability of dropping. In the range <1-100>
`Packets, bytes, kbytes`	Specify the thresholds in Packets, Bytes, or Kilobytes.
`ecn`	Explicit Congestion Notification
`weight`	Specify the weight level . In the range <0-15>

Default

No default value is specified

Command Mode

Policy-class map mode

Applicability

This command was introduced before OcNOS version 1.3.

Drop-probability and weight were introduced on OcNOS DC version 4.2.

This command applies only to the Trident II, Trident II+, Trident III, Tomahawk, and Helix platforms.

Examples

```
(config)# policy-map type queuing default xyz
(config-pmap-que)#class type queuing default q1
(config-pmap-c-que)#random-detect minimum-threshold 200 maximum-threshold 512
kbytes drop-probability 50 ecn
(config-pmap-c-que)#random-detect weight 10
(config-pmap-c-que)#no random-detect
```


© 2021 IP Infusion Inc. Proprietary

service-policy

Use this command to attach a child policy onto a parent policy.

Use the `no` command detach child policy from the parent policy.

Command Syntax

```
service-policy NAME
no service-policy NAME
```

Parameters

`NAME`	Specify the policy map to attach to the parent policy.

Default

No default value is specified

Command Mode

Policy-class-map queuing mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
(config)#policy-map type queuing P1
(config-pmap-que)#class type queuing empty5b
(config-pmap-c-que)#service-policy PQOS
```

service-policy type qos

Use this command to attach a service-policy of type qos to the interface.

Use the `no` command to remove a service-policy from an interface.

Command Syntax

```
service-policy type qos (input|output) NAME
no service-policy type qos (input|output) NAME
```

Parameters

`type`	Specify whether the policy map is of type qos.
`NAME`	Specify the policy map to attach to this interface.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#int xe3
(config-if)#service-policy type qos input PQOS
```


© 2021 IP Infusion Inc. Proprietary

service-policy type queuing

Use this command to attach a service-policy of type queuing to the interface.

Use the `no` command to remove a service-policy from an interface.

Command Syntax

```
service-policy type queuing output NAME
no service-policy type queuing output NAME
```

Parameters

`type`	Specify whether the policy map is of type queuing.
`NAME`	Specify the policy map to attach to this interface.

Default

By default, default-out-policy is attached on all interface

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#int xe3
(config-if)#service-policy type queuing output PQOS
```

set bridge cos

Use this command to set the Class-of-Service (CoS) value for L2 packets only.

Use the `no` parameter with this command to unset a CoS value.

Command Syntax

```
set bridge cos (<0-7>)
no set bridge cos
```

Parameters

`<0-7>`	CoS value.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set bridge cos 2
```


© 2021 IP Infusion Inc. Proprietary

set bridge dscp

Use this command to set the DSCP value for L3 packets only.

Use the `no` parameter with this command to unset a DSCP value.

Command Syntax

```
set bridge dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|
                af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|
                cs6| cs7| default| ef )
no set bridge dscp
```

Parameters

`<0-63>`	DSCP value
`af11`	DSCP (001011) decimal value 11
`af12`	DSCP (001100) decimal value 12
`af13`	DSCP (001101) decimal value 13
`af21`	DSCP (010101) decimal value 21
`af22`	DSCP (010110) decimal value 22
`af23`	DSCP (010111) decimal value 23
`af31`	DSCP (011111) decimal value 31
`af32`	DSCP (010000) decimal value 32
`af33`	DSCP (010001) decimal value 33
`af41`	DSCP (101001) decimal value 41
`af42`	DSCP (101010) decimal value 42
`af43`	DSCP (101011) decimal value 38
`cs1`	(Precedence 1) DSCP (001000) decimal value 8
`cs2`	(Precedence 2) DSCP (010000) decimal value 16
`cs3`	(Precedence 3) DSCP (011000) ecimal value 24
`cs4`	(Precedence 4) DSCP (100000) decimal value 32
`cs5`	(Precedence 5) DSCP (101000) decimal value 40
`cs6`	(Precedence 6) DSCP (110000) decimal value 48
`cs7`	(Precedence 7) DSCP (111000) decimal value 56
`default`	DSCP (000000) decimal value 0
`ef`	DSCP (101110) decimal value 46

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set bridge dscp 25
```


© 2021 IP Infusion Inc. Proprietary

set cos

Use this command for matching traffic classes set action as change cos in the egress packet to the prescribed value.

Use the `no command` to remove the assigned value from the class.

Command Syntax

```
set cos <0-7>
no set cos
```

Parameters

`<0-7>`	Specify CoS value to assign for this class of traffic

Default

No default value is specified

Command Mode

Policy-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map my_policy1
(config-pmap-qos)# class traffic_class2
(config-pmap-c-qos)# no set cos
(config-pmap-c-qos)#
```

set dscp

Use this command for matching traffic classes set action as change DSCP in the egress packet to the prescribed value.

Use the `no` command to remove the assigned value from the class

Command Syntax

```
set dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|
              af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|
              cs6| cs7| default| ef )
no set dscp
```

Parameters

`<0-63>`	DSCP value
`af11`	DSCP (001011) decimal value 11
`af12`	DSCP (001100) decimal value 12
`af13`	DSCP (001101) decimal value 13
`af21`	DSCP (010101) decimal value 21
`af22`	DSCP (010110) decimal value 22
`af23`	DSCP (010111) decimal value 23
`af31`	DSCP (011111) decimal value 31
`af32`	DSCP (010000) decimal value 32
`af33`	DSCP (010001) decimal value 33
`af41`	DSCP (101001) decimal value 41
`af42`	DSCP (101010) decimal value 42
`af43`	DSCP (101011) decimal value 38
`cs1`	(Precedence 1) DSCP (001000) decimal value 8
`cs2`	(Precedence 2) DSCP (010000) decimal value 16
`cs3`	(Precedence 3) DSCP (011000) ecimal value 24
`cs4`	(Precedence 4) DSCP (100000) decimal value 32
`cs5`	(Precedence 5) DSCP (101000) decimal value 40
`cs6`	(Precedence 6) DSCP (110000) decimal value 48
`cs7`	(Precedence 7) DSCP (111000) decimal value 56
`default`	DSCP (000000) decimal value 0
`ef`	DSCP (101110) decimal value 46

Default

No default value is specified

© 2021 IP Infusion Inc. Proprietary

Command Mode

Policy map class mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set dscp af12
```

set mpls class

Use this command to set mpls class(queue) for the matched packet.

Use the no command to remove the assigned value from the class.

Command Syntax

```
set mpls class <0-7>
no set mpls class
```

Parameters

<0-7>	Specify class value to assign for this traffic.

Default

No default value is specified

Command Mode

Policy-map type qos

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map my_policy1
(config-pmap-qos)# class traffic_class2
(config-pmap-c-qos)# set mpls class 3
(config-pmap-c-qos)#
```


© 2021 IP Infusion Inc. Proprietary

set precedence

Use this command for matching traffic classes set action as change precedence in the egress packet to the prescribed value.

Use the `no command` to leave the precedence value unchanged for the class

Command Syntax

```
set (precedence (<0-7>| critical| flash | flash-override|immediate|internet|
  network| priority| routine))
no set precedence
```

Parameters

`<0-7>`	Specify IP precedence value to assign for this class of traffic
`critical`	Critical precedence
`flash`	Flash precedence
`flash-override`	Flash override precedence
`immediate`	Immediate precedence
`internet`	Internetwork control precedence
`network`	Network control precedence
`priority`	Priority precedence
`routine`	Routine precedence

Default

No default value is specified

Command Mode

Policy-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map policy1
(config-pmap-qos)# class class2
(config-pmap-c-qos)# set precedence 3
(config-pmap-c-qos)#
```

set qos-group

Use this command to match a QoS group in a type queuing class map.

Use the `no` command to remove a QoS group match on a queue number from a type queuing class map.

Command Syntax

```
set qos-group <1-2000>
no set qos-group <1-2000>
```

Parameters

`<1-2000>`	Specify the QoS group value to assign for this class of traffic.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
(config)#
(config)#policy-map type qos PQOS
(config-pmap-qos)#class type qos C_QOS1
(config-pmap-c-qos)#set qos-group 1
```


© 2021 IP Infusion Inc. Proprietary

set qos queue scheduler

Use this command to change the scheduler mode of Unicast Queue and Non-Unicast queue groups to WRR or SP.

Use the `no` command to disable the set mode, and to change to the default mode

Command Syntax

```
set qos ((wrr uc <1-127> non-uc <1-127>)|sp)
no set qos (wrr|sp)
```

Parameters

`wrr`	Weighted Round Robin Mode
`uc`	Unicast Queues from 1 to 127
`non-uc`	Non-Unicast Queues from 1 to 127
`sp`	Strict Priority Mode

Default

The default is WRR with 32:2.

Command Mode

Configure Mode

Applicability

This command was introduced before OcNOS version 1.3 for platforms Trident II and Trident II+

Tomahawk support is provided with OcNOS DC version 4.2.

Tomahawk supports only wrr setting between uc and mc queues.

Examples

```
(config)#set qos wrr uc 30 non-uc 40
(config)#no set qos wrr
```

set queue

Use this command for matching traffic classes set action as change cos in the egress packet to the prescribed value.

Use the `no` command to remove the assigned value from the class.

Command Syntax

```
set queue <0-7>
no set queue
```

Parameters

`<0-7>`	Specify queue value to assign for this class of traffic

Default

No default value is specified

Command Mode

Policy-map mode

Applicability

'This command was introduced before OcNOS version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map my_policy1
(config-pmap-qos)# class traffic_class2
(config-pmap-c-qos)# set queue 4
(config-pmap-c-qos)#
```


© 2021 IP Infusion Inc. Proprietary

shape

Use this command to configure shaping on an egress queue to impose a maximum rate on it.

Use the `no command` to remove a shaping configuration.

Command Syntax

```
shape (<1-1000000000> (kbps|mbps|gbps) | percent <1-100>)
no shape
```

Parameters

`average`	Specify an optional keyword. Shaping is based on an average rate. Average rate for shaping in the range of `<1-1000000000>`
`kbps`	Specify the units of kbps per second.
`mbps`	Specify the units of mbps per second.
`gbps`	Specify the units of gbps per second.
`percent`	Specify the percentage from 1 to 100.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)# policy-map type queuing my_queue
(config-pmap-que)# class type queuing PQOS
(config-pmap-c-que)# shape percent 25
(config-pmap-c-que)#
```

shape rate

Use this command to configure shaping on an egress port to impose a maximum rate on it.

Use the `no` form of the command to remove a shaping configuration.

Command Syntax

```
shape rate <1-1000000000> (kbps|mbps|gbps) burst SHAPE_BURST_RATE
no shape rate
```

Parameters

`<1-1000000000>`	Average rate for shaping in the following range: 8 kbps to 1000 gbps for Trident3 1 kbps to 1000 gbps for other XGS platforms
`kbps`	Units of kbps per second.
`mbps`	Units of mbps per second.
`gbps`	Units of gbps per second.
`SHAPE_BURST_RATE`	Burst value in kbits in the following range: <2-1000000> for Trident3 and tomahwak <1-1000000> for other XGS platforms

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
(config)#interface xe11
(config-if)#shape rate 100 mbps burst 20
```


© 2021 IP Infusion Inc. Proprietary

show class-map

Use this command to display qos/queuing class maps.

Command Syntax

```
show class-map (type (qos|queuing)|) (NAME|)
```

Parameters

NAME	Specify the named class map

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show class-map type qos
Type qos class-maps
===================
class-map type qos 1234
match cos 3
class-map type qos 2345
QOS-ACCESS-LIST-NAME: 101


#show class-map 1234
Type qos class-maps
===================
class-map type qos 1234
match cos 3
```

show cpu-queue details

Use this command to display details about CPU queue for QoS.

Command Syntax

```
show cpu-queue details
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.8

Example

```
#show cpu-queue details
* - Can not configure the parameter
Cpu queue       Rate In PPS             Lossy Status            Monitor Status
Name      Configured  Default     Configured  Default     Configured  Default
========= ==========  =======     ==========  ==========  ==========  ===========
sflow     10000       32000           -       *lossy      no-monitor   monitor
bgp           -       1500            -        lossless       -        monitor
vrrp          -       500             -        lossless       -        monitor
ldp-rsvp      -       500             -        lossless       -        monitor
rip           -       500             -        lossless       -        monitor
ospf      0           2000        lossy        lossless   monitor      monitor
dhcp          -       100             -        lossy          -        no-monitor
nd        200         6000        lossless     lossless   monitor      monitor
mpls          -       500             -        lossy          -        no-monitor
pim           -       4000            -       *lossy          -       *no-monitor
arp       100         6000        lossy        lossless   no-monitor   monitor
igmp          -       4000            -       *lossy          -       *no-monitor
bpdu      1000        10000           -        lossless   monitor      monitor
ccm           -       500             -        lossy          -        no-monitor
bfd           -       2000            -        lossy          -        no-monitor
ptp           -       1000            -        lossy          -        no-monitor
isis          -       500             -        lossless       -        monitor
trill-isis    -       1000            -        lossless       -        monitor
acl           -       200             -       *lossy          -       *no-monitor
```


© 2021 IP Infusion Inc. Proprietary

```
    vxlan          -       500             -       lossy          -       monitor
```

Table 1-235 explains the output fields.

Table 1-235: show CPU Queue fields

Entry	Description
CPU queue name	Name of the CPU queue
Rate In PPS	At which packets are successfully delivered
`Lossy Status`	Status of the network lossy or lossless
`Monitor Status`	Status of the network monitor

show policy-map

Use this command to display qos/queuing policy-map.

Command Syntax

```
show policy-map (type (qos (statistics |)|queuing|vlan-queuing|hybrid-queuing)|)
show policy-map (type (qos (statistics |)|vlan-queuing|hybrid-queuing|queuing
  (default |))|) NAME
```

Parameters

`qos`	Specify the policy maps of the type qos only.
`statistics`	Displays QoS statistics.
`queuing`	Specify the policy maps of the type queuing only.
`default`	Default queue of the port
`NAME`	Specify named policy map.

Command Mode

Exec and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

Examples

```
#show policy-map type qos statistics
+-------------+--------------------+-----------------+-----------------+-----------------+------------------+
|  Interface  |      Class-map     |    Match pkts   |   Match bytes   |   Dropped pkts  |   Dropped Bytes  |
+-------------+--------------------+-----------------+-----------------+-----------------+------------------+
Policy-map: p5 (input)
xe3/1          c5                   213537882         14520578356       -                 -
Policy-map: q5 (input)
xe3/2          c5                   213538483         14520618816       -                 -

#show policy-map type qos statistics p5
+-------------+--------------------+-----------------+-----------------+-----------------+------------------+
|  Interface  |      Class-map     |    Match pkts   |   Match bytes   |   Dropped pkts  |   Dropped Bytes  |
+-------------+--------------------+-----------------+-----------------+-----------------+------------------+
Policy-map: p5 (input)
xe3/1          c5                   246954616         16792916200       -                 -
```


© 2021 IP Infusion Inc. Proprietary

show policy-map interface

Use this command to display the statistics and the configurations of the input and output policies that are attached to an interface.

Command Syntax

```
show policy-map interface (NAME (input | output | ) (type (qos | queuing)|) | brief)
```

Parameters

NAME	Policy name.
brief	brief policy interface.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show policy-map interface xe19/1


Interface xe19/1
Global statistics status : enabled

Service-policy (qos) input : p1
---------------------------------
 Class-map (qos): c1 (match all)
 match vlan 2
 police cir 2 mbps
      matched    : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (qos): c3 (match all)
 police cir 2 mbps
      matched    : 2172408 packets, 2172408000 bytes
      dropped    : 2128959 packets, 2128959000 bytes


Service-policy (queuing) output: default-out-policy
---------------------------------
 Class-map (queuing): q0
 priority level 1
 bandwidth percent 1
      output     : 0 packets, 0 bytes
      dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
 priority level 1
```

```
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q2
priority level 1
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q3
priority level 1
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q4
priority level 1
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q5
priority level 1
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q6
 priority level 1
bandwidth percent 1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): q7
priority level 1
bandwidth percent 1
     output     : 1445 packets, 92536 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes
```


© 2021 IP Infusion Inc. Proprietary

```
Class-map (queuing): mc-q2
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q4
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
     output     : 0 packets, 0 bytes
     dropped    : 0 packets, 0 bytes
```

show qos-profile

Use this command to show the all configured QoS profiles configurations like type, name, maps configured except for the default maps, attached info (to how many interfaces it is attached) etc,

Command Syntax

```
show qos-profile (type (cos-to-queue | dscp-to-queue | queue-color-to-cos | queue-
  color-to-dscp | dscp-to-exp)| precedence-to-queue | queue-to-precedence |)(NAME|)
```

Parameters

`cos-to-queue`	Profile for CoS to queue map
`dscp-to-queue`	Profile for DSCP to queue map
`queue-color-to-cos`	Profile for queue color to CoS map
`queue-color-to-dscp`	Profile for queue color to DSCP map
`dscp-to-exp`	Profile for DSCP to exp map
`exp-to-queue`	Profile for exp to queue map
`precedence-to-queue`	profile for precedence to queue map
`queue-to-precedence`	profile for queue to precedence map
`NAME`	Profile map name (maximum 32 characters)

Command Mode

Exec, config, interface, class-map, policy-map and policy-map-class

Applicability

This command was introduced in OcNOS DC version 4.2.

Examples

```
OcNOS#show qos-profile in xe1
profile name: default
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS   |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       2       green    |  2       1       2       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow
```


© 2021 IP Infusion Inc. Proprietary

```
profile name: default
 profile type: queue-color-to-cos (Egress)
 Status: Inactive
mapping:
 ----------------+-------- | ----------------+-------- | ----------------+----
----
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      |
OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+----
----
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+----
----
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7
```

show qos-profile interface

Use this command to show the all configured QoS profiles configurations attached on an interface.

Command Syntax

```
show qos-profile interface NAME
```

Parameters

NAME	Profile map name (maximum 32 characters)

Command Mode

Exec, config, interface, class-map, policy-map and policy-map-class

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
(config)#show qos-profile interface xe11
 profile name: cos-map
 profile type: cos-to-queue
 mapping:
 qos profile cos-to-queue cos-map
 cos 0 dei 0 queue 0 color green
 cos 0 dei 1 queue 0 color yellow
 cos 0 queue 0
 cos 1 dei 0 queue 1 color green
 cos 1 dei 1 queue 1 color yellow
 cos 1 queue 1
 cos 2 dei 0 queue 2 color green
 cos 2 dei 1 queue 2 color yellow
 cos 2 queue 2
 cos 3 dei 0 queue 3 color green
 cos 3 dei 1 queue 3 color yellow
 cos 3 queue 3
 cos 4 dei 0 queue 4 color green
 cos 4 dei 1 queue 4 color yellow
 cos 4 queue 4
 cos 5 dei 0 queue 5 color green
 cos 5 dei 1 queue 5 color yellow
 cos 5 queue 5
 cos 6 dei 0 queue 6 color green
```


© 2021 IP Infusion Inc. Proprietary

show queuing interface

Use this command to dispay the configurations of queues attached to an interface.

Command Syntax

```
show queuing interface NAME
```

Parameters

NAME	Interface name.

Command Mode

Exec & config mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
# show queuing interface xe1/1
Egress Queuing for Ethernet xe1/1 [System]
------------------------------------------------------------------------------------------
-------------
L0              L1              L2              Group PrioLevel   Shape Bandwidth
------------------------------------------------------------------------------------------
-------------
q0                                                      -      High        - -
q1                                                      -      High        - -
q2                                                      -      High        - -
q3                                                      -      High        - -
q4                                                      -      High        - -
q5                                                      -      High        - -
q6                                                      -      High        - -
q7                                                      -      High        - -
```

show running-config qos

Use this command to show the user configured QoS configurations.

Command Syntax

```
show running-config qos (all|)
```

Parameters

`all`	Show all QoS related configuration information including all defaults.

Command Mode

Exec, config, interface, class-map, policy-map and policy-map-class

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config qos
qos enable
!
!
#show running-config qos  ?
  all  diplay all qos info including defaults
  |    Output modifiers
  >    Output redirection
  <cr>

#show running-config qos  all
qos enable
!
 qos profile cos-to-queue default
 cos 0 dei 0 queue 0 color green
 cos 0 dei 1 queue 0 color yellow
 cos 0 queue 0
 cos 1 dei 0 queue 1 color green
 cos 1 dei 1 queue 1 color yellow
 cos 1 queue 1
 cos 2 dei 0 queue 2 color green
 cos 2 dei 1 queue 2 color yellow
 cos 2 queue 2
 cos 3 dei 0 queue 3 color green
 cos 3 dei 1 queue 3 color yellow
 cos 3 queue 3
 cos 4 dei 0 queue 4 color green
 cos 4 dei 1 queue 4 color yellow
 cos 4 queue 4
 cos 5 dei 0 queue 5 color green
 cos 5 dei 1 queue 5 color yellow
 cos 5 queue 5
 cos 6 dei 0 queue 6 color green
 cos 6 dei 1 queue 6 color yellow
 cos 6 queue 6
```


© 2021 IP Infusion Inc. Proprietary

```
 cos 7 dei 0 queue 7 color green
 cos 7 dei 1 queue 7 color yellow
 cos 7 queue 7
!
qos profile queue-color-to-cos default
 queue 0 color green cos 0
 queue 0 color yellow cos 0
 queue 0 color red cos 0
 queue 0 color all cos 0
 queue 1 color green cos 1
 queue 1 color yellow cos 1
 queue 1 color red cos 1
 queue 1 color all cos 1
 queue 2 color green cos 2
 queue 2 color yellow cos 2
 queue 2 color red cos 2
 queue 2 color all cos 2
 queue 3 color green cos 3
 queue 3 color yellow cos 3
 queue 3 color red cos 3
 queue 3 color all cos 3
 queue 4 color green cos 4
queue 4 color yellow cos 4
 queue 4 color red cos 4
 queue 4 color all cos 4
 queue 5 color green cos 5
 queue 5 color yellow cos 5
 queue 5 color red cos 5
 queue 5 color all cos 5
 queue 6 color green cos 6
 queue 6 color yellow cos 6
 queue 6 color red cos 6
 queue 6 color all cos 6
 queue 7 color green cos 7
 queue 7 color yellow cos 7
 queue 7 color red cos 7
 queue 7 color all cos 7
!
qos profile dscp-to-queue default
 dscp 0 queue 0 color green
 dscp 1 queue 0 color green
 dscp 2 queue 0 color green
 dscp 3 queue 0 color green
 dscp 4 queue 0 color green
 dscp 5 queue 0 color green
 dscp 6 queue 0 color green
 dscp 7 queue 0 color green
 dscp 8 queue 1 color green
 dscp 9 queue 1 color green
 dscp 10 queue 1 color green
 dscp 11 queue 1 color green
 dscp 12 queue 1 color yellow
 dscp 13 queue 1 color green
 dscp 14 queue 1 color red
 dscp 15 queue 1 color green
 dscp 16 queue 2 color green
 dscp 17 queue 2 color green
```

```
 dscp 18 queue 2 color green
 dscp 19 queue 2 color green
 dscp 20 queue 2 color yellow
 dscp 21 queue 2 color green
 dscp 22 queue 2 color red
 dscp 23 queue 2 color green
 dscp 24 queue 3 color green
 dscp 25 queue 3 color green
 dscp 26 queue 3 color green
 dscp 27 queue 3 color green
 dscp 28 queue 3 color yellow
dscp 29 queue 3 color green
 dscp 30 queue 3 color red
 dscp 31 queue 3 color green
 dscp 32 queue 4 color green
 dscp 33 queue 4 color green
 dscp 34 queue 4 color green
 dscp 35 queue 4 color green
 dscp 36 queue 4 color yellow
 dscp 37 queue 4 color green
 dscp 38 queue 4 color red
 dscp 39 queue 4 color green
 dscp 40 queue 5 color green
 dscp 41 queue 5 color green
 dscp 42 queue 5 color green
 dscp 43 queue 5 color green
 dscp 44 queue 5 color green
 dscp 45 queue 5 color green
 dscp 46 queue 5 color green
 dscp 47 queue 5 color green
 dscp 48 queue 6 color green
 dscp 49 queue 6 color green
 dscp 50 queue 6 color green
 dscp 51 queue 6 color green
 dscp 52 queue 6 color green
 dscp 53 queue 6 color green
 dscp 54 queue 6 color green
 dscp 55 queue 6 color green
 dscp 56 queue 7 color green
 dscp 57 queue 7 color green
 dscp 58 queue 7 color green
 dscp 59 queue 7 color green
 dscp 60 queue 7 color green
 dscp 61 queue 7 color green
 dscp 62 queue 7 color green
 dscp 63 queue 7 color green
!
qos profile queue-color-to-dscp default
 queue 0 color green dscp 0
 queue 0 color yellow dscp 0
 queue 0 color red dscp 0
 queue 0 color all dscp 0
 queue 1 color green dscp 10
 queue 1 color yellow dscp 12
 queue 1 color red dscp 14
 queue 1 color all dscp 8
 queue 2 color green dscp 18
```

 © 2021 IP Infusion Inc. Proprietary

```
 queue 2 color yellow dscp 20
 queue 2 color red dscp 22
 queue 2 color all dscp 16
 queue 3 color green dscp 26
 queue 3 color yellow dscp 28
 queue 3 color red dscp 30
 queue 3 color all dscp 24
 queue 4 color green dscp 34
 queue 4 color yellow dscp 36
 queue 4 color red dscp 38
 queue 4 color all dscp 32
 queue 5 color green dscp 40
 queue 5 color yellow dscp 40
 queue 5 color red dscp 40
 queue 5 color all dscp 40
 queue 6 color green dscp 48
 queue 6 color yellow dscp 48
 queue 6 color red dscp 48
 queue 6 color all dscp 48
 queue 7 color green dscp 56
 queue 7 color yellow dscp 56
 queue 7 color red dscp 56
 queue 7 color all dscp 56
!
policy-map type queuing default default-out-policy
 class type queuing default q0
  priority
  exit
 class type queuing default q1
  priority
  exit
class type queuing default q2
  priority
  exit
 class type queuing default q3
  priority
  exit
 class type queuing default q4
  priority
  exit
 class type queuing default q5
  priority
  exit
 class type queuing default q6
  priority
  exit
 class type queuing default q7
  priority
  exit
!
interface xe1/1
 service-policy type queuing default default-out-policy
!
interface xe1/2
 service-policy type queuing default default-out-policy
!
interface xe1/3
```

```
 service-policy type queuing default default-out-policy
!
interface xe1/4
 service-policy type queuing default default-out-policy
!
interface xe2/1
 service-policy type queuing default default-out-policy
```


© 2021 IP Infusion Inc. Proprietary

show running-config cpu-queue

Use this command to display details about CPU queue information based on processes running.

Command Syntax

```
show running-config cpu-queue
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.8

Example

```
#show running-config | in cpu-queue
cpu-queue sflow rate 10000 no-monitor
cpu-queue ospf rate 0 lossy monitor
cpu-queue nd rate 200 lossless monitor
cpu-queue arp rate 100 lossy no-monitor
cpu-queue bpdu rate 1000 monitor
```

storm-control

Use this command to set the rising threshold level for broadcast, multicast, or destination lookup failure traffic. The storm control action occurs when traffic utilization reaches this level.

Storm control is used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

Use the `no` form of this command to disable storm control.

Command Syntax

```
storm-control (broadcast|multicast|dlf) (level LEVEL | <0-1000000000>
(kbps|mbps|gbps) burst-size <32-16M>)
no storm-control (broadcast|multicast|dlf)
```

Parameters

`broadcast`	Broadcast rate limiting.
`multicast`	Multicast rate limiting.
`dlf`	Destination lookup failure limiting.
`level`	Sets the percentage of the threshold.
`LEVEL`	The percentage of the threshold; percentage of the maximum speed (pps) of the interface <0.0000-1000.0000>.
`<0-1000000000>`	Sets absolute threshold value <0-1000000000>
`kbps`	specifies the units of Kilobits per second.
`mbps`	specifies the units of Megabits per second.
`gbps`	specifies the units of Gigabits per second.
`burst-size`	Set burst size
`<32-16M>`	value of burst in kbps

Default

By default, storm control is disabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#storm-control broadcast level 30
```


© 2021 IP Infusion Inc. Proprietary

```
(config)#interface xe2
(config-if)#storm-control multicast level 30

(config)#interface xe3
(config-if)#storm-control multicast 300 mbps

(config)#interface xe4
(config-if)#no storm-control multicast
```

trust dscp

Use this command to use dscp value to decide queue mapping for packets in Layer 2 interfaces.

The no parameter with this command un-sets trust dscp.

Command Syntax

```
trust dscp
no trust dscp
```

Parameters

None

Default

By default, trust dscp is disabled on L2 interface

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#int xe1/1
(config-if)#trust dscp
```


© 2021 IP Infusion Inc. Proprietary

wrr-queue weight

Use this command to set wrr-queue weight for a queue.

Use the priority command to un-set configured wrr configuration.

Command Syntax

```
wrr-queue weight <1-127>
```

Parameters

<1-127>	wrr queue weight to be configured.

Default

No default value is specified

Command Mode

Policy-class-map queuing Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#policy-map type queuing default default-out-policy
(config-pmap-que-def)# class type queuing default q0
(config-pmap-c-que-def)#wrr-queue weight 2
(config-pmap-c-que-def)#priority
```

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

SECTION 13 Virtual eXtensible Local Area Network

Virtual eXtensible Local Area Network Configuration Guide

Contents

This guide contains the chapters:

- Chapter 1, *Overview*
- Chapter 2, *VXLAN Unicast Configuration*
- Chapter 3, *VXLAN-EVPN Configuration*
- Chapter 4, *VXLAN EVPN EVC Configuration*
- Chapter 5, *VXLAN Hybrid Access Port Configuration*
- Chapter 6, *VXLAN Multi-homing Configuration*
- Chapter 7, *VXLAN Quality of Service Configuration*
- Chapter 8, *VXLAN Trunk Access Port*
- Chapter 9, *VXLAN Tunnel Over SVI*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Overview

This chapter provides an overview of Virtual eXtensible Local Area Network (VXLAN) and its implementation with OcNOS. VXLAN creates LAN segments using a MAC in IP encapsulation. The encapsulation carries the original L2 frame received from a host to the destination in another server using IP tunnels. The endpoints of the virtualized tunnel formed using VXLAN are called VTEPs (VXLAN Tunnel EndPoints). This technology allows the network to support several tenants with minimum changes in the network. The VTEPs carry tenant data in L3 tunnels over the network. The tenant data is not used in routing or switching. This aids in tenant machine movement and allows the tenants to have the same IP or MAC addresses on end devices, hosts/VM's.

OcNOS supports VxLAN IPv4 tunnels, but both IPv4 and IPv6 hosts are supported.

Terminology

Terms related to VXLAN configuration are defined in the table below.

IGMP	Internet Group Management Protocol
PIM	Protocol Independent Multicast
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNI	VXLAN Network Identifier (or VXLAN Segment ID)
VTEP	VXLAN Tunnel End Point. An entity that originates and/or terminates VXLAN tunnels
VXLAN	Virtual eXtensible Local Area Network
VXLAN Segment	VXLAN Layer 2 overlay network over which VMs communicate
VXLAN Gateway	An entity that forwards traffic between VXLANs

VXLAN Architecture

VXLAN runs over the existing networking infrastructure. It provides a means to "stretch" a Layer 2 network. In short, VXLAN is a Layer 2 overlay scheme on a Layer 3 network.

Each overlay is termed as a VXLAN segment. Only VMs within the same VXLAN segment can communicate with each other. Each VXLAN segment is identified through a 24-bit segment ID termed the "VXLAN Network Identifier (VNI)". This allows up to 16 million VXLAN segments to coexist within the same administrative domain.

VNI identifies the scope of the inner MAC frame originated by the individual VM. Hence, we can have overlapping MAC addresses across segments but never have traffic "cross over" since the traffic is isolated using the VNI. The VNI is in an outer header that encapsulates the inner MAC frame originated by the VM.

Any packets (including ARP-ND) that are uplifted to the VxLAN CPU queue from any port are rate limited to 500 packets/second. This is done to protect the system and CPU during an ARP storm.

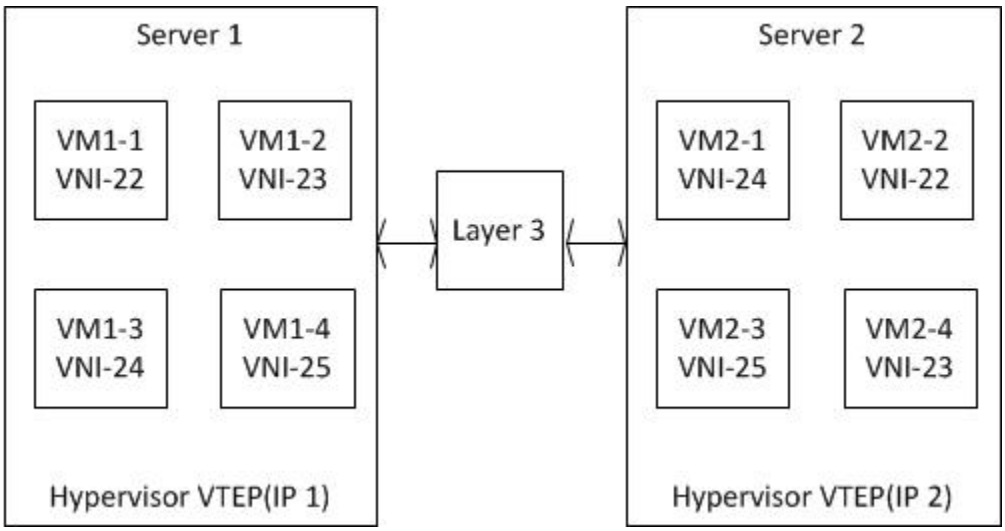


Figure 1-70: VXLAN Deployment - VTEPs across a Layer 3 Network

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 VXLAN Unicast Configuration

This chapter contains basic Static-VXLAN unicast configuration examples.

Port Mapping

In this example each VTEP (VTEP1 and VTEP2) is a multilayer switch where xe2 is an access port while xe1 is network port.

After we start sending a packet (say untagged ipv4 packet) from VM1, it hits the VTEP1,VTEP1 does encapsulation based on the VNID configured and send it on xe1. Now the packet reaches VTEP2 and it does decapsulation of the packet. Now based on VNID packet is sent out on access port and it reaches destination VM, VM2.

Topology

The procedures in this section use the topology in Figure 2-71

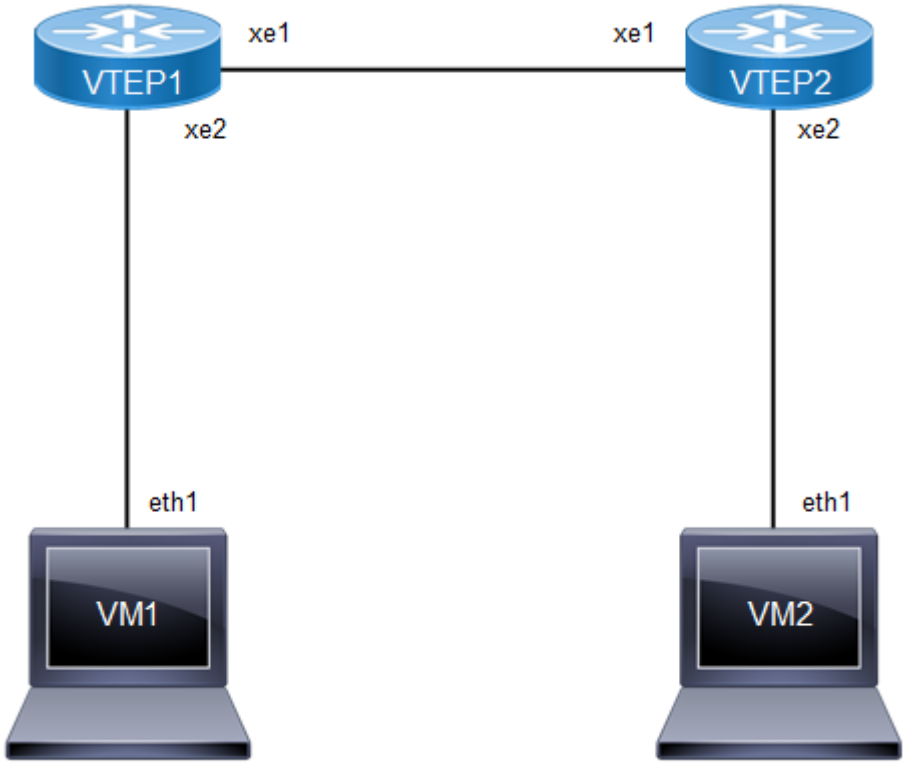


Figure 2-71: VXLAN unicast

VTEP1

`#configure terminal`	Enter the configure mode
`(config)#interface xe2`	Enter interface mode
`(config-if)#switchport`	Configure the interface as switchport
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown

(config-if)#exit	Exit interface mode
(config)#interface lo	Enter the configure mode
(config-if)#ip address 1.1.1.1/32 secondary	Configure IP address on the interface xe1
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode
(config)#interface xe1	Enter the configure mode
(config-if)#ip address 5.5.5.2/24	Configure IP address on the interface xe1
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode
(config)#ip route 2.2.2.2/32 5.5.5.4	Configure static route
(config)#nvo vxlan enable	Enable VXLAN globally on this vtep
(config)#interface tunnel 4	Specify the interface (Tunnel4)to be configured and Enter interface mode
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN
(config-if)#tunnel source 1.1.1.1	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1
(config-if)#tunnel destination 2.2.2.2	Configure the destination IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP2.
(config-if)#exit	Exit interface mode
(config)#nvo vxlan id 2	Configure a VNID on this VTEP and enter the nvo mode.
(config-nvo)#vxlan map-network tunnel Tunnel4	Map the tunnel 4 with VNID 2
(config-nvo)#vxlan static-entry host-mac 0000.0000.aaaa remote-vtep-ip 2.2.2.2	Configure a static entry for remote VM with MAC address and IP address.
(config-nvo)#exit	Exit the nvo mode
(config)#nvo vxlan access-if port xe2	Map the access port xe2 of this VTEP
(config-nvo-acc-if)#map vnid 2	Map the VNID 2 to access-port xe2
(config-nvo-acc-if)#exit	Exit the nvo access-if mode
(config)#commit	Perform commit operation for the changes to take effect.

VTEP2

#configure terminal	Enter the configure mode
(config)#interface xe2	Enter interface mode
(config-if)#switchport	Configure the interface as switchport
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode
(config)#interface lo	Enter the configure mode
(config-if)#ip address 2.2.2.2/32 secondary	Configure IP address on the interface xe1
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode
(config)#interface xe1	Enter the configure mode

© 2021 IP Infusion Inc. Proprietary

(config-if)#ip address 5.5.5.4/24	Configure IP address on the interface xe1
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode
(config)#ip route 1.1.1.1/32 5.5.5.2	Configure static route
(config)#nvo vxlan enable	Enable VXLAN globally on this vtep
(config)#interface tunnel 4	Specify the interface (Tunnel4)to be configured and Enter interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN
(config-if)#tunnel source 2.2.2.2	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
(config-if)#tunnel destination 1.1.1.1	Configure the destination IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP2.
(config-if)#exit	Exit interface mode.
(config)#nvo vxlan id 2	Configure a VNID on this VTEP and enter the nvo mode.
(config-nvo)#vxlan map-network tunnel Tunnel4	Map the tunnel 4 with VNID 2
(config-nvo)#vxlan static-entry host-mac 0000.0000.bbbb remote-vtep-ip 1.1.1.1	Configure a static entry for remote VM with MAC address and IP address.
(config-nvo)#exit	Exit the nvo mode.
(config)#nvo vxlan access-if port xe2	Map the access port xe2 of this VTEP
(config-nvo-acc-if)#map vnid 2	Map the VNID 2 to access-port xe2
(config-nvo-acc-if)#exit	Exit the nvo access-if mode
(config)#commit	Perform commit operation for the changes to take effect.

Validation

VTEP1

```
VTEP1#show nvo vxlan tunnel
VVXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
2.2.2.4          3.3.3.4          Installed     00:37:56     00:37:56

Total number of entries are 1
VTEP1#

VTEP1#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface     ESI                             VLAN DF-
Status Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________
```

```
3        ----          L2       NW   ----          ------                          ---- --
--      2.2.2.4          3.3.3.4
3       ----        --       AC   xe2        --- Single Homed Port ---     ---- ----
----              ----

Total number of entries are 2

VTEP1#show nvo vxlan mac-table
================================================================================================
=========================================================
======
                         VXLAN MAC Entries
================================================================================================
=========================================================
======
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
________________________________________________________________________________________________
_____________________________________________________
_______

3         ----       ----   ----         0000.0000.aaaa 3.3.3.4
Static Remote        -------             -------
3        xe2     ----   ----        0000.0000.bbbb Local                        Dynamic
Local        -------             -------

Total number of entries are : 2

VTEP1#show nvo vxlan mac-table vnid 3

================================================================================================
=========================================================
======
                           VXLAN MAC Entries
================================================================================================
=========================================================
======
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
________________________________________________________________________________________________
_____________________________________________________
_______

3         ----       ----   ----         0000.0000.aaaa 3.3.3.4
Static Remote        -------             -------
3        xe2     ----   ----        0000.0000.bbbb Local                        Dynamic
Local        -------             -------

Total number of entries are : 2
```

RTR1

```
RTR1#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface           Uptime     Expires   State    Last Reporter
```


© 2021 IP Infusion Inc. Proprietary

```
2.2.2.1           xe1               00:11:25   00:03:44  Active   2.2.2.4
3.3.3.1           xe2               00:01:36   00:04:17  Active   3.3.3.4
```

VTEP2

```
VTEP2#show nvo vxlan tunnel
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface     ESI                             VLAN DF-
Status Src-Addr         Dst-Addr
_____________________________________________________________________________________________
_____________________________________
3         ----         L2       NW   ----          ------                          ---- --
--      3.3.3.4          2.2.2.4
3         ----         L2       NW   ----          ------                          ---- --
--      3.3.3.4          239.10.10.9
3         ----         --       AC   xe1           --- Single Homed Port ---     ---- --
--      ----             ----
 Total number of entries are 3
VTEP2#

VTEP#2show nvo vxlan vnid 3
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface     ESI                             VLAN DF-
Status Src-Addr         Dst-Addr
_____________________________________________________________________________________________
_____________________________________
3         ----         L2       NW   ----          ------                          ---- --
--      3.3.3.4          2.2.2.4
3         ----         --       AC   xe2           --- Single Homed Port ---     ---- --
--      ----             ----

Total number of entries are 2
VTEP#show vno vxlan mac-table
=============================================================================================
=====================================================
======
                                                                VXLAN MAC Entries
=============================================================================================
=====================================================
======
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
_____________________________________________________________________________________________
_____________________________________________________
```

```
______

3         xe2         ----   ----         0000.0000.aaaa Local
Dynamic Local         -------              -------
3         ----        ----   ----         0000.0000.bbbb 2.2.2.4
Static Remote         -------              -------

Total number of entries are : 2

VTEP2#show nvo vxlan mac-table vnid 3
================================================================================
================================================
======
                            VXLAN MAC Entries
================================================================================
================================================
======
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
________________________________________________________________________________
________________________________________________
______

3         xe2         ----   ----         0000.0000.aaaa Local
Dynamic Local         -------              -------
3         ----        ----   ----         0000.0000.bbbb 2.2.2.4
Static Remote         -------              -------

Total number of entries are : 2
```

Intermediate Non-VXLAN Router

This example is same as port mapping but we have an intermediate non VXLAN router. It does forwarding based on IP header.

Topology

The procedures in this section use the topology in Figure 2-72

© 2021 IP Infusion Inc. Proprietary

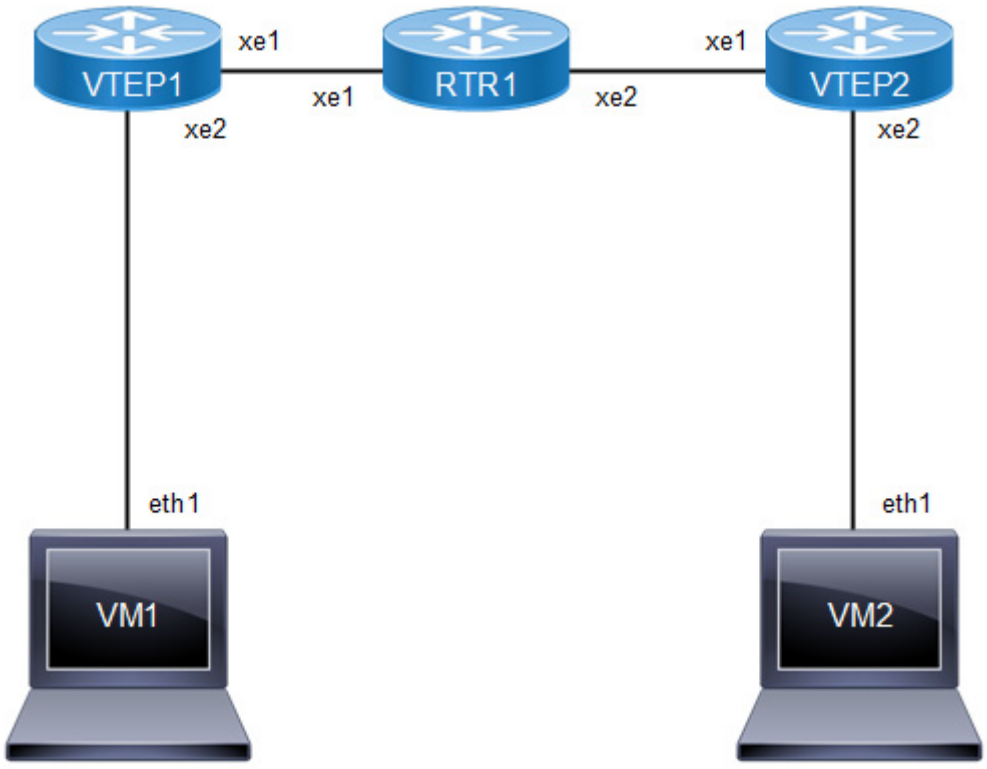


Figure 2-72: VXLAN unicast

VTEP1

`#configure terminal`	Enter the configure mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as switchport.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter the configure mode.
`(config-if)#ip address 2.2.2.4/24`	Configure IP address on the interface xe1.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#exit`	Exit interface mode.
`(config)#ip route 3.3.3.0/24 2.2.2.1`	Configuring static route
`(config)#nvo vxlan enable`	Enable VXLAN globally on this vtep.
`(config)#interface tunnel 4`	Specify the interface (Tunnel4)to be configured and Enter interface mode.
`(config-if)#tunnel mode vxlan`	Assign this tunnel mode as VXLAN.
`(config-if)#tunnel source 2.2.2.4`	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
`(config-if)#tunnel destination 3.3.3.4`	Configure the destination IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP2.
`(config-if)#exit`	Exit interface mode.
`(config)#nvo vxlan id 3`	Configure a VNID on this VTEP and enter the nvo mode.

`(config-nvo)#vxlan map-network tunnel Tunnel4`	Map the tunnel 4 with this VNID
`(config-nvo)#vxlan static-entry host-mac 0000.0000.aaaa remote-vtep-ip 3.3.3.4`	Configure a static entry for remote VM with MAC address and IP address.
`(config)#nvo vxlan access-if port xe2`	Map the access port xe2 of this VTEP
`(config-nvo-acc-if)#map vnid 3`	Map the VNID 2 to access-port xe2
`(config-nvo-acc-if)#exit`	Exit NVO access-interface mode
`(config)#commit`	Perform commit operation for the changes to take effect.

RTR1

`(config)#interface xe1`	Enter the configure mode.
`(config-if)#ip address 2.2.2.1/24`	Configure IP address on the interface xe1.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter the configure mode.
`(config-if)#ip address 3.3.3.1/24`	Configure IP address on the interface xe2.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#exit`	Exit interface mode.
`(config)#commit`	Perform commit operation for the changes to take effect.

VTEP2

`#configure terminal`	Enter the configure mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as switchport.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter the configure mode.
`(config-if)#ip address 3.3.3.4/24`	Configure IP address on the interface xe1.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#exit`	Exit interface mode.
`(config)#ip route 2.2.2.0/24 3.3.3.1`	Configuring static route
`(config)#nvo vxlan enable`	Enable VXLAN globally on this vtep.
`(config)#interface tunnel 4`	Specify the interface (Tunnel4)to be configured and Enter interface mode.
`(config-if)#tunnel mode vxlan`	Assign this tunnel mode as VXLAN.
`(config-if)#tunnel source 3.3.3.4`	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
`(config-if)#tunnel destination 2.2.2.4`	Configure the destination IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP2.
`(config-if)#exit`	Exit interface mode.
`(config)#nvo vxlan id 3`	Configure a VNID on this VTEP and enter the nvo mode.

© 2021 IP Infusion Inc. Proprietary

(config-nvo)#vxlan map-network tunnel Tunnel4	Map the tunnel 4 with this VNID
(config-nvo)#vxlan static-entry host-mac 0000.0000.bbbb remote-vtep-ip 2.2.2.4	Configure a static entry for remote VM with MAC address and IP address.
(config)#nvo vxlan access-if port xe2	Map the access port xe2 of this VTEP
(config-nvo-acc-if)#map vnid 3	Map the VNID 3 to access-port xe2
(config-nvo-acc-if)#exit	Exit the NVO access interface mode
(config)#commit	Perform commit operation for the changes to take effect.

Validation

VTEP1

```
VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
2.2.2.4          3.3.3.4          Installed     00:37:56     00:37:56
Total number of entries are 1
VTEP1#
VTEP1#
VTEP1#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface     ESI                             VLAN DF-
Status Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________
3        ----         L2       NW   ----          ------                          ---- --
--      2.2.2.4          3.3.3.4
3       ----        --       AC   xe2        --- Single Homed Port ---     ---- ----
----             ----
 Total number of entries are 2
VTEP1#
VTEP1#show nvo vxlan mac-table
================================================================================
========================================================
======
                                                              VXLAN MAC Entries
================================================================================
========================================================
======
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status             AccessPortDesc
_____________________________________________________________________________________
_____________________________________________________
_______
```

```
3         ----       ----   ----         0000.0000.aaaa 3.3.3.4
Static Remote        -------              -------
3        xe2      ----   ----        0000.0000.bbbb Local                        Dynamic
Local        -------              -------

Total number of entries are : 2

VTEP1#
VTEP1#
VTEP1#sh nvo vxlan mac-table vnid 3
================================================================================================
=========================================================
======
                                                                  VXLAN MAC Entries
================================================================================================
=========================================================
======
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
________________________________________________________________________________________________
_____________________________________________________
______

3         ----       ----   ----         0000.0000.aaaa 3.3.3.4
Static Remote        -------              -------
3        xe2      ----   ----        0000.0000.bbbb Local                        Dynamic
Local        -------              -------

Total number of entries are : 2

VTEP1#
```

VTEP2

```
VTEP2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
3.3.3.4          2.2.2.4          Installed     00:34:02     00:34:02
Total number of entries are 1
VTEP2#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface     ESI                             VLAN DF-
Status Src-Addr         Dst-Addr
________________________________________________________________________________________
_____________________________________
```


© 2021 IP Infusion Inc. Proprietary

```
3         ----          L2       NW   ----          ------                          ---- --
--      3.3.3.4           2.2.2.4
3         ----          --       AC   xe1           --- Single Homed Port ---     ---- --
--      ----              ----
 Total number of entries are 2
VTEP2#sh nvo vxlan mac-table
================================================================================================
=======================================================
======
                                                                VXLAN MAC Entries
================================================================================================
=======================================================
======
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
________________________________________________________________________________________________
_____________________________________________________
_______

3         xe1        ----   ----         0000.0000.aaaa Local
Dynamic Local        -------             -------
3         ----       ----   ----         0000.0000.bbbb 2.2.2.4
Static Remote        -------             -------

Total number of entries are : 2

VTEP2#sh nvo vxlan mac-table vnid 3
================================================================================================
=======================================================
======
                                                                VXLAN MAC Entries
================================================================================================
=======================================================
======
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
________________________________________________________________________________________________
_____________________________________________________
_______

3         xe1        ----   ----         0000.0000.aaaa Local
Dynamic Local        -------             -------
3         ----       ----   ----         0000.0000.bbbb 2.2.2.4
Static Remote        -------             -------

Total number of entries are : 2

VTEP2#
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 VXLAN-EVPN Configuration

This section contains basic VXLAN-EVPN configuration examples.

VXLAN (Virtual eXtended LAN) creates LAN segments using a MAC-in-IP encapsulation. The encapsulation carries the original L2 frame received from a host to the destination in another host using IP tunnels. The endpoints of the virtualized tunnel formed using VXLAN are called VTEPs (VXLAN Tunnel End Points). The VTEPs carry tenant data in L3 tunnels over the network which permits the network to support multiple tenants.The tenant data is not used in routing or switching. This aids in tenant machine movement and allows the tenants to have same IP/MAC addresses.

Information about the given VM to get to the VTEP is crucial in VXLAN protocol; therefore BGP-MP is used to carry this information across VTEPS.

Note: For port-channel/Static-channel interface, storm control will be applied on each member port. For Example: if Interface eth1 and interface eth2 is part of port-channel i.e. po1 and storm control 2mbps is applied for broadcast traffic, then the storm control settings will be applied on each member port and broadcast traffic on each member port will be rate limited to 2mbps each.

Topology

The procedures in this section use the topology in Figure 3-73.

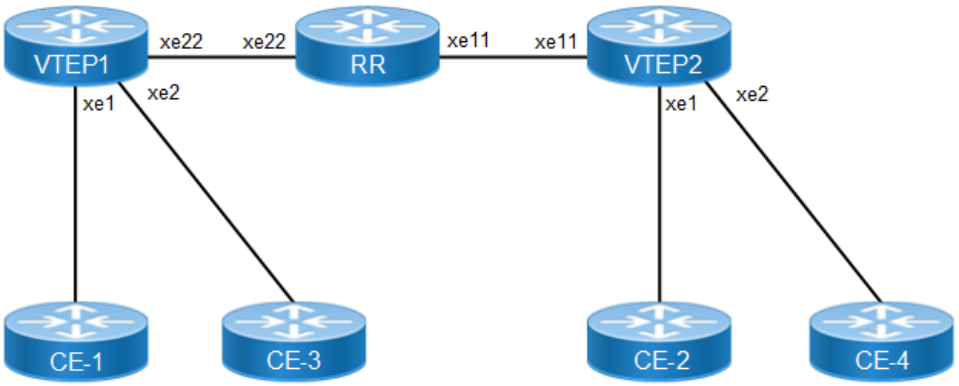


Figure 3-73: VXLAN EVPN

VTEP1

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode
`(config)#interface xe2`	Enter interface mode
`(config-if)#switchport`	Configure the interface as switch port.
`(config-if)#no shutdown`	Bring the interface into operation.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe22`	Enter interface mode.
`(config-if)#ip address 10.1.1.1/24`	Set an IP address on the interface.

(config-if)#no shutdown	Bring the interface into operation.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 1.1.1.1/32 secondary	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.1111.1111.1111.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe22	Enter interface mode
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 1.1.1.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#router bgp 1	Define the routing process. The number 1 specifies the AS number of VTEP1.
(config-router)#bgp router-id 1.1.1.1	Configure router-id for this BGP process.
(config-router)#neighbor 2.2.2.2 remote-as 1	Define BGP neighbor: 2.2.2.2 is the IP address of the neighbor (VTEP2), and 1 is the neighbor's AS number.
(config-router)# neighbor 2.2.2.2 update-source 1.1.1.1	Define BGP neighbor: 1.1.1.1 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 2.2.2.2 activate	Activate the neighbor in the EVPN address family.
(config-router-af)#exit-address-family	Exit the address-family mode.
(config-router)#exit	Exit router mode.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.
(config)#nvo vxlan vtep-ip-global 1.1.1.1	Assign a global IP to the VTEP.
(config)#nvo vxlan id 100 ingress-replication	Configure a VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with vrf_evpn_100.
(config-nvo)#exit	Exit NVO mode.

© 2021 IP Infusion Inc. Proprietary

(config)#nvo vxlan access-if port-vlan xe1 2	Configure access-port xe1 and map vlan 2
(config-nvo-acc-if)#map vnid 100	Map VNID 100 to access-port xe1.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan id 200 ingress-replication	Configure second VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with vrf_evpn_100
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe2 3	Configure access-port xe2 and map vlan 3
(config-nvo-acc-if)#map vnid 200	Map VNID 200 to access-port xe2.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.

RR

#configure terminal	Enter configure mode.
(config)#interface xe22	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe11	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.3333.3333.3333.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe22	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe11	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

VTEP2

#configure terminal	Enter configure mode.
(config)#interface xe1	Enter interface mode.
(config-if)#switchport	Configure the interface as switchport.

(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe11	Enter interface mode.
(config-if)#ip address 20.1.1.1/24	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 2.2.2.2/32 secondary	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.2222.2222.2222.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe11	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 2.2.2.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#router bgp 1	Define the routing process. The number 1 specifies the AS number of VTEP1.
(config-router)#neighbor 1.1.1.1 remote-as 1	Define BGP neighbor: 1.1.1.1 is the IP address of the neighbor (VTEP1), and 1 is the neighbor's AS number.
(config-router)# neighbor 1.1.1.1 update-source 2.2.2.2	Define BGP neighbor: 2.2.2.2 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor in the EVPN address family.
(config-router-af)#exit-address-family	Exit address-family mode.
(config-router)#exit	Exit router mode.

© 2021 IP Infusion Inc. Proprietary

`(config)#nvo vxlan enable`	Enable VXLAN globally on this VTEP.
`(config)#nvo vxlan vtep-ip-global 2.2.2.2`	Assign a global IP to the VTEP.
`(config)#nvo vxlan id 100 ingress-replication`	Configure a VNID on this VTEP and enter NVO mode.
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100`	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with `vrf_evpn_100`.
`(config-nvo)#exit`	Exit NVO mode.
`(config)#nvo vxlan access-if port-vlan xe1 2`	Configure access-port xe1 and map vlan 2
`(config-nvo-acc-if)#map vnid 100`	Map VNID 100 to access-port xe1.
`(config-nvo-acc-if)#exit`	Exit NVO access-if mode.
`(config)#nvo vxlan id 200 ingress-replication`	Configure second VNID on this VTEP and enter NVO mode.
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100`	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with `vrf_evpn_100`
`(config-nvo)#exit`	Exit NVO mode.
`(config)#nvo vxlan access-if port-vlan xe2 3`	Configure access-port xe2 and map vlan 3
`(config-nvo-acc-if)#map vnid 200`	Map VNID 200 to access-port xe2.
`(config-nvo-acc-if)#exit`	Exit NVO access-if mode.

Validation

CE1 and CE2 have hosts configured with MAC addresses, IP addresses, and VLAN identifiers as shown below.

		VLAN	IP Address	Mac Address
VTEP1	CE-1	2	12.12.12.10	0000.0000.abab
VTEP2	CE-2	2	12.12.12.20	0000.0000.cdcd
VTEP1	CE-1	3	13.13.13.10	0000:0b60:25f2
VTEP2	CE-2	3	13.13.13.20	0000:0b60:25f3

Perform a tagged ping of VLAN 2 from CE1 to CE2 and vice-versa. Also perform a tagged ping of VLAN 3 from CE1 to CE2 and vice-versa.

VTEP Tunnel Status

```
VTEP-1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
1.1.1.1          2.2.2.2          Installed     00:05:53     00:05:53
Total number of entries are 1


VTEP-2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
```

```
================================================================================
2.2.2.2          1.1.1.1          Installed     00:05:46     00:05:46
Total number of entries are 1
```

VTEP ARP Cache

```
VTEP-1#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
ARP Timeout : 300 sec Random-Jitter-Max : 640
VNID     Ip-Addr          Mac-Addr              Type                    Age-Out
Retries-Left

_____________________________________________________________________________
200      13.13.13.10    0000.0b60.25f2     Dynamic Local        246              2
200      13.13.13.20    0000.0b60.25f3     Dynamic Remote   ------
100      12.12.12.20    0000.0000.cdcd     Dynamic Remote   ------
100      12.12.12.10   0000.0000.abab     Dynamic Local        246              2
Total number of entries are 4

VTEP-2#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
ARP Timeout : 300 sec Random-Jitter-Max : 640
VNID      Ip-Addr              Mac-Addr                Type                    Age-
Out       Retries-Left

_____________________________________________________________________________
200     13.13.13.10        0000.0b60.25f2       Dynamic Remote      -------
200     13.13.13.20        0000.0b60.25f3     Dynamic Local            257
2
100     12.12.12.10        0000.0000.abab      Dynamic Remote      -------
100     12.12.12.20        0000.0000.cdcd     Dynamic Local            257
2
Total number of entries are 4
```

VTEP MAC Tables

```
VTEP-1#show nvo vxlan mac-table
================================================================================
                                VXLAN MAC Entries
================================================================================
VNID   Interface   VlanId    Inner-VlanId    Mac-Addr        VTEP-Ip/ESI     Type
Status   AccessPortDesc

________________________________________________________________________________

100      ----             ----           ----        0000.0000.cdcd      2.2.2.2
Dynamic Remote   -------    -------
100      xe1              2              ----        0000.0000.abab      1.1.1.1
Dynamic Local        -------    -------
200      xe2              3             ----        0000.0b60.25f2       1.1.1.1
Dynamic Local        -------    -------
200      ----             ----           ----        0000.0b60.25f3      2.2.2.2
Dynamic Remote   -------    -------
Total number of entries are : 4
```


© 2021 IP Infusion Inc. Proprietary

```
VTEP-2#show nvo vxlan mac-table
================================================================================
                              VXLAN MAC Entries
================================================================================
VNID   Interface  VlanId    Inner-VlanId    Mac-Addr      VTEP-Ip/ESI     Type
Status     AccessPortDesc
________________________________________________________________________________

100      xe1            2          ----              0000.0000.cdcd     2.2.2.2
Dynamic Local      -------    -------
100      ----           ----       ----              0000.0000.abab     1.1.1.1
Dynamic Remote -------     -------
200      ----           ----       ----              0000.0b60.25f2      1.1.1.1
Dynamic Remote  -------     -------
200      xe2            3         ----              0000.0b60.25f3      2.2.2.2
Dynamic Local      -------     -------
Total number of entries are : 4
```

VTEP MAC-IP BGP EVPN Entries

```
VTEP-1#show bgp l2vpn evpn mac-ip
RD[1.1.1.1:1] VRF[vrf_evpn_100]:
ESI              Eth-Tag      Mac-Address           IP-Address     VNID     L3VNID
Nexthop         GW-Type
0                  100        0000:0000:abab    12.12.12.10    100      0
1.1.1.1             --
0                  200        0000:0b60:25f2     13.13.13.10    200      0
1.1.1.1             --

RD[2.2.2.2:1]
ESI         Eth-Tag     Mac-Address         IP-Address   VNID     L3VNID   Nexthop
GW-Type
0                100        0000:0000:cdcd     12.12.12.20    100          0
2.2.2.2             --
0                 200        0000:0b60:25f3     13.13.13.20    200          0
2.2.2.2              --


VTEP-2#show bgp l2vpn evpn mac-ip
RD[1.1.1.1:1]
ESI             Eth-Tag     Mac-Address         IP-Address          VNID      L3VNID
Nexthop         GW-Type
0                100        0000:0000:abab    12.12.12.10       100         0
1.1.1.1             --
0                200        0000:0b60:25f2     13.13.13.10       200         0
1.1.1.1             --

RD[2.2.2.2:1] VRF[vrf_evpn_100]:
ESI               Eth-Tag     Mac-Address         IP-Address       VNID      L3VNID
Nexthop         GW-Type
0                  100        0000:0000:cdcd     12.12.12.20     100         0
2.2.2.2                 --
```

```
0                 100         0000:0b60:25f2      13.13.13.10      100         0
2.2.2.2                   --
```

LAG as Access Port with ECMP on the Network Side

This section contains basic VXLAN EVPN configuration with LAG as an access port and ECMP on the network side.

Topology

The procedures in this section use the topology in Figure 3-74.

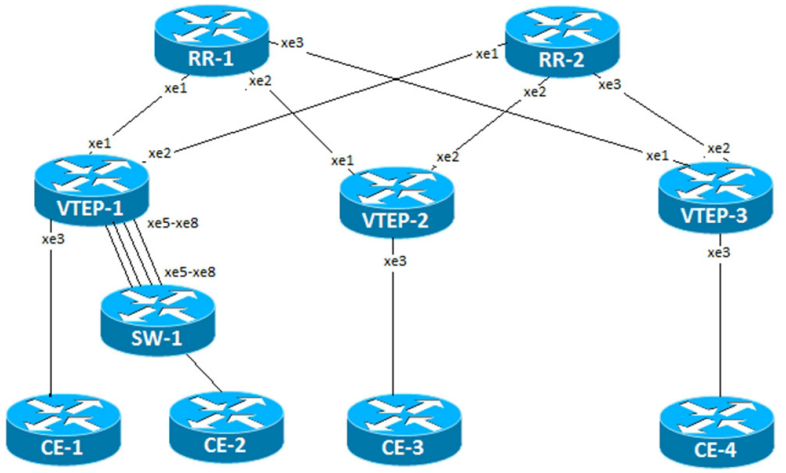


Figure 3-74: VXLAN EVPN with LAG and ECMP

SW-1

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure IEEE vlan bridge
`(config)#vlan database`	Enter into the vlan database
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure vlan 2 and associate with bridge 1
`(config-vlan)#vlan 3 bridge 1 state enable`	Configure vlan 3 and associate with bridge 1
`(config-vlan)#exit`	Exit from the vlan database
`(config)#in xe41`	Enter interface mode
`(config-if)#no shutdown`	Make interface admin up
`(config-if)#switchport`	Set the interface as Layer2 port
`(config-if)#bridge-group 1`	Associate the Interface with bridge-group.
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode
`(config-if)#switchport trunk allowed vlan add 2`	Configure the VLANs that should be allowed through this interface
`(config-if)#switchport trunk allowed vlan add 3`	Configure the VLANs that should be allowed through this interface
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

(config)#interface po1	Enter interface mode
(config-if)#switchport	Set the interface as Layer2 port
(config-if)#exit	Exit interface mode.
(config)#in xe29	Enter interface mode
(config-if)#switchport	Set the interface as Layer2 port
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#exit	Exit interface mode.
(config)#in xe30	Enter interface mode
(config-if)#switchport	Set the interface as Layer2 port
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#exit	Exit interface mode.
(config)#in xe31	Enter interface mode
(config-if)#switchport	Set the interface as Layer2 port
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#exit	Exit interface mode.
(config)#in xe32	Enter interface mode
(config-if)#switchport	Set the interface as Layer2 port
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#exit	Exit interface mode.
(config-if)#inter po1	Enter interface mode
(config-if)#bridge-group 1	Associate the Interface with bridge-group.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode
(config-if)#switchport trunk allowed vlan add 2	Configure the VLANs that should be allowed through this interface
(config-if)#switchport trunk allowed vlan add 3	Configure the VLANs that should be allowed through this interface
(config-if)#exit	Exit interface mode.

VTEP-1

#configure terminal	Enter configure mode
(config)#interface po1	Create interface po1
(config-if)#switchport	Configure the interface as switchport.
(config-if)#exit	Exit interface mode
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode
(config)#interface xe5	Enter interface mode
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1

(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode
(config)#interface xe6	Enter interface mode
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode
(config)#interface xe7	Enter interface mode
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode
(config)#interface xe8	Enter interface mode
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip address 10.1.1.0/31	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 10.1.1.2/31	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 1.1.1.1/32 secondary	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net	Set a Network Entity Title for this instance, specifying the
49.0001.1111.1111.1111.00	area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).

© 2021 IP Infusion Inc. Proprietary

(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 1.1.1.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#load-balance rtag7	Enable load balancing for RTAG7 globally.
(config)#load-balance rtag7 ipv4 src-ipv4	Enable load balancing for RTAG7 for IPv4 for source IP.
(config)#router bgp 65535	Define the routing process. The number 65535 specifies the AS number of VTEP1.
(config-router)#bgp router-id 1.1.1.1	Configure router-id for this BGP process.
(config-router)#neighbor 2.2.2.2 remote-as 65535	Define BGP neighbor: 2.2.2.2 is the IP address of the neighbor (VTEP2), and 65535 is the neighbor's AS number.
(config-router)# neighbor 2.2.2.2 update-source 1.1.1.1	Define BGP neighbor: 1.1.1.1 is the peer interface.
(config-router)#neighbor 3.3.3.3 remote-as 65535	Define BGP neighbor: 3.3.3.3 is the IP address of the neighbor (VTEP3), and 65535 is the neighbor's AS number.
(config-router)# neighbor 3.3.3.3 update-source 1.1.1.1	Define BGP neighbor: 1.1.1.1 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 2.2.2.2 activate	Activate the neighbor at VTEP2 in the EVPN address family.
(config-router-af)#neighbor 3.3.3.3 activate	Activate the neighbor at VTEP3 in the EVPN address family.
(config-router-af)#exit-adress-family	Exit address-family mode.
(config-router)#exit	Exit router mode.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.
(config)#nvo vxlan vtep-ip-global 1.1.1.1	Assign a global IP to the VTEP.
(config)#nvo vxlan id 100001 ingress-replication	Configure a VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf_evpn_100.
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe3 2	Configure access-port xe3 and map vlan 2
(config-nvo-acc-if)#map vnid 100001	Map VNID 100001 to access-port xe3.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan access-if port-vlan po1 2	Configure access-port po1 and map vlan 2
(config-nvo-acc-if)#map vnid 100001	Map VNID 100001 to access-port po1.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.

(config)#nvo vxlan id 200001 ingress-replication	Configure second VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf_evpn_100.
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe3 3	Configure access-port xe3 and map vlan 3
(config-nvo-acc-if)#map vnid 200001	Map VNID 200001 to access-port xe3.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan access-if port-vlan po1 3	Configure access-port po1 and map vlan 3
(config-nvo-acc-if)#map vnid 200001	Map VNID 200001 to access-port xe3.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.

RR-1

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 12.12.12.12/32 secondary	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip address 10.1.1.1/31	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 20.1.1.1/31	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter intereface mode.
(config-if)#ip address 30.1.1.1/31	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.4444.4444.4444.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

(config)#interface xe1	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

RR-2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 13.13.13.13/32 secondary	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip address 10.1.1.3/31	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 20.1.1.3/31	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#ip address 30.1.1.3/31	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.5555.5555.5555.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

(config)#interface xe1	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

VTEP-2

#configure terminal	Enter configure mode
(config)#interface po1	Enter interface mode
(config-if)#switchport	Configure the interface as switchport
(config-if)#exit	Exit interface mode
(config)#interface xe3	Enter interface mode
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip address 20.1.1.0/31	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 20.1.1.2/31	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 2.2.2.2/32 secondary	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.2222.2222.2222.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe1	Enter interface mode.

© 2021 IP Infusion Inc. Proprietary

(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 1.1.1.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#load-balance rtag7	Enable load balancing for RTAG7 globally.
(config)#load-balance rtag7 ipv4 src-ipv4	Enable load balancing for RTAG7 for IPv4 for source IP.
(config)#router bgp 65535	Define the routing process. The number 65535 specifies the AS number of VTEP1.
(config-router)#neighbor 1.1.1.1 remote-as 65535	Define BGP neighbor: 1.1.1.1 is the IP address of the neighbor (VTEP1), and 65535 is the neighbor's AS number.
(config-router)#neighbor 1.1.1.1 update-source 2.2.2.2	Define BGP neighbor: 2.2.2.2 is the peer interface.
(config-router)#neighbor 3.3.3.3 remote-as 65535	Define BGP neighbor: 3.3.3.3 is the IP address of the neighbor (VTEP3), and 65535 is the neighbor's AS number.
(config-router)#neighbor 3.3.3.3 update-source 2.2.2.2	Define BGP neighbor: 2.2.2.2 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor at VTEP1 in the EVPN address family.
(config-router-af)#neighbor 3.3.3.3 activate	Activate the neighbor at VTEP3 in the EVPN address family.
(config-router-af)#exit-adress-family	Exit address-family mode.
(config-router)#exit	Exit router mode.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.
(config)#nvo vxlan vtep-ip-global 2.2.2.2	Assign a global IP to the VTEP.
(config)#nvo vxlan id 100001 ingress-replication	Configure a VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf_evpn_100.
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe3 2	Configure access-port xe3 and map vlan 2
(config-nvo-acc-if)#map vnid 100001	Map VNID 100001 to access-port xe3.

(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan id 200001 ingress-replication	Configure second VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf_evpn_100.
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe3 3	Configure access-port xe3 and map vlan 3
(config-nvo-acc-if)#map vnid 200001	Map VNID 200001 to access-port xe3.
(config-nvo-acc-if)#exit-adress-family	Exit NVO access-if mode.

VTEP-3

#configure terminal	Enter configure mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip address 30.1.1.0/31	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 30.1.1.2/31	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 3.3.3.3/32 secondary	Configure IP address on the loopback interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.3333.3333.3333.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe1	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.

© 2021 IP Infusion Inc. Proprietary

(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 1.1.1.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#load-balance rtag7	Enable load balancing for RTAG7 globally.
(config)#load-balance rtag7 ipv4 src-ipv4	Enable load balancing for RTAG7 for IPv4 for source IP.
(config)#router bgp 65535	Define the routing process. The number 65535 specifies the AS number of VTEP1.
(config-router)#neighbor 1.1.1.1 remote-as 65535	Define BGP neighbor: 1.1.1.1 is the IP address of the neighbor (RR1), and 65535 is the neighbor's AS number.
(config-router)#neighbor 1.1.1.1 update-source 3.3.3.3	Define BGP neighbor: 3.3.3.3 is the peer interface.
(config-router)#neighbor 2.2.2.2 remote-as 65535	Define BGP neighbor: 2.2.2.2 is the IP address of the neighbor (VTEP3), and 65535 is the neighbor's AS number.
(config-router)#neighbor 2.2.2.2 update-source 3.3.3.3	Define BGP neighbor: 3.3.3.3 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor at VTEP1 in the EVPN address family.
(config-router-af)#neighbor 2.2.2.2 activate	Activate the neighbor at VTEP2 in the EVPN address family.
(config-router-af)#exit-adress-family	Exit address-family mode.
(config-router)#exit	Exit router mode.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.
(config)#nvo vxlan vtep-ip-global 3.3.3.3	Assign a global IP to the VTEP.
(config)#nvo vxlan id 100001 ingress-replication	Configure a VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf_evpn_100.
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe3 2	Configure access-port xe3 and map vlan 2
(config-nvo-acc-if)#map vnid 100001	Map VNID 100001 to access-port xe3.
(config-nvo-acc-if)#exit-address-family	Exit NVO access-if mode.
(config)#nvo vxlan id 200001 ingress-replication	Configure second VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf_evpn_100
(config-nvo)#exit	Exit NVO mode.

`(config)#nvo vxlan access-if port-vlan xe3 3`	Configure access-port xe3 and map vlan 3
`(config-nvo-acc-if)#map vnid 200001`	Map VNID 200001 to access-port xe3.
`(config-nvo-acc-if)#exit`	Exit NVO access-if mode.

Validation

CE1, CE2, CE3, and CE4 have hosts configured with MAC addresses, IP addresses, and VLAN identifiers as shown below.

		VLAN	IP Address	MAC Address
VTEP1	CE-1	2	12.12.12.10	0000.0000.aaaa
VTEP1	CE-2	2	12.12.12.20	0000.0000.bbbb
VTEP2	CE-3	2	12.12.12.30	0000.0000.cccc
VTEP3	CE-4	2	12.12.12.40	0000.0000.dddd
VTEP1	CE-1	3	14.14.14.10	0000.058e.2181
VTEP1	CE-2	3	14.14.14.20	0000.058e.2182
VTEP2	CE-3	3	14.14.14.30	0000.058e.2183
VTEP3	CE-4	3	14.14.14.40	0000.058e.2184

Perform a tagged ping of VLAN 2 from CE1 to CE2,CE3 and CE4 and vice-versa. Also perform a tagged ping of VLAN 3 from CE1 to CE2, CE3 and CE4 and vice-versa.

VTEP Tunnel Status

```
VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
1.1.1.1          3.3.3.3          Installed     01:25:20     01:25:20
1.1.1.1          2.2.2.2          Installed     01:35:19     01:35:19
Total number of entries are 2

VTEP2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
2.2.2.2          1.1.1.1          Installed     01:35:42     01:35:42
2.2.2.2          3.3.3.3          Installed     01:25:43     01:25:43
Total number of entries are 2

VTEP3#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
3.3.3.3          2.2.2.2          Installed     01:25:35     01:25:35
```


© 2021 IP Infusion Inc. Proprietary

```
3.3.3.3          1.1.1.1          Installed     01:25:35     01:25:35
Total number of entries are 2
```

VTEP ARP Tables

```
VTEP-1#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
ARP Timeout : 300 sec Random-Jitter-Max : 640
VNID     Ip-Addr           Mac-Addr            Type         Age-Out    Retries-Left
_____________________________________________________________________________________
200      13.13.13.10    0000.0b60.25f2     Dynamic Local        246              2
200      13.13.13.20    0000.0b60.25f3     Dynamic Remote   ------
100      12.12.12.20    0000.0000.cdcd     Dynamic Remote   ------
100      12.12.12.10    0000.0000.abab     Dynamic Local        246              2
Total number of entries are 4


VTEP-2#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
ARP Timeout : 300 sec Random-Jitter-Max : 640
VNID      Ip-Addr          Mac-Addr               Type        Age-Out    Retries-Left
_____________________________________________________________________________________
200     13.13.13.10       0000.0b60.25f2      Dynamic Remote  -------
200      13.13.13.20      0000.0b60.25f3      Dynamic Local      257           2
100     12.12.12.10       0000.0000.abab      Dynamic Remote   -------
100      12.12.12.20      0000.0000.cdcd      Dynamic Local      257            2
Total number of entries are 4


VTEP3#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
100001   12.12.12.30      0000.0000.cccc Dynamic Remote ----
100001   12.12.12.10      0000.0000.aaaa Dynamic Remote ----
100001   12.12.12.20      0000.0000.bbbb Dynamic Remote ----
100001   12.12.12.40      0000.0000.dddd Dynamic Local  ----
200001   14.14.14.20      0000.058e.2182 Dynamic Remote ----
200001   14.14.14.10      0000.058e.2181 Dynamic Remote ----
200001   14.14.14.40      0000.058e.2184 Dynamic Local  ----
200001   14.14.14.30      0000.058e.2183 Dynamic Remote ----
Total number of entries are 8
VTEP3#
```

VTEP MAC Tables

```
VTEP1#show nvo vxlan mac-table
```

```
================================================================================
================================================================================
                              VXLAN MAC Entries
================================================================================
================================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
       Type                  Status              AccessPortDesc
________________________________________________________________________________
________________________________________________________________

1         xe1/1      1000   2000         0000.339a.9abb 33.33.33.0
       Dynamic Local        -------             -------
1         ----       ----   ----         0000.339a.9397 34.34.34.0
       Dynamic Remote       -------             -------

Total number of entries are : 2

VTEP2#show nvo vxlan mac-table
================================================================================
================================================================================
                              VXLAN MAC Entries
================================================================================
================================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
       Type                  Status              AccessPortDesc
________________________________________________________________________________
________________________________________________________________

1         ----       ----   ----         0000.339a.9abb 33.33.33.0
       Dynamic Remote       -------             -------
1         xe1/1      1000   2000         0000.339a.9397 34.34.34.0
       Dynamic Local        -------             -------

Total number of entries are : 2
```

VTEP MAC-IP BGP EVPN Entries

```
VTEP-1#show bgp l2vpn evpn mac-ip
RD[1.1.1.1:1] VRF[vrf_evpn_100]:
ESI               Eth-Tag      Mac-Address           IP-Address     VNID     L3VNID
Nexthop         GW-Type
0                    100        0000:0000:abab     12.12.12.10    100       0
1.1.1.1              --
0                   200        0000:0b60:25f2     13.13.13.10    200       0
1.1.1.1              --

RD[2.2.2.2:1]
ESI          Eth-Tag     Mac-Address         IP-Address   VNID     L3VNID   Nexthop
GW-Type
0                 100        0000:0000:cdcd     12.12.12.20    100           0
2.2.2.2              --
```


© 2021 IP Infusion Inc. Proprietary

```
0                  200        0000:0b60:25f3     13.13.13.20    200           0
2.2.2.2               --


VTEP-2#show bgp l2vpn evpn mac-ip
RD[1.1.1.1:1]
ESI              Eth-Tag     Mac-Address         IP-Address           VNID      L3VNID
Nexthop          GW-Type
0                100         0000:0000:abab     12.12.12.10       100         0
1.1.1.1             --
0                200         0000:0b60:25f2     13.13.13.10       200         0
1.1.1.1             --

RD[2.2.2.2:1] VRF[vrf_evpn_100]:
ESI                Eth-Tag     Mac-Address         IP-Address        VNID      L3VNID
Nexthop          GW-Type
0                  100         0000:0000:cdcd     12.12.12.20     100         0
2.2.2.2                --
0                  100         0000:0b60:25f2     13.13.13.10     100         0
2.2.2.2                --


VTEP-3#show bgp l2vpn evpn mac-ip

RD[1.1.1.1:1] VRF[vrf_evpn_100]:
ESI                          Eth-Tag    Mac-Address    IP-Address
VNID      L3VNID    Nexthop          GW-Type
0                            100001     0000:0000:dddd --
100001    0         3.3.3.3          --
0                           100001     0000:0000:dddd 12.12.12.40
100001    0         3.3.3.3          --
0                            200001     0000:058e:2184 --
200001    0         3.3.3.3          --
0                           200001     0000:058e:2184 14.14.14.40
200001    0         3.3.3.3          --

RD[1.1.1.1:1]
ESI                          Eth-Tag    Mac-Address    IP-Address
VNID      L3VNID    Nexthop          GW-Type
0                            100001     0000:0000:aaaa --
100001    0         1.1.1.1          --
0                           100001     0000:0000:aaaa 12.12.12.10
100001    0         1.1.1.1          --
0                            100001     0000:0000:bbbb --
100001    0         1.1.1.1          --
0                           100001     0000:0000:bbbb 12.12.12.20
100001    0         1.1.1.1          --
0                            100001     0000:0000:cccc --
100001    0         2.2.2.2          --
0                           100001     0000:0000:cccc 12.12.12.30
100001    0         2.2.2.2          --
0                            200001     0000:058e:2181 --
200001    0         1.1.1.1          --
0                           200001     0000:058e:2181 14.14.14.10
200001    0         1.1.1.1          --
```

```
0                          200001     0000:058e:2182 --
200001    0          1.1.1.1          --
0                          200001     0000:058e:2182 14.14.14.20
200001    0          1.1.1.1          --
0                          200001     0000:058e:2183 --
200001    0          2.2.2.2          --
0                          200001     0000:058e:2183 14.14.14.30
200001    0          2.2.2.2          --
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 VXLAN EVPN EVC Configuration

This chapter shows how to configure VXLAN EVPN Ethernet Virtual Circuit (EVC) which embeds the functionality of EVPN-VXLAN access ports to allow EVC frames across VTEPs. With this configuration, customers in the same VLAN can communicate even they are placed across distributed data centers.

Overview

An EVC represents a logical relationship between Ethernet User Network Interface (UNI) in a provider-based Ethernet service. An EVC represents the service offered and is carried through the provider network. Each EVC is configured by a unique name across the provider network.

An EVC is an end–to–end representation of a single instance of a Layer 2 service that a service provider offers. An EVC embodies the different parameters based on which the service is offered. EVC prevents data transfer between sites that are not part of the same EVC.

EVC is an A–Z circuit that enables you to pass customer VLANs from one port on a node to another port on another node in the network. EVC represents a Carrier Ethernet service and is an entity that provides end–to–end connection between two or more customer end points.

Topology



Figure 4-75: VXLAN EVPN EVC

RTR1/VTEP1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 33.33.33.0/31 secondary`	Assign secondary IP address.
`(config-if)#exit`	Exit interface mode.
`(config)#mac vrf vrf1`	Create mac routing/forwarding instance with vrf1 name and enter into VRF mode
`(config-vrf)# rd 100:11`	Assign RD value

`(config-vrf)# route-target export 200:11`	Assign route-target value for export
`(config-vrf)# route-target import 400:11`	Assign route-target value for import
`(config-vrf)#exit`	Exit VRF configuration mode
`(config)#interface xe37`	Enter interface mode for xe37
`(config-if)#ip address 11.11.11.0/31`	Assign IP address in /31 mask.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe15`	Enter interface mode for xe15
`(config-if)#switchport`	Make it L2 interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter BGP router mode
`(config-router)# bgp router-id 1.1.1.1`	Assign BGP router ID
`(config-router)#neighbor 11.11.11.1 remote-as 200`	Specify a neighbor router with peer IP address and remote-as defined
`(config-router)#neighbor 11.11.11.1 fall-over bfd`	Configure single-hop BFD session for its BGP peer
`(config-router)#address-family ipv4 unicast`	Enter into ipv4 unicast address family
`(config-router-af)#network 33.33.33.0/31`	Advertise loopback network into BGP for VTEP ID reachability
`(config-router-af)#exit-address-family`	Exit ipv4 unicast address family mode
`(config-router)#address-family l2vpn evpn`	Enter into l2vpn address family mode
`(config-router-af)#neighbor 11.11.11.1 activate`	Activate the peer into address family mode
`(config-router-af)#exit-address-family`	Exit l2vpn address family mode
`(config-router)#exit`	Exit BGP router mode
`(config)#nvo vxlan enable`	Enable VXLAN
`(config)#nvo vxlan vtep-ip-global 33.33.33.0`	Configure Source vtep-ip-global configuration
`(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled`	Configure VXLAN Network identifier with/without inner-vid-disabled configure and enter into VXLAN tenant mode
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1`	Assign VRF for evpn-bgp to carry EVPN route
`(config-nvo)#exit`	Exit VXLAN tenant mode.
`(config)#nvo vxlan access-if port-vlan xe15 1000 inner-vlan 2000`	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
`(config-nvo-acc-if)#map vnid 1`	Map VXLAN Identified to access-port for VXLAN
`(config-nvo-acc-if)#exit`	Exit VXLAN access-interface mode
`(config)#exit`	Exit configuration mode

RTR2

`#configure terminal`	Enter configure mode.
`(config)#interface xe13/3`	Enter interface mode for xe13/3
`(config-if)#ip address 11.11.11.1/31`	Assign IP address in /31 mask.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe13/1`	Enter interface mode for xe13/1

© 2021 IP Infusion Inc. Proprietary

(config-if)#ip address 12.12.12.1/31	Assign IP address in /31 mask.
(config-if)#exit	Exit interface mode
(config)#router bgp 200	Enter BGP router mode
(config-router)# bgp router-id 2.2.2.2	Assign BGP router ID
(config-router)#neighbor 11.11.11.0 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 11.11.11.0 fall-over bfd	Configure single-hop BFD session for its BGP peer
(config-router)#neighbor 12.12.12.0 remote-as 300	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 12.12.12.0 fall-over bfd	Configure single-hop BFD session for its BGP peer
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 11.11.11.0 activate	Activate the peer into address family mode
(config-router-af)#neighbor 12.12.12.0 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit l2vpn address family mode
(config-router)#exit	Exit BGP router mode

RTR3/VTEP2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode for loopback.
(config-if)#ip address 34.34.34.0/31 secondary	Assign secondary IP address.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf1	Create mac routing/forwarding instance with vrf1 name and enter into vrf mode
(config-vrf)#rd 300:11	Assign RD value
(config-vrf)#route-target export 400:11	Assign route-target value for export
(config-vrf)#route-target import 200:11	Assign route-target value for import
(config-vrf)#exit	Exit vrf configuration mode
(config)#interface xe13	Enter interface mode for xe13
(config-if)#ip address 12.12.12.0/31	Assign IP address in /31 mask.
(config-if)#exit	Exit interface mode.
(config)#interface xe6	Enter interface mode for xe6
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit interface mode.
(config)#router bgp 300	Enter BGP router mode
(config-router)# bgp router-id 3.3.3.3	Assign BGP router ID
(config-router)#neighbor 12.12.12.1 remote-as 200	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 12.12.12.1 fall-over bfd	Configure single-hop BFD session for its BGP peer

© 2021 IP Infusion Inc. Proprietary

(config-router)#address-family ipv4 unicast	Enter into ipv4 unicast address family
(config-router-af)#network 34.34.34.0/31	Advertise loopback network into BGP for VTEP ID reachability
(config-router-af)#exit-address-family	Exit ipv4 unicast address family mode
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 12.12.12.1 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit l2vpn address family mode
(config-router)#exit	Exit BGP router mode
(config)#nvo vxlan enable	Enable VXLAN
(config)#nvo vxlan vtep-ip-global 34.34.34.0	Configure Source vtep-ip-global configuration
(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-vid-disabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign VRF for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit VXLAN tenant mode.
(config)#nvo vxlan access-if port-vlan xe6 1000 inner-vlan 2000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#map vnid 1	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit VXLAN access-interface mode
(config)#exit	Exit configuration mode

Validation

Retaining SVLAN and CVLAN tags across Data Centers

RTR1/VTEP1

```
VTEP1#show running-config nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 33.33.33.0
!
nvo vxlan id 1 ingress-replication inner-vid-disabled
 vxlan host-reachability-protocol evpn-bgp vrf1
!
nvo vxlan access-if port-vlan xe1/1 1000 inner-vlan 2000
 map vnid 1
!
!
VTEP1#show bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 8
2 BGP AS-PATH entries
0 BGP community entries
```


© 2021 IP Infusion Inc. Proprietary

```
Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Dow
n   State/PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
11.11.11.1               4   200   73         73       8      0      0  00:30:41
               2      0      1      1      0      0

Total number of neighbors 1

Total number of Established sessions 1

VTEP1#show bgp l2vpn evpn
BGP table version is 8, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf       Weight     Path
 Peer          Encap

RD[100:11] VRF[vrf1]:
*    [2]:[0]:[1]:[48,0000.339a.9397]:[0]:[1]
                       34.34.34.0           0         100           0       200
300 i  11.11.11.1      VXLAN
*>   [2]:[0]:[1]:[48,0000.339a.9abb]:[0]:[1]
                       33.33.33.0           0         100           32768    i  -
---------      VXLAN
*>   [3]:[1]:[32,33.33.33.1]
33.33.33.0           0        100     32768
i  ----------      VXLAN


*    [3]:[1]:[32,34.34.34.0]
                       34.34.34.0           0         100           0       200
300 i  11.11.11.1      VXLAN

RD[300:11]
*>   [2]:[0]:[1]:[48,0000.339a.9397]:[0]:[1]
                       34.34.34.0           0         100           0       200
300 i  11.11.11.1      VXLAN
*>   [3]:[1]:[32,34.34.34.0]
                       34.34.34.0           0         100           0       200
300 i  11.11.11.1      VXLAN

Total number of prefixes 6
```

```
VTEP1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     11.11.11.0/31 is directly connected, xe10/1, 00:36:00
C     33.33.33.0/31 is directly connected, lo, 00:37:33
B     34.34.34.0/31 [20/0] via 11.11.11.1, xe10/1, 00:27:03
C     127.0.0.0/8 is directly connected, lo, 23:14:51

Gateway of last resort is not set
VTEP1


VTEP1#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
           AC - Access Port
          (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface     ESI
VLAN DF-Status Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________________
1        ----         L2       NW   ----          ------
---- ----      33.33.33.0       34.34.34.0
1        ----         --       AC   xe1/1         --- Single Homed Port ---
1000 ----      ----              ----
 Total number of entries are 2


VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
====
33.33.33.0       34.34.34.0       Installed     00:26:27     00:26:27
Total number of entries are 1
VTEP1#show nvo vxlan mac-table

================================================================================
================================================================
                                                          VXLAN MAC Entries
```


© 2021 IP Infusion Inc. Proprietary

```
================================================================================
================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
       Type                Status             AccessPortDesc
________________________________________________________________________________
________________________________________________________________

1         xe1/1      1000   2000         0000.339a.9abb 33.33.33.0
       Dynamic Local        -------            -------
1         ----       ----   ----         0000.339a.9397 34.34.34.0
       Dynamic Remote       -------            -------

Total number of entries are : 2
VTEP1#
```

RTR3/VTEP2

```
#show running-config nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 34.34.34.0
!
nvo vxlan id 1 ingress-replication  inner-vid-disabled
 vxlan host-reachability-protocol evpn-bgp vrf1
!
nvo vxlan access-if port-vlan xe6 1000 inner-vlan 2000
 map vnid 1
!
VTEP2#show bgp l2vpn evpn summary
BGP router identifier 3.3.3.3, local AS number 300
BGP table version is 7
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Dow
n   State/PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
12.12.12.1               4   200   63         64       7      0      0  00:26:54
               2      0      1      1      0      0

Total number of neighbors 1

Total number of Established sessions 1


VTEP2#show bgp l2vpn evpn
BGP table version is 7, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf       Weight     Path
 Peer          Encap

RD[100:11]
*>   [2]:[0]:[1]:[48,0000.339a.9abb]:[0]:[1]
                      33.33.33.0           0         100           0       200
100 i  12.12.12.1      VXLAN
*>   [3]:[1]:[32,33.33.33.0]
                      33.33.33.0           0         100           0       200
100 i  12.12.12.1      VXLAN


*>   [2]:[0]:[1]:[48,0000.339a.9397]:[0]:[1]
                      34.34.34.0          0         100           32768    i  -
---------      VXLAN
*    [2]:[0]:[1]:[48,0000.339a.9abb]:[0]:[1]
                      33.33.33.0           0         100           0       200
100 i  12.12.12.1      VXLAN
*    [3]:[1]:[32,33.33.33.0]
                      33.33.33.0           0         100           0       200
100 i  12.12.12.1      VXLAN
*>   [3]:[1]:[32,34.34.34.0]
                      34.34.34.0          0         100           32768    i  -
---------      VXLAN

Total number of prefixes 6

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     12.12.12.0/31 is directly connected, xe13, 00:28:41
B     33.33.33.0/31 [20/0] via 12.12.12.1, xe13, 00:26:56
C     34.34.34.0/31 is directly connected, lo, 00:29:36
C     127.0.0.0/8 is directly connected, lo, 00:52:46
```


© 2021 IP Infusion Inc. Proprietary

```
Gateway of last resort is not set

VTEP2#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface     ESI
VLAN DF-Status Src-Addr         Dst-Addr
_____________________________________________________________________________________________
_____________________________________________
1        ----         L2       NW   ----          ------
---- ----      34.34.34.0       33.33.33.0
1        ----         --       AC   xe1/1         --- Single Homed Port ---
1000 ----      ----              ----
 Total number of entries are 2


VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
====
33.33.33.0       34.34.34.0       Installed     00:26:27     00:26:27
Total number of entries are 1


VTEP2#show nvo vxlan mac-table
================================================================================
================================================================
                                                          VXLAN MAC Entries
================================================================================
================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
       Type                Status              AccessPortDesc
_____________________________________________________________________________________
_____________________________________________________________

1         ----       ----   ----         0000.339a.9abb 33.33.33.0
       Dynamic Remote       -------             -------
1         xe6      1000   2000         0000.339a.9397 34.34.34.0
       Dynamic Local        -------             -------

Total number of entries are : 2
#
```

Popping SVLAN and CVLAN Tag

Use the previous configuration on VTEP1 and perform the configuration below on VTEP2.

VTEP2

(config)#nvo vxlan access-if port xe6	Enable port-only mapping for access port
(config-nvo-acc-if)#map vnid 1	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit VXLAN access-interface mode
(config)#exit	Exit configuration mode

RTR3/VTEP2

```
#show nvo vxlan
VXLAN Information
=================
Codes: NW - Network Port
AC - Access Port
(u) - Untagged
VNID VNI-Name VNI-Type Type Interface ESI
VLAN DF-Status Src-Addr Dst-Addr

_____________________________________________________________________________________
1 ---- L2 NW ---- ------
---- ---- 34.34.34.0 33.33.33.0
1 ---- -- AC xe6 --- Single Homed Port ---
---- ---- ---- ----
Total number of entries are 2

VTEP2#show nvo vxlan mac-table
=====================================================================================
=================================================================
                                                          VXLAN MAC Entries
=====================================================================================
=================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
       Type                 Status              AccessPortDesc
_____________________________________________________________________________________
_____________________________________________________________________

1         ----       ----   ----         0000.339a.9abb 33.33.33.0
       Dynamic Remote       -------             -------

Total number of entries are : 1
#
VTEP2#show running-config nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 34.34.34.0
!
```


© 2021 IP Infusion Inc. Proprietary

```
nvo vxlan id 1 ingress-replication inner-vid-disabled
 vxlan host-reachability-protocol evpn-bgp vrf1
!
nvo vxlan access-if port-vlan xe1/1 3000 inner-vlan 2000
 map vnid 1

VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down         Update
================================================================================
====
33.33.33.0       34.34.34.0       Installed     00:26:27     00:26:27
Total number of entries are 1
```

Popping and Later Pushing SVLAN Tag

Use the previous configuration on VTEP1 and perform the configuration below on VTEP2.

`(config)#nvo vxlan access-if port-vlan xe6 3000 inner-vlan 2000`	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
`(config-nvo-acc-if)#map vnid 1`	Map VXLAN Identified to access-port for VXLAN
`(config-nvo-acc-if)#exit`	Exit VXLAN access-interface mode
`(config)#exit`	Exit configuration mode

RTR3/VTEP2

```
#show running-config nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 34.34.34.0
!
nvo vxlan id 1 ingress-replication  inner-vid-disabled
 vxlan host-reachability-protocol evpn-bgp vrf1
!
nvo vxlan access-if port-vlan xe1/1 3000 inner-vlan 2000
 map vnid 1
!
#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface     ESI
VLAN DF-Status Src-Addr         Dst-Addr

_____________________________________________________________________________
1        ----         L2       NW   ----          ------
---- ----      34.34.34.0       33.33.33.0
```

```
1        ----          --       AC   xe6          --- Single Homed Port ---
3000 ----      ----              ----

Total number of entries are 2

#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
34.34.34.0       33.33.33.0       Installed     00:06:48     00:06:48
Total number of entries are 1

VTEP2#show nvo vxlan mac-table
================================================================================
================================================================
                              VXLAN MAC Entries
================================================================================
================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
       Type                  Status              AccessPortDesc
________________________________________________________________________________
________________________________________________________________

1         ----       ----   ----         0000.339a.9abb 33.33.33.0
       Dynamic Remote       -------             -------

Total number of entries are : 1

#
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 VXLAN Hybrid Access Port Configuration

This chapter shows how to configure a hybrid access port which is a Layer 2 Port (configured switchport) that is part of both a VXLAN domain and a Layer 2 bridge with different VLANs.

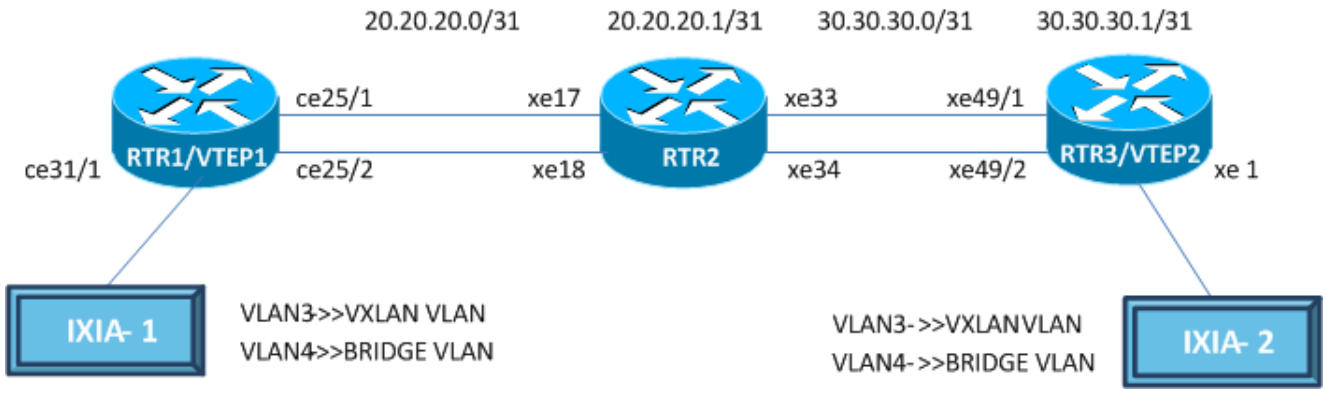
Overview

A hybrid VXLAN access port is Layer 2 port that is part of regular Layer 2 bridge (RSTP/MSTP/STP) and a VXLAN bridge at the same time. A switch port cannot be a part of VXLAN domain and Layer 2 Bridge if the VXLAN port is created with “port only” mapping. The same VLAN cannot be a part of both a VXLAN domain and a Layer 2 bridge.

If a port is created with “all” VLANS, then the port should not allow VXLAN access-port configurations. If a VXLAN with a specific VLAN is mapped, then configuring VLAN “all” on the same port does not allow that specified VLAN in a Layer 2 bridge. If the VXLAN access-port configurations are removed, then the specified VLAN is added immediately in a Layer 2 bridge.

Ingress traffic with a VXLAN VLAN does not receive Layer 2 traffic or vice-versa. STP states on the Port P1 do not affect VXLAN traffic.

Topology



RTR1/VTEP1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode for loopback.
`(config-if)#ip address 10.10.10.10/32 secondary`	Assign secondary IP address.
`(config-if)#exit`	Exit interface mode.
`(config)#mac vrf vrf12345`	Create mac routing/forwarding instance with vrf12345 name and enter VRF mode.
`(config-vrf)#rd 1.1.1.1:1`	Assign Rd value.
`(config-vrf)#route-target both 10.10.10.10:10`	Assign route-target both value.
`(config-vrf)#exit`	Exit VRF configuration mode.
`(config)#bridge 32 protocol ieee vlan-bridge`	Configure the ieee vlan-bridge with Id 32.

© 2021 IP Infusion Inc. Proprietary

(config)#vlan 2-5 bridge 32	Configure the vlans 2-5 for the configured bridge Id 32.
(config)#interface ce25/1	Enter interface mode for ce25/1.
(config-if)#ip address 20.20.20.0/31	Assign IP address 20.20.20.0 in /31 mask.
(config-if)#exit	Exit interface mode.
(config)#interface ce25/2	Enter interface mode for ce25/2.
(config-if)#switchport	Make it L2 interface.
(config-if)#bridge-group 32	Associate the bridge-group 32 to the interface.
(config-if)#switchport mode hybrid	Configure the Hybrid mode.
(config-if)# switchport hybrid allowed vlan add 4 egress-tagged enable	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
(config-if)#exit	Exit interface mode.
(config)#interface ce31/1	Enter interface mode for ce31/1.
(config-if)#switchport	Make it L2 interface.
(config-if)#bridge-group 32	Associate the bridge-group 32 to the interface.
(config-if)#switchport mode hybrid	Configure the Hybrid mode.
(config-if)# switchport hybrid allowed vlan add 4 egress-tagged enable	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
(config-if)#exit	Exit interface mode.
(config)#router bgp 64512	Enter BGP router mode.
(config-router)# bgp router-id 1.1.1.1	Assign BGP router ID
(config-router)#neighbor 20.20.20.1 remote-as 64513	Specify a neighbor router with peer ip address and remote-as defined.
(config-router)#address-family l2vpn evpn	Enter l2vpn address family mode.
(config-router-af)#neighbor 20.20.20.1 activate	Activate the peer into address family mode.
(config-router)#address-family ipv4 unicast	Enter into ipv4 unicast address family
(config-router-af)#network 10.10.10.10/32	Advertise loopback network into BGP for VTEP ID reachability
(config-router-af)#exit-address-family	Exit ipv4 unicast address family mode
(config-router-af)#exit-address-family	Exit l2vpn address family mode.
(config-router)#exit	Exit BGP router mode.
(config)#nvo vxlan enable	Enable Vxlan.
(config)#nvo vxlan vtep-ip-global 10.10.10.10	Configure the source Vtep-ip.
(config)#nvo vxlan id 16777215 ingress-replication inner-vid-disabled	Configure Vxlan Network identifier with/without inner-vid-disabled configure and enter Vxlan tenant mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf12345	Assign VRF for evpn-bgp to carry evpn route.
(config-nvo)#exit	Exit Vxlan tenant mode.
(config)#nvo vxlan access-if port-vlan ce31/1 3	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) mapping.
(config-nvo-acc-if)#map vnid 16777215	Map Vxlan Identifier to access-port.
(config-nvo-acc-if)#exit	Exit Vxlan access-interface mode.

© 2021 IP Infusion Inc. Proprietary

RTR2

`#configure terminal`	Enter configure mode.
`(config)#bridge 32 protocol ieee vlan-bridge`	Configure the ieee vlan-bridge with Id 32.
`(config)#vlan 2-5 bridge 32`	Configure the vlans 2-5 for the configured bridge Id 32.
`(config)#interface xe17`	Enter interface mode for xe17.
`(config-if)#ip address 20.20.20.1/31`	Assign IP address 20.20.20.1 in /31 mask.
`(config-if)#exit`	Exit interface mode.
`(config)#interface  xe18`	Enter interface mode for xe18.
`(config-if)#switchport`	Make it L2 interface .
`(config-if)#bridge-group 32`	Associate the bridge-group 32 to the interface.
`(config-if)#switchport mode hybrid`	Configure the Hybrid mode.
`(config-if)#switchport hybrid allowed vlan add 4 egress-tagged enable`	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
`(config-if)#exit`	Exit interface mode.
`(config)#interface  xe33`	Enter interface mode for xe33.
`(config-if)#ip address 30.30.30.0/31`	Assign IP address 30.30.30.0 in /31 mask.
`(config-if)#exit`	Exit interface mode.
`(config)#interface  xe34`	Enter interface mode for xe34.
`(config-if)#switchport`	Make it L2 interface.
`(config-if)#bridge-group 32`	Associate the bridge-group 32 to the interface.
`(config-if)#switchport mode hybrid`	Configure the Hybrid mode.
`(config-if)#switchport hybrid allowed vlan add 4 egress-tagged enable`	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 64513`	Enter BGP router mode.
`(config-router)#bgp router-id 2.2.2.2`	Assign BGP router ID
`(config-router)#neighbor 20.20.20.0 remote-as 64512`	Specify a neighbor router with peer ip address and remote-as defined.
`(config-router)#neighbor 30.30.30.1 remote-as 64514`	Specify a neighbor router with peer ip address and remote-as defined.
`(config-router)#address-family l2vpn evpn`	Enter l2vpn address family mode.
`(config-router-af)#neighbor 20.20.20.0 activate`	Activate the peer into address family mode.
`(config-router-af)#neighbor 30.30.30.1 activate`	Activate the peer into address family mode.
`(config-router-af)#exit-address-family`	Exit l2vpn address family mode.
`(config-router)#exit`	Exit BGP router mode.

RTR3/VTEP2

`#configure terminal`	Enter configure mode.
`(config)#interface  lo`	Enter interface mode for loopback.

(config-if)#ip address 40.40.40.40/32 secondary	Assign secondary IP address.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf12345	Create mac routing/forwarding instance with vrf12345 name and enter VRF mode.
(config-vrf)#rd 2.2.2.2:2	Assign Rd value.
(config-vrf)#route-target both 10.10.10.10:10	Assign route-target both value.
(config-vrf)#exit	Exit VRF configuration mode.
(config)#bridge 32 protocol ieee vlan-bridge	Configure the ieee vlan-bridge with Id 32.
(config)#vlan 2-5 bridge 32	Configure the vlans 2-5 for the configured bridge Id 32.
(config)#interface xe 49/1	Enter interface mode for xe49/1.
(config-if)#ip address 30.30.30.1/31	Assign Ip address 30.30.30.1 in /31 mask.
(config-if)#exit	Exit interface mode.
(config)#interface xe49/2	Enter interface mode for xe49/2.
(config-if)#switchport	Make it L2 interface .
(config-if)#bridge-group 32	Associate the bridge-group 32 to the interface.
(config-if)#switchport mode hybrid	Configure the Hybrid mode.
(config-if)#switchport hybrid allowed vlan add 4 egress-tagged enable	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode for xe1.
(config-if)#switchport	Make it L2 interface .
(config-if)#bridge-group 32	Associate the bridge-group 32 to the interface.
(config-if)#switchport mode hybrid	Configure the Hybrid mode.
(config-if)#switchport hybrid allowed vlan add 4 egress-tagged enable	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
(config-if)#exit	Exit interface mode.
(config)#router bgp 64514	Enter BGP router mode.
(config-router)# bgp router-id 3.3.3.3	Assign BGP router ID
(config-router)#neighbor 30.30.30.0 remote-as 64513	Specify a neighbor router with peer IP address and remote-as defined.
(config-router)#address-family ipv4 unicast	Enter into ipv4 unicast address family
(config-router-af)#network 40.40.40.40/32	Advertise loopback network into BGP for VTEP ID reachability
(config-router-af)#exit-address-family	Exit ipv4 unicast address family mode
(config-router)#address-family l2vpn evpn	Enter l2vpn address family mode.
(config-router-af)#neighbor 30.30.30.0 activate	Activate the peer into address family mode.
(config-router-af)#exit-address-family	Exit l2vpn address family mode.
(config-router)#exit	Exit BGP router mode.
(config)#nvo vxlan enable	Enable Vxlan.
(config)#nvo vxlan vtep-ip-global 40.40.40.40	Configure the source Vtep-ip.

© 2021 IP Infusion Inc. Proprietary

(config)#nvo vxlan id 16777215 ingress-replication inner-vid-disabled	Configure Vxlan Network identifier with/without inner-vid-disabled configure and enter Vxlan tenant mode.
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf12345	Assign VRF for evpn-bgp to carry evpn route.
(config-nvo)#exit	Exit Vxlan tenant mode.
(config)#nvo vxlan access-if port-vlan xe1 3	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) mapping.
(config-nvo-acc-if)#map vnid 16777215	Map Vxlan Identifier to access-port.
(config-nvo-acc-if)#exit	Exit Vxlan access-interface mode.

Validation

VTEP1

```
#show running-config nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 10.10.10.10
!
nvo vxlan id 16777215 ingress-replication inner-vid-disabled
 vxlan host-reachability-protocol evpn-bgp vrf12345
!
nvo vxlan access-if port-vlan ce31/1 3
 map vnid 16777215
!

VTEP1#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface     ESI                             VLAN DF-
Status Src-Addr         Dst-Addr

_____________________________________________________________________________________
_____________________________________
16777215 ----         L2       NW   ----          ------                          ---- --
--      10.10.10.10      40.40.40.40
16777215 ----         --       AC   ce31/1         --- Single Homed Port ---     3    -
---      ----             ----
 Total number of entries are 2


VTEP1#show nvo vxlan vnid 16777215
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
```

```
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface     ESI                             VLAN DF-
Status Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________
16777215 ----         L2       NW   ----          ------                          ---- --
--      10.10.10.10      40.40.40.40
16777215 ----         --       AC   ce31/1         --- Single Homed Port ---     3    -
---      ----            ----
 Total number of entries are 2!

VTEP1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C     10.10.10.10/32 is directly connected, lo, 01:15:55
C     20.20.20.0/31 is directly connected, xe10/1, 01:07:53
B     40.40.40.40/32 [20/0] via 20.20.20.1, xe10/1, 00:42:54
C     127.0.0.0/8 is directly connected, lo, 1d05h02m

Gateway of last resort is not set


VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
33.33.33.0       34.34.34.0       Installed     00:26:27     00:26:27
Total number of entries are 1


VTEP1#show bgp l2vpn evpn summary
BGP router identifier 10.10.10.2, local AS number 64512
BGP table version is 10
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
20.20.20.1              4 64513  108       109     10      0     0  00:48:14
3      0      2      1       0       0

Total number of neighbors 1
```


© 2021 IP Infusion Inc. Proprietary

```
Total number of Established sessions 1

VTEP1#show bgp l2vpn evpn
BGP table version is 4, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

   Network         Next Hop           Metric    LocPrf      Weight     Path  Peer
Encap

RD[1.1.1.1:1] VRF[vrf12345]:
*    [2]:[0]:[16777215]:[48,0000.0744.4433]:[0]:[16777215]
                       40.40.40.40          0         100           0       64513 64514
i  20.20.20.1      VXLAN
*>   [2]:[0]:[16777215]:[48,0000.2222.2222]:[0]:[16777215]
                       10.10.10.10          0         100           32768    i  --------
--      VXLAN
*>   [3]:[16777215]:[32,10.10.10.10]
                       10.10.10.10          0         100           32768    i  --------
--      VXLAN
*    [3]:[16777215]:[32,40.40.40.40]
                       40.40.40.40          0         100           0       64513 64514
i  20.20.20.1      VXLAN

RD[2.2.2.2:2]
*>   [2]:[0]:[16777215]:[48,0000.0744.4433]:[0]:[16777215]
                       40.40.40.40          0         100           0       64513 64514
i  20.20.20.1      VXLAN
*>   [3]:[16777215]:[32,40.40.40.40]
                       40.40.40.40          0         100           0       64513 64514
i  20.20.20.1      VXLAN

Total number of prefixes 6

VTEP1#show nvo vxlan mac-table
================================================================================================
============================================================
                                VXLAN MAC Entries
================================================================================================
============================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc

________________________________________________________________________________________________
____________________________________________________________
```

```
16777215  ce31/1      3      ----         0000.2222.2222 10.10.10.10
Dynamic Local        -------              -------
16777215  ----       ----   ----          0000.0744.4433 40.40.40.40
Dynamic Remote       -------              -------

Total number of entries are : 2

VTEP1#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
Total number of entries are 0

VTEP1#show vlan brief
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                         (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
32      1       default          ACTIVE  Success    ce25/2(u) ce31/1(u)
32      2       VLAN0002         ACTIVE  Success
32      3       VLAN0003         ACTIVE  Success
32      4       VLAN0004         ACTIVE  Success    ce25/2(t) ce31/1(t)
32      5       VLAN0005         ACTIVE  Success
```

RTR2

```
RTR2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
B     10.10.10.10/32 [20/0] via 20.20.20.0,  xe17, 00:29:48
C     20.20.20.0/31 is directly connected,  xe17, 02:33:29
C     30.30.30.0/31 is directly connected, xe33, 02:31:56
B     40.40.40.40/32 [20/0] via 30.30.30.1, xe33, 02:23:26
C     127.0.0.0/8 is directly connected, lo, 21:17:41

Gateway of last resort is not set


RTR2#show bgp l2vpn evpn summary
BGP router identifier 11.11.11.1, local AS number 64513
BGP table version is 10
2 BGP AS-PATH entries
0 BGP community entries
```

 © 2021 IP Infusion Inc. Proprietary

```
Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
20.20.20.0              4 64512  111       112     10      0      0  00:49:36
3      0      2      1      0      0
30.30.30.1              4 64514  101       103     10      0      0  00:45:10
3      0      2      1      0      0

Total number of neighbors 2

Total number of Established sessions 2


#show nvo vxlan vnid 16777215
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface     ESI                             VLAN DF-
Status Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________
16777215 ----          L2       NW   ----          ------                          ---- --
--      40.40.40.40      10.10.10.10
16777215 ----        --      AC   xe1        --- Single Homed Port ---     3    ----
----             ----
 Total number of entries are 2


RTR2#show vlan brief
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                         (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
32      1       default          ACTIVE  Success    ce10/2(u) ce11/2(u)
32      2       VLAN0002         ACTIVE  Success
32      3       VLAN0003         ACTIVE  Success
32      4       VLAN0004         ACTIVE  Success    ce10/2(t) ce11/2(t)
32      5       VLAN0005         ACTIVE  Success
```

VTEP2

```
#show running-config nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 40.40.40.40
!
nvo vxlan id 16777215 ingress-replication inner-vid-disabled
 vxlan host-reachability-protocol evpn-bgp vrf12345
```

```
!
nvo vxlan access-if port-vlan xe1 3
 no shutdown
 map vnid 16777215
!

VTEP2#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name   VNI-Type Type Interface    ESI  VLAN DF-Status Src-Addr   Dst-Addr
_____________________________________________________________________________________
_____________________________________
16777215 ----         L2       NW   ----          ------                         ---- --
--      40.40.40.40      10.10.10.10
16777215 ----        --      AC   xe1        --- Single Homed Port ---     3    ----
----             ----
 Total number of entries are 2

VTEP2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
B     10.10.10.10/32 [20/0] via 30.30.30.0, xe11/1, 00:27:32
C     30.30.30.0/31 is directly connected, xe11/1, 00:30:00
C     40.40.40.40/32 is directly connected, lo, 00:31:00
C     127.0.0.0/8 is directly connected, lo, 06:25:00

Gateway of last resort is not set


VTEP2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
40.40.40.40      10.10.10.10      Installed     00:14:40     00:14:40
Total number of entries are 1


VTEP2#show bgp l2vpn evpn summary
BGP router identifier 33.33.33.33, local AS number 64514
```


© 2021 IP Infusion Inc. Proprietary

```
BGP table version is 8
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
30.30.30.0              4 64513  267       270      8     0     0  02:09:07
2      0      1      1      0      0

Total number of neighbors 1

Total number of Established sessions 1

VTEP2#show nvo vxlan access-if-config
nvo vxlan access-if port-vlan xe1/1 3
 no shutdown
 map vnid 16777215
!

VTEP2#show bgp l2vpn evpn
BGP table version is 8, local router ID is 40.40.40.40
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

   Network         Next Hop           Metric    LocPrf      Weight     Path  Peer
Encap

RD[1.1.1.1:1]
*>   [2]:[0]:[16777215]:[48,0000.2222.2222]:[0]:[16777215]
                       10.10.10.10          0         100           0       64513 64512
i  30.30.30.0      VXLAN
*>   [3]:[16777215]:[32,10.10.10.10]
                       10.10.10.10          0         100           0       64513 64512
i  30.30.30.0      VXLAN

RD[2.2.2.2:2] VRF[vrf12345]:
*>   [2]:[0]:[16777215]:[48,0000.0744.4433]:[0]:[16777215]
                       40.40.40.40          0         100           32768    i  --------
--      VXLAN
*    [2]:[0]:[16777215]:[48,0000.2222.2222]:[0]:[16777215]
                       10.10.10.10          0         100           0       64513 64512
i  30.30.30.0      VXLAN
*    [3]:[16777215]:[32,10.10.10.10]
```

```
                       10.10.10.10          0         100           0       64513 64512
i  30.30.30.0      VXLAN
*>   [3]:[16777215]:[32,40.40.40.40]
                       40.40.40.40          0         100           32768    i  --------
--      VXLAN

Total number of prefixes 6


VTEP2#show nvo vxlan mac-table
================================================================================================
============================================================
                                    VXLAN MAC Entries
================================================================================================
============================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
________________________________________________________________________________________________
________________________________________________________________

16777215  ----       ----   ----         0000.2222.2222 10.10.10.10
Dynamic Remote       -------             -------
16777215  xe1      3      ----         0000.0744.4433 40.40.40.40
Dynamic Local        -------             -------

Total number of entries are : 2

VTEP2#show vlan brief
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                         (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
32      1       default          ACTIVE  Success    xe1(u) xe49/2(u)
32      2       VLAN0002         ACTIVE  Success
32      3       VLAN0003         ACTIVE  Success
32      4       VLAN0004         ACTIVE  Success    xe1(t) xe49/2(t)
32      5       VLAN0005         ACTIVE  Success

VTEP2#
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 6 VXLAN Multi-homing Configuration

This chapter contains the configurations for VXLAN Multi-homing feature.

Overview

VXLAN EVPN Multi-homing features enables to connect a CE/Host node to two VTEPs with all-active redundancy mode.EVPN Multi-homing helps in VTEP to host failure and VTEP failure. If one VTEP goes down, other will forward the entire traffic.

Below are Multi-homing concepts:

- Ethernet Segment: Set of links which connect host/CE to two active-active multi-homed VTEP (only two VTEPs are supported) which appears as LACP link for host.
- Ethernet Segment Identifier: Ethernet Segment Identifier (ESI) which is an 10 octet-value, which can be configured in two ways, system mac is configured as esi in case of Dynamic Lag and 10-octet ESI format config is used on physical interface ES.
- Ethernet Segment Route (ES route): When a multi-homed CE is configured as an VXLAN access-port, Ethernet segment route is sent. The main purpose of this route is to discover other VTEPs which share the ES and to perform DF election.
- Ethernet A-D route per ESI: This route is used for Fast Convergence and Split Horizon.
- Ethernet A-D route per EVI: This route is used for load sharing between DF and NON-DF by the remote VTEPs

Topology

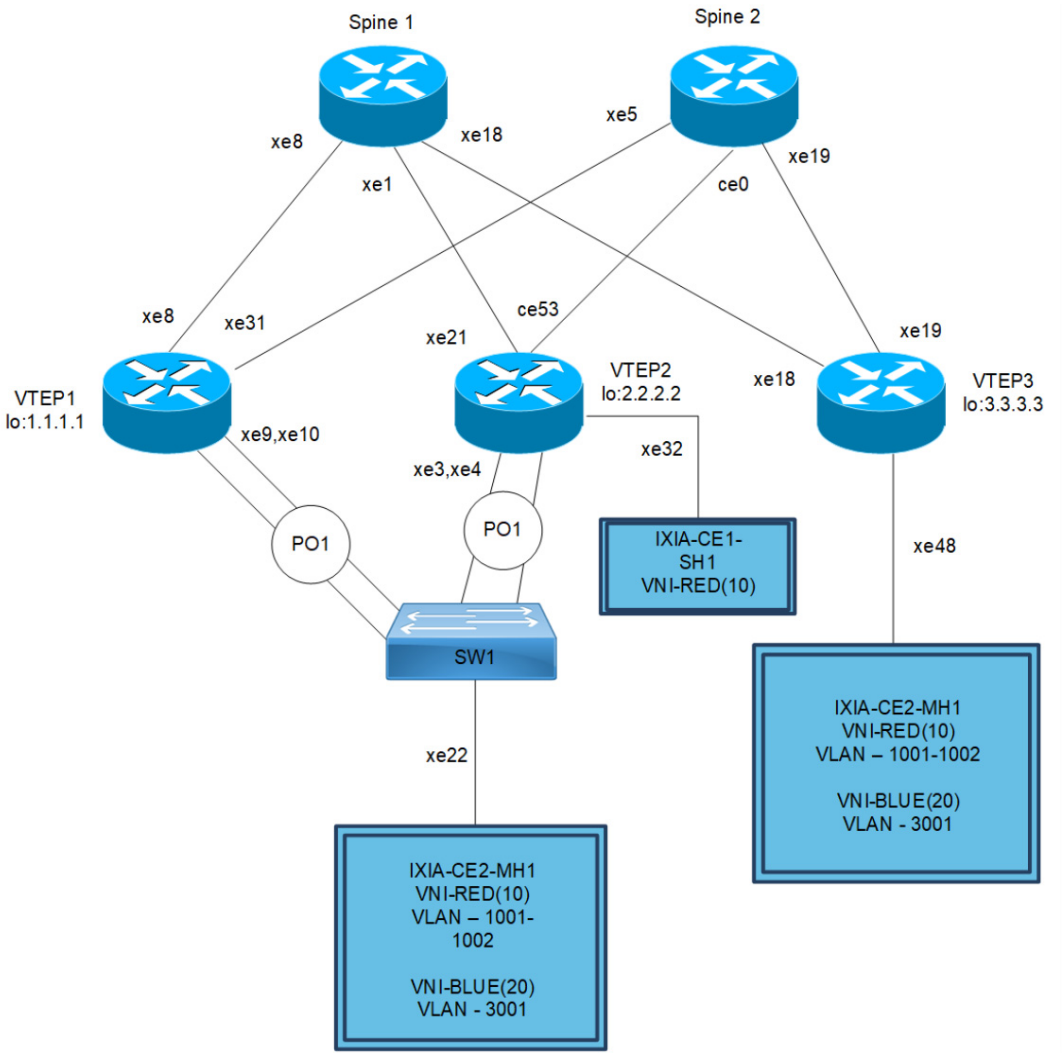


Figure 6-76: VxLAN-Multihoming

Configurations

VXLAN-EVPN MH Configuration

ESI can be configured in below two ways

Ethernet Segment through Dynamic Lag interface

`#configure terminal`	Enter configure mode.
`(config)#interface po1`	Enter interface mode for po1

© 2021 IP Infusion Inc. Proprietary

(config-if)#switchport	Make it L2 interface
(config-if)#evpn multi-homed system-mac 8899.4400.6745	Configure system mac as ESI value for Lag (po1) interface
(config-if)#exit	Exit interface mode.

OR

Ethernet Segment through Physical interface

#configure terminal	Enter configure mode.
(config)#interface xe41	Enter interface mode for xe41
(config-if)#switchport	Make it L2 interface
(config-if)# evpn multi-homed esi 00:01:02:03:04:05:06:07:08	Configure 9-octet ESI value for xe41 interface (in static config, out of 10-octet ESI value, first octet is reserved)
(config-if)#exit	Exit interface mode.

VTEP1

(Multi-homed group1) – Part of both Multi-homed with po1 (MH1)

Generic Configuration

`#configure terminal`	Enter Configure mode.
`(config)#evpn vxlan multihoming enable`	Enable Multihoming, save configs and reboot the board for multihoming to be effective
`(config)#qos enable`	Enabling QoS

Interface and Loopback Configuration

`(config)#interface po1`	Enter Interface mode for po1 (MH1)
`(config-if)#switchport`	Make it L2 interface
`(config-if)# evpn multi-homed system-mac 0000.0000.1111`	Configure system MAC as ESI value for LAG (po1) interface
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe9`	Enter Interface mode for xe9
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe10`	Enter Interface mode for xe10
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface lo`	Enter Interface mode for lo
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure loopback ip address as 1.1.1.1 for VTEP1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe8`	Enter Interface mode for xe8
`(config-if)#ip address 10.10.10.1/24`	Configure IP address as 10.10.10.1 on network side of Spine1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe31`	Enter Interface mode for xe31
`(config-if)#ip address 20.20.20.1/24`	Configure IP address as 20.20.20.1 on network side of Spine2
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

OSPF Configuration

`(config)#router ospf 100`	Enter into router OSPF mode
`(config-router)#ospf router-id 1.1.1.1`	Configure router-id as 1.1.1.1 (lo ip address)
`(config-router)#network 1.1.1.1/32 area 0.0.0.0`	Add 1.1.1.1 (lo IP address) network into area 0
`(config-router)#network 10.10.10.0/24 area 0.0.0.0`	Add 10.10.10.0 (Spine1) network into area 0
`(config-router)#network 20.20.20.0/24 area 0.0.0.0`	Add 20.20.20.0 (Spine2) network into area 0
`(config-router)#bfd all-interfaces`	Enabling BFD on all OSPF interface for fast convergence
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

© 2021 IP Infusion Inc. Proprietary

BGP Configuration

`(config)#router bgp 500`	Enter into Router BGP mode
`(config-router)#bgp router-id 1.1.1.1`	Configure router-id as 1.1.1.1 (lo IP address)
`(config-router)#neighbor 2.2.2.2 remote-as 500`	Specify a VTEP2 loopback IP address and remote-as defined
`(config-router)#neighbor 2.2.2.2 update-source lo`	Configure update as loopback for VTEP2
`(config-router)#neighbor 2.2.2.2 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for VTEP2
`(config-router)#neighbor 3.3.3.3 remote-as 500`	Specify a VTEP3 loopback IP address and remote-as defined
`(config-router)#neighbor 3.3.3.3 update-source lo`	Configure update as loopback for VTEP3
`(config-router)#neighbor 3.3.3.3 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for VTEP3
`(config-router)#address-family ipv4 unicast`	Enter into ipv4 unicast address family mode
`(config-router-af)#network 1.1.1.1/32`	Advertise loopback network into BGP for VTEP ID reachability
`(config-router-af)#neighbor 2.2.2.2 activate`	Activate 2.2.2.2 (VTEP2) into ipv4 unicast address family mode
`(config-router-af)#neighbor 3.3.3.3 activate`	Activate 3.3.3.3 (VTEP2) into ipv4 unicast address family mode
`(config-router-af)#exit-address-family`	Exit from ipv4 unicast address family mode
`(config-router)#address-family l2vpn evpn`	Enter into L2VPN EVPN address family mode
`(config-router-af)#neighbor 2.2.2.2 activate`	Activate 2.2.2.2 (VTEP2) into L2VPN evpn address family mode
`(config-router-af)#neighbor 3.3.3.3 activate`	Activate 3.3.3.3 (VTEP3) into L2VPN evpn address family mode
`(config-router-af)#exit-address-family`	Exit from L2VPN address family mode
`(config-router)#exit`	Exit from Router BGP mode and enter into config mode

VRF Configuration

`(config)#mac vrf VRF1`	Create mac routing/forwarding instance with VRF1 name and enter into VRF mode
`(config-vrf)#rd 1.1.1.1:11`	Assign RD value
`(config-vrf)#route-target both 9.9.9.9:100`	Assign route-target value for same for import and export. Should be same on all node for VRF1
`(config-vrf)#exit`	Exit from VRF mode
`(config)#mac vrf VRF2`	Create MAC routing/forwarding instance with VRF1 name and enter into VRF mode
`(config-vrf)#rd 1.1.1.1:21`	Assign RD value
`(config-vrf)#route-target both 90.90.90.90:100`	Assign route-target value for same for import and export
`(config-vrf)#exit`	Exit from VRF mode

VxLAN Configuration

`(config)#nvo vxlan enable`	Enable VxLAN
`(config)#evpn esi hold-time 90`	Configure ESI hold time to allow tunnel to come up at the time of VxLAN initialization before making the ESI up
`(config)#nvo vxlan vtep-ip-global 1.1.1.1`	Configure Source VTEP-IP-global configuration
`(config)#nvo vxlan id 10 ingress-replication inner-vid-disabled`	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF1`	Assign VRF for EVPN-BGP to carry EVPN route
`(config-nvo)#vni-name VNI-RED`	Configure VNI-name as VNI-RED
`(config-nvo)#exit`	Exit from VxLAN tenant mode and enter into configuration mode.
`(config)#nvo vxlan id 20 ingress-replication inner-vid-disabled`	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF2`	Assign VRF for EVPN-BGP to carry EVPN route
`(config-nvo)#vni-name VNI-BLUE`	Configure VNI-name as VNI-BLUE
`(config-nvo)#exit`	Exit from VxLAN tenant mode and enter into configuration mode.
`(config)#nvo vxlan access-if port-vlan po1 1001`	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
`(config-nvo-acc-if)#map vni-name VNI-RED`	Map VxLAN Identified to access-port for VxLAN
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-interface mode and enter into configuration mode
`(config)#nvo vxlan access-if port-vlan po1 1002`	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
`(config-nvo-acc-if)#map vni-name VNI-RED`	Map VxLAN Identified to access-port for VxLAN
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-interface mode and enter into configuration mode
`(config)#nvo vxlan access-if port-vlan po1 3001`	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
`(config-nvo-acc-if)#map vni-name VNI-BLUE`	Map VxLAN Identified to access-port for VxLAN
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-interface mode and enter into configuration mode
`(config)#exit`	Exit from configuration mode

VTEP2

(Multi-homed group1) – Part of both Multi-homed with p01. And it has xe32 as single home access-if port (SH2)

© 2021 IP Infusion Inc. Proprietary

Generic Configuration

`#configure terminal`	Enter Configure mode.
`(config)#evpn vxlan multihoming enable`	Enable Multihoming, save configs and reboot the board for multihoming to be effective
`(config)#qos enable`	Enabling QoS

Interface and Loopback Configuration

`(config)#interface po1`	Enter Interface mode for po1 (MH1)
`(config-if)#switchport`	Make it L2 interface
`(config-if)# evpn multi-homed system-mac 0000.0000.1111`	Configure system MAC as ESI value for LAG (po1) interface
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe3`	Enter Interface mode for xe3
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe4`	Enter Interface mode for xe4
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe32`	Enter Interface mode for xe32 (SH2)
`(config-if)#switchport`	Make it L2 interface
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface lo`	Enter Interface mode for lo
`(config-if)#ip address 2.2.2.2/32 secondary`	Configure loopback IP address as 2.2.2.2 for VTEP2
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe21`	Enter Interface mode for xe21
`(config-if)#ip address 30.30.30.1/24`	Configure IP address as 30.30.30.1 on network side of Spine1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface ce53`	Enter Interface mode for ce53
`(config-if)#ip address 40.40.40.1/24`	Configure IP address as 40.40.40.1 on network side of Spine2
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

OSPF Configuration

`(config)#router ospf 100`	Enter into router OSPF mode
`(config-router)#ospf router-id 2.2.2.2`	Configure router-id as 2.2.2.2 (lo IP address)
`(config-router)#network 2.2.2.2/32 area 0.0.0.0`	Add 2.2.2.2 (lo IP address) network into area 0
`(config-router)#network 30.30.30.0/24 area 0.0.0.0`	Add 30.30.30.0 (Spine1) network into area 0
`(config-router)#network 40.40.40.0/24 area 0.0.0.0`	Add 40.40.40.0 (Spine2) network into area 0
`(config-router)#bfd all-interfaces`	Enabling BFD on all OSPF interface for fast convergence
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

BGP Configuration

`(config)#router bgp 500`	Enter into Router BGP mode
`(config-router)#bgp router-id 2.2.2.2`	Configure router-id as 2.2.2.2 (lo IP address)
`(config-router)#neighbor 1.1.1.1 remote-as 500`	Specify a VTEP1 loopback IP address and remote-as defined
`(config-router)#neighbor 1.1.1.1 update-source lo`	Configure update as loopback for VTEP1
`(config-router)#neighbor 1.1.1.1 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for VTEP1
`(config-router)#neighbor 3.3.3.3 remote-as 500`	Specify a VTEP3 loopback IP address and remote-as defined
`(config-router)#neighbor 3.3.3.3 update-source lo`	Configure update as loopback for VTEP3
`(config-router)#neighbor 3.3.3.3 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for VTEP3
`(config-router)#address-family ipv4 unicast`	Enter into ipv4 unicast address family mode
`(config-router-af)#network 2.2.2.2/32`	Advertise loopback network into BGP for VTEP ID reachability
`(config-router-af)#neighbor 1.1.1.1 activate`	Activate 1.1.1.1 (VTEP2) into ipv4 unicast address family mode
`(config-router-af)#neighbor 3.3.3.3 activate`	Activate 3.3.3.3 (VTEP2) into ipv4 unicast address family mode
`(config-router-af)#exit-address-family`	Exit from ipv4 unicast address family mode
`(config-router)#address-family l2vpn evpn`	Enter into L2VPN EVPN address family mode
`(config-router-af)#neighbor 1.1.1.1 activate`	Activate 1.1.1.1(VTEP1) into L2VPN evpn address family mode
`(config-router-af)#neighbor 3.3.3.3 activate`	Activate 3.3.3.3(VTEP3) into L2VPN evpn address family mode
`(config-router-af)#exit-address-family`	Exit from L2VPN address family mode
`(config-router)#exit`	Exit from Router BGP mode and enter into config mode

© 2021 IP Infusion Inc. Proprietary

VRF Configuration

`(config)# mac vrf VRF1`	Create mac routing/forwarding instance with VRF1 name and enter into VRF mode
`(config-vrf)#rd 2.2.2.2:11`	Assign RD value
`(config-vrf)#route-target both 9.9.9.9:100`	Assign route-target value for same for import and export. Should be same on all node for VRF1
`(config-vrf)#exit`	Exit from VRF mode
`(config)#mac vrf VRF2`	Create MAC routing/forwarding instance with VRF1 name and enter into VRF mode
`(config-vrf)#rd 2.2.2.2:21`	Assign RD value
`(config-vrf)#route-target both 90.90.90.90:100`	Assign route-target value for same for import and export
`(config-vrf)#exit`	Exit from VRF mode

VxLAN Configuration

`(config)#nvo vxlan enable`	Enable VxLAN
`(config)#evpn esi hold-time 90`	Configure ESI hold time to allow tunnel to come up at the time of VxLAN initialization before making the ESI up
`(config)#nvo vxlan vtep-ip-global 2.2.2.2`	Configure Source VTEP-IP-global configuration
`(config)#nvo vxlan id 10 ingress-replication inner-vid-disabled`	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF1`	Assign VRF for EVPN-BGP to carry EVPN route
`(config-nvo)#vni-name VNI-RED`	Configure VNI-name as VNI-RED
`(config-nvo)#exit`	Exit from VxLAN tenant mode and enter into configuration mode.
`(config)#nvo vxlan id 20 ingress-replication inner-vid-disabled`	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF2`	Assign VRF for EVPN-BGP to carry EVPN route
`(config-nvo)#vni-name VNI-BLUE`	Configure VNI-name as VNI-BLUE
`(config-nvo)#exit`	Exit from VxLAN tenant mode and enter into configuration mode.
`(config)#nvo vxlan access-if port-vlan po1 1001`	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
`(config-nvo-acc-if)#map vni-name VNI-RED`	Map VxLAN Identified to access-port for VxLAN
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-interface mode and enter into configuration mode
`(config)#nvo vxlan access-if port-vlan po1 1002`	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
`(config-nvo-acc-if)#map vni-name VNI-RED`	Map VxLAN Identified to access-port for VxLAN
`(config-nvo-acc-if)#exit`	Exit from VXLAN access-interface mode and enter into configuration mode
`(config)#nvo vxlan access-if port-vlan po1 3001`	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
`(config-nvo-acc-if)#map vni-name VNI-BLUE`	Map VxLAN Identified to access-port for VxLAN

(config-nvo-acc-if)#exit	Exit from VxLAN access-interface mode and enter into configuration mode
(config)#nvo vxlan access-if port xe32	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
(config-nvo-acc-if)#map vni-name VNI-RED	Map VxLAN Identified to access-port for VxLAN
(config-nvo-acc-if)#exit	Exit from VxLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

VTEP3

It has xe48 as Single home access-if port (SH2)

Generic Configuration

#configure terminal	Enter Configure mode.
(config)#evpn vxlan multihoming enable	Enable Multihoming, save configs and reboot the board for multihoming to be effective
(config)#qos enable	Enabling QoS

Interface and loopback configuration

(config)#interface xe48	Enter Interface mode for xe48 (SH3)
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface lo	Enter Interface mode for lo
(config-if)#ip address 3.3.3.3/32 secondary	Configure loopback IP address as 3.3.3.3 for VTEP3
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe18	Enter Interface mode for xe18
(config-if)#ip address 50.50.50.1/24	Configure IP address as 50.50.50.1 on network side of Spine1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe19	Enter Interface mode for xe19
(config-if)#ip address 60.60.60.1/24	Configure IP address as 60.60.60.1 on network side of Spine2
(config-if)#exit	Exit Interface mode and return to Configure mode.

OSPF Configuration

(config)#router ospf 100	Enter into router OSPF mode
(config-router)#ospf router-id 3.3.3.3	Configure router-ID as 3.3.3.3 (lo IP address)
(config-router)#network 3.3.3.3/32 area 0.0.0.0	Add 3.3.3.3 (lo IP address) network into area 0
(config-router)#network 50.50.50.0/24 area 0.0.0.0	Add 50.50.50.0 (Spine1) network into area 0
(config-router)#network 60.60.60.0/24 area 0.0.0.0	Add 60.60.60.0 (Spine2) network into area 0

© 2021 IP Infusion Inc. Proprietary

(config-router)#bfd all-interfaces	Enabling BFD on all OSPF interface for fast convergence
(config-if)#exit	Exit Interface mode and return to Configure mode.

BGP Configuration

(config)#router bgp 500	Enter into Router BGP mode
(config-router)#bgp router-id 3.3.3.3	Configure router-ID as 3.3.3.3 (lo ip address)
(config-router)#neighbor 1.1.1.1 remote-as 500	Specify a VTEP1 loopback IP address and remote-as defined
(config-router)#neighbor 1.1.1.1 update-source lo	Configure update as loopback for VTEP1
(config-router)#neighbor 1.1.1.1 advertisement-interval 0	Configure advertisement-interval as 0 for fast convergence for VTEP1
(config-router)#neighbor 2.2.2.2 remote-as 500	Specify a VTEP2 loopback IP address and remote-as defined
(config-router)#neighbor 2.2.2.2 update-source lo	Configure update as loopback for VTEP2
(config-router)#neighbor 2.2.2.2 advertisement-interval 0	Configure advertisement-interval as 0 for fast convergence for VTEP3
(config-router)#address-family ipv4 unicast	Enter into ipv4 unicast address family mode
(config-router-af)#network 3.3.3.3/32	Advertise loopback network into BGP for VTEP ID reachability
(config-router-af)#neighbor 1.1.1.1 activate	Activate 1.1.1.1 (VTEP2) into ipv4 unicast address family mode
(config-router-af)#neighbor 2.2.2.2 activate	Activate 2.2.2.2 (VTEP2) into ipv4 unicast address family mode
(config-router-af)#exit-address-family	Exit from ipv4 unicast address family mode
(config-router)#address-family l2vpn evpn	Enter into L2VPN EVPN address family mode
(config-router-af)#neighbor 1.1.1.1 activate	Activate 1.1.1.1 (VTEP1) into L2VPN evpn address family mode
(config-router-af)#neighbor 2.2.2.2 activate	Activate 2.2.2.2 (VTEP2) into L2VPN evpn address family mode
(config-router-af)#exit-address-family	Exit from L2VPN address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode

VRF Configuration

`(config)# mac vrf VRF1`	Create MAC routing/forwarding instance with VRF1 name and enter into VRF mode
`(config-vrf)#rd 3.3.3.3:11`	Assign RD value
`(config-vrf)#route-target both 9.9.9.9:100`	Assign route-target value for same for import and export. Should be same on all node for VRF1
`(config-vrf)#exit`	Exit from VRF mode
`(config)#mac vrf VRF2`	Create MAC routing/forwarding instance with VRF2 name and enter into VRF mode
`(config-vrf)#rd 3.3.3.3:21`	Assign RD value
`(config-vrf)#route-target both 90.90.90.90:100`	Assign route-target value for same for import and export
`(config-vrf)#exit`	Exit from VRF

© 2021 IP Infusion Inc. Proprietary

VxLAN Configuration

`(config)#nvo vxlan enable`	Enable VxLAN
`(config)#nvo vxlan vtep-ip-global 3.3.3.3`	Configure Source VTEP-IP-global configuration
`(config)#nvo vxlan id 10 ingress-replication inner-vid-disabled`	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF1`	Assign VRF for EVPN-BGP to carry EVPN route
`(config-nvo)#vni-name VNI-RED`	Configure VNI-name as VNI-RED
`(config-nvo)#exit`	Exit from VxLAN tenant mode and enter into configuration mode.
`(config)#nvo vxlan id 20 ingress-replication inner-vid-disabled`	Configure VxLAN Network identifier with/without inner-VID-disabled configure and enter into VxLAN tenant mode
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp VRF2`	Assign VRF for EVPN-BGP to carry EVPN route
`(config-nvo)#vni-name VNI-BLUE`	Configure VNI-name as VNI-BLUE
`(config-nvo)#exit`	Exit from VxLAN tenant mode and enter into configuration mode.
`(config)#nvo vxlan access-if port-vlan xe48 1001`	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
`(config-nvo-acc-if)#map vni-name VNI-RED`	Map VxLAN Identified to access-port for VxLAN
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-interface mode and enter into configuration mode
`(config)#nvo vxlan access-if port-vlan xe48 1002`	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
`(config-nvo-acc-if)#map vni-name VNI-RED`	Map VxLAN Identified to access-port for VxLAN
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-interface mode and enter into configuration mode
`(config)#nvo vxlan access-if port-vlan xe48 3001`	Enable port-VLAN mapping i.e. access port to outer-VLAN (SVLAN) - Multihomed access port
`(config-nvo-acc-if)#map vni-name VNI-BLUE`	Map VxLAN Identified to access-port for VxLAN
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-interface mode and enter into configuration mode
`(config)#exit`	Exit from configuration mode

Switch (CE2)

Multihomed to 2-VTEPs (VTEP1 and VTEP2)

`#configure terminal`	Enter Configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure IEEE VLAN bridge
`(config)#vlan 1001-1002 bridge 1 state enable`	Configure VLANs from 1001-1002 and associate with bridge 1
`(config)#vlan 3001 bridge 1 state enable`	Configure VLANs from 3001 and associate with bridge 1
`(config)#interface xe22`	Enter Interface mode for xe22
`(config-if)#switchport`	Make xe22 as L2 port by configuring switchport
`(config-if)#bridge-group 1`	Associate xe22 to bridge 1

`(config-if)#switchport mode hybrid`	Configure xe22 as hybrid port
`(config-if)#switchport hybrid allowed vlan add 1001-1002,3001 egress-tagged enable`	Allow 1001-1002 and 3001 configured VLANs on xe22
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface po1`	Enter Interface mode for po1
`(config-if)#switchport`	Make po1 as L2 port by configuring switchport
`(config-if)#bridge-group 1`	Associate po1 to bridge 1
`(config-if)#switchport mode hybrid`	Configure po1 as hybrid port
`(config-if)#switchport hybrid allowed vlan add 1001-1002,3001 egress-tagged enable`	Allow 1001-1002 and 3001 configured VLANs on po1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe3`	Enter Interface mode for xe3
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config)#interface xe4`	Enter Interface mode for xe4
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config)#exit`	Exit from configuration mode
`(config)#interface xe9`	Enter Interface mode for xe9
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config)#interface xe10`	Enter Interface mode for xe10
`(config-if)#channel-group 1 mode active`	Make it member port of po1
`(config)#exit`	Exit from configuration mode

Spine 1

Spine node where all VTEPs are connected

© 2021 IP Infusion Inc. Proprietary

Generic Configuration

`#configure terminal`	Enter Configure mode.
`(config)#qos enable`	Enabling QoS

Interface and Loopback Configuration

`#configure terminal`	Enter Configure mode.
`(config)#qos enable`	Enabling QoS
`(config)#interface lo`	Enter Interface mode for lo
`(config-if)#ip address 11.11.11.11/32 secondary`	Configure loopback IP address as 11.11.11.11 for Spine1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe8`	Enter Interface mode for xe8
`(config-if)#ip address 10.10.10.2/24`	Configure IP address as 10.10.10.2 on network side of VTEP1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe1`	Enter Interface mode for xe1
`(config-if)#ip address 30.30.30.2/24`	Configure IP address as 30.30.30.2 on network side of VTEP2
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe18`	Enter Interface mode for xe18
`(config-if)#ip address 50.50.50.2/24`	Configure IP address as 50.50.50.2 on network side of VTEP3
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

OSPF configuration

`(config)#router ospf 100`	Enter into router OSPF mode
`(config-router)#ospf router-id 11.11.11.11`	Configure router-ID as 11.11.11.11 (lo IP address)
`(config-router)#network 11.11.11.11/32 area 0.0.0.0`	Add 11.11.11.11 (lo IP address) network into area 0
`(config-router)#network 10.10.10.0/24 area 0.0.0.0`	Add 10.10.10.0 (VTEP1) network into area 0
`(config-router)#network 30.30.30.0/24 area 0.0.0.0`	Add 30.30.30.0 (VTEP2) network into area 0
`(config-router)#network 50.50.50.0/24 area 0.0.0.0`	Add 50.50.50.0 (VTEP3) network into area 0
`(config-router)#bfd all-interfaces`	Enabling BFD on all OSPF interface for fast convergence
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

Spine 2

Spine node where all VTEPs are connected

Generic configuration

`#configure terminal`	Enter Configure mode.
`(config)#qos enable`	Enabling QoS

Interface and loopback configuration

`(config)#interface lo`	Enter Interface mode for lo
`(config-if)#ip address 22.22.22.22/32 secondary`	Configure loopback IP address as 22.22.22.22 for Spine2
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe5`	Enter Interface mode for xe5
`(config-if)#ip address 20.20.20.2/24`	Configure IP address as 20.20.20.2 on network side of VTEP1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface ce0`	Enter Interface mode for ce0
`(config-if)#ip address 40.40.40.2/24`	Configure IP address as 40.40.40.2 on network side of VTEP2
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe19`	Enter Interface mode for xe19
`(config-if)#ip address 60.60.60.2/24`	Configure IP address as 60.60.60.2 on network side of VTEP3
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

OSPF configuration

`(config)#router ospf 100`	Enter into router OSPF mode
`(config-router)#ospf router-id 22.22.22.22`	Configure router-id as 11.11.11.11 (lo IP address)
`(config-router)#network 22.22.22.22/32 area 0.0.0.0`	Add 22.22.22.22 (lo IP address) network into area 0
`(config-router)#network 20.20.20.0/24 area 0.0.0.0`	Add 20.20.20.0 (VTEP1) network into area 0
`(config-router)#network 40.40.40.0/24 area 0.0.0.0`	Add 40.40.40.0 (VTEP2) network into area 0
`(config-router)#network 60.60.60.0/24 area 0.0.0.0`	Add 60.60.60.0 (VTEP3) network into area 0
`(config-router)#bfd all-interfaces`	Enabling BFD on all OSPF interface for fast convergence
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

Validation

VTEP1

```
VTEP1#show nvo vxlan
```


© 2021 IP Infusion Inc. Proprietary

```
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID    VNI-Name     VNI-Type Type Interface ESI                            VLAN DF-Status
Src-Addr         Dst-Addr
_____________________________________________________________________________________________
_____________________________
10      VNI-RED      L2       NW   ----      ----                           ---- ----
1.1.1.1          3.3.3.3
10      VNI-RED      L2       NW   ----      ----                           ---- ----
1.1.1.1          2.2.2.2
10      VNI-RED      --       AC   po1       00:00:00:00:00:11:11:00:00:00 1001 NON-DF
----             ----
10      VNI-RED      --       AC   po1       00:00:00:00:00:11:11:00:00:00 1002 DF
----             ----
20      VNI-BLUE     L2       NW   ----      ----                           ---- ----
1.1.1.1          3.3.3.3
20      VNI-BLUE     L2       NW   ----      ----                           ---- ----
1.1.1.1          2.2.2.2
20      VNI-BLUE     --       AC   po1       00:00:00:00:00:11:11:00:00:00 3001 NON-DF
----             ----

Total number of entries are 7

VTEP1#show nvo vxlan access-if brief

                 Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
po1        1002  ---   500001   10        up      up
po1        1001  ---   500000   10        up      up
po1        3001  ---   500002   20        up      up

Total number of entries are 3

VTEP1#show bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 500
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
2.2.2.2                 4   500  161       163      5     0     0  01:05:15
6      3      0      2      1      0
3.3.3.3                 4   500  157       161      5     0     0  01:05:07
2      0      0      2      0      0

Total number of neighbors 2
```

```
Total number of Established sessions 2

VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status           Up/Down        Update
================================================================================
1.1.1.1          3.3.3.3          Installed        00:31:11       00:31:11
1.1.1.1          2.2.2.2          Installed        01:05:25       00:31:11

Total number of entries are 2

VTEP1#show bgp l2vpn evpn multihoming es-route

RD[1.1.1.1:1] VRF[evpn-gvrf-1]:
ESI                             PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  1.1.1.1         1.1.1.1         VXLAN
00:00:00:00:00:11:11:00:00:00  2.2.2.2         2.2.2.2         VXLAN

RD[2.2.2.2:1]
ESI                             PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  2.2.2.2         2.2.2.2         VXLAN

VTEP1#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[1.1.1.1:1] VRF[evpn-gvrf-1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              1.1.1.1         VXLAN

RD[1.1.1.1:11] VRF[VRF1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              2.2.2.2         VXLAN

RD[1.1.1.1:21] VRF[VRF2]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              2.2.2.2         VXLAN

RD[2.2.2.2:1]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  4294967295  0              2.2.2.2         VXLAN
VTEP1#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[1.1.1.1:11] VRF[VRF1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  10          10             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00  10          10             1.1.1.1         VXLAN

RD[1.1.1.1:21] VRF[VRF2]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  20          20             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00  20          20             1.1.1.1         VXLAN
```


© 2021 IP Infusion Inc. Proprietary

```
RD[2.2.2.2:11]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   10          10             2.2.2.2         VXLAN

RD[2.2.2.2:21]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   20          20             2.2.2.2         VXLAN

VTEP1#show bgp l2vpn evpn
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

   Network         Next Hop           Metric    LocPrf      Weight     Path  Peer
Encap

RD[1.1.1.1:1] VRF[evpn-gvrf-1]:
*>   [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                     1.1.1.1              0         100           32768    i  -------
---      VXLAN
*>   [4]:[00:00:00:00:00:11:11:00:00:00]:[32,1.1.1.1]
                     1.1.1.1              0         100           32768    i  -------
---      VXLAN
* i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,2.2.2.2]
                   2.2.2.2            0        100          0       i  2.2.2.2
VXLAN

RD[1.1.1.1:11] VRF[VRF1]:
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                   2.2.2.2            0        100          0       i  2.2.2.2
VXLAN
*>                   1.1.1.1              0         100           32768    i  -------
---      VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                   2.2.2.2            0        100          0       i  2.2.2.2
VXLAN
*>   [3]:[10]:[32,1.1.1.1]
                     1.1.1.1              0         100           32768    i  -------
---      VXLAN
* i  [3]:[10]:[32,2.2.2.2]
                   2.2.2.2            0        100          0       i  2.2.2.2
VXLAN
* i  [3]:[10]:[32,3.3.3.3]
```

```
                    3.3.3.3             0        100          0       i  3.3.3.3
VXLAN

RD[1.1.1.1:21] VRF[VRF2]:
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                    2.2.2.2             0        100          0       i  2.2.2.2
VXLAN
*>                     1.1.1.1              0         100           32768    i  -------
---      VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                    2.2.2.2             0        100          0       i  2.2.2.2
VXLAN
*>   [3]:[20]:[32,1.1.1.1]
                      1.1.1.1              0         100           32768    i  -------
---      VXLAN
* i  [3]:[20]:[32,2.2.2.2]
                    2.2.2.2             0        100          0       i  2.2.2.2
VXLAN
* i  [3]:[20]:[32,3.3.3.3]
                    3.3.3.3             0        100          0       i  3.3.3.3
VXLAN

RD[2.2.2.2:1]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                    2.2.2.2             0        100          0       i  2.2.2.2
VXLAN
*>i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,2.2.2.2]
                    2.2.2.2             0        100          0       i  2.2.2.2
VXLAN

RD[2.2.2.2:11]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                    2.2.2.2             0        100          0       i  2.2.2.2
VXLAN
*>i  [3]:[10]:[32,2.2.2.2]
                    2.2.2.2             0        100          0       i  2.2.2.2
VXLAN

RD[2.2.2.2:21]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                    2.2.2.2             0        100          0       i  2.2.2.2
VXLAN
*>i  [3]:[20]:[32,2.2.2.2]
                    2.2.2.2             0        100          0       i  2.2.2.2
VXLAN

RD[3.3.3.3:11]
*>i  [3]:[10]:[32,3.3.3.3]
                    3.3.3.3             0        100          0       i  3.3.3.3
VXLAN

RD[3.3.3.3:21]
*>i  [3]:[20]:[32,3.3.3.3]
```


© 2021 IP Infusion Inc. Proprietary

```
                    3.3.3.3            0        100          0       i  3.3.3.3
VXLAN

Total number of prefixes 21
```

VTEP2

```
VTEP2#show nvo vxlan
VXLAN Information
================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID    VNI-Name     VNI-Type Type Interface ESI                          VLAN DF-Status
Src-Addr         Dst-Addr
_____________________________________________________________________________________________
_____________________________
10      VNI-RED      L2       NW   ----      ----                         ---- ----
2.2.2.2          1.1.1.1
10      VNI-RED      L2       NW   ----      ----                         ---- ----
2.2.2.2          3.3.3.3
10      VNI-RED      --       AC   xe32      --- Single Homed Port ---    ---- ----
----             ----
10      VNI-RED      --       AC   po1       00:00:00:00:00:11:11:00:00:00 1001 DF
----             ----
10      VNI-RED      --       AC   po1       00:00:00:00:00:11:11:00:00:00 1002 NON-DF
----             ----
20      VNI-BLUE     L2       NW   ----      ----                         ---- ----
2.2.2.2          1.1.1.1
20      VNI-BLUE     L2       NW   ----      ----                         ---- ----
2.2.2.2          3.3.3.3
20      VNI-BLUE     --       AC   po1       00:00:00:00:00:11:11:00:00:00 3001 DF
----             ----

Total number of entries are 8

VTEP2#show nvo vxlan access-if
% Incomplete command.

VTEP2#show nvo vxlan access-if brief

                Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
xe32       ---   ---   500004   10        up      up
po1        1002  ---   500001   10        up      up
po1        1001  ---   500000   10        up      up
po1        3001  ---   500002   20        up      up

Total number of entries are 4

VTEP2#show bgp l2vpn evpn summary
```

```
BGP router identifier 2.2.2.2, local AS number 500
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
1.1.1.1                 4   500  172       171      4      0      0  01:09:28
6      3      0      2      1      0
3.3.3.3                 4   500  165       173      4      0      0  01:09:29
2      0      0      2      0      0

Total number of neighbors 2

Total number of Established sessions 2

VTEP2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status           Up/Down        Update
================================================================================
2.2.2.2          1.1.1.1          Installed        01:09:38       00:35:24
2.2.2.2          3.3.3.3          Installed        01:09:39       01:09:39

Total number of entries are 2

VTEP2#show bgp l2vpn evpn multihoming es-route

RD[1.1.1.1:1]
ESI                             PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   1.1.1.1         1.1.1.1         VXLAN

RD[2.2.2.2:1] VRF[evpn-gvrf-1]:
ESI                             PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   1.1.1.1         1.1.1.1         VXLAN
00:00:00:00:00:11:11:00:00:00   2.2.2.2         2.2.2.2         VXLAN
VTEP2#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[1.1.1.1:1]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   4294967295  0              1.1.1.1         VXLAN

RD[2.2.2.2:1] VRF[evpn-gvrf-1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   4294967295  0              2.2.2.2         VXLAN

RD[2.2.2.2:11] VRF[VRF1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   4294967295  0              1.1.1.1         VXLAN

RD[2.2.2.2:21] VRF[VRF2]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
```


© 2021 IP Infusion Inc. Proprietary

```
00:00:00:00:00:11:11:00:00:00  4294967295  0              1.1.1.1         VXLAN

VTEP2#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[1.1.1.1:11]
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  10          10             1.1.1.1         VXLAN

RD[1.1.1.1:21]
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  20          20             1.1.1.1         VXLAN

RD[2.2.2.2:11] VRF[VRF1]:
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  10          10             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00  10          10             1.1.1.1         VXLAN

RD[2.2.2.2:21] VRF[VRF2]:
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00  20          20             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00  20          20             1.1.1.1         VXLAN

VTEP2# show bgp l2vpn evpn
BGP table version is 4, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

   Network         Next Hop           Metric    LocPrf      Weight     Path  Peer
Encap

RD[1.1.1.1:1]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                    1.1.1.1            0        100          0       i  1.1.1.1
VXLAN
*>i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,1.1.1.1]
                    1.1.1.1            0        100          0       i  1.1.1.1
VXLAN

RD[1.1.1.1:11]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                    1.1.1.1            0        100          0       i  1.1.1.1
VXLAN
*>i  [3]:[10]:[32,1.1.1.1]
```

```
                    1.1.1.1             0        100          0       i  1.1.1.1
VXLAN

RD[1.1.1.1:21]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                    1.1.1.1             0        100          0       i  1.1.1.1
VXLAN
*>i  [3]:[20]:[32,1.1.1.1]
                    1.1.1.1             0        100          0       i  1.1.1.1
VXLAN

RD[2.2.2.2:1] VRF[evpn-gvrf-1]:
*>   [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                      2.2.2.2           0         100          32768    i  -------
---      VXLAN
* i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,1.1.1.1]
                    1.1.1.1             0        100          0       i  1.1.1.1
VXLAN
*>   [4]:[00:00:00:00:00:11:11:00:00:00]:[32,2.2.2.2]
                      2.2.2.2           0         100          32768    i  -------
---      VXLAN

RD[2.2.2.2:11] VRF[VRF1]:
*>   [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                      2.2.2.2           0         100          32768    i  -------
---      VXLAN
* i                  1.1.1.1             0        100          0       i  1.1.1.1
VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                    1.1.1.1             0        100          0       i  1.1.1.1
VXLAN
* i  [3]:[10]:[32,1.1.1.1]
                    1.1.1.1             0        100          0       i  1.1.1.1
VXLAN
*>   [3]:[10]:[32,2.2.2.2]
                      2.2.2.2           0         100          32768    i  -------
---      VXLAN
* i  [3]:[10]:[32,3.3.3.3]
                    3.3.3.3             0        100          0       i  3.3.3.3
VXLAN

RD[2.2.2.2:21] VRF[VRF2]:
*>   [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                      2.2.2.2           0         100          32768    i  -------
---      VXLAN
* i                  1.1.1.1             0        100          0       i  1.1.1.1
VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                    1.1.1.1             0        100          0       i  1.1.1.1
VXLAN
* i  [3]:[20]:[32,1.1.1.1]
                    1.1.1.1             0        100          0       i  1.1.1.1
VXLAN
*>   [3]:[20]:[32,2.2.2.2]
```


© 2021 IP Infusion Inc. Proprietary

```
                        2.2.2.2              0         100           32768    i  -------
---      VXLAN
* i  [3]:[20]:[32,3.3.3.3]
                     3.3.3.3             0        100          0       i  3.3.3.3
VXLAN

RD[3.3.3.3:11]
*>i  [3]:[10]:[32,3.3.3.3]
                     3.3.3.3             0        100          0       i  3.3.3.3
VXLAN

RD[3.3.3.3:21]
*>i  [3]:[20]:[32,3.3.3.3]
                     3.3.3.3             0        100          0       i  3.3.3.3
VXLAN

Total number of prefixes 21
```

VTEP3

```
VTEP3#  show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
           AC - Access Port
          (u) - Untagged

VNID    VNI-Name    VNI-Type Type Interface ESI                          VLAN DF-Status
Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________
10      VNI-RED     L2       NW   ----     ----                         ---- ----
3.3.3.3          2.2.2.2
10      VNI-RED     L2       NW   ----     ----                         ---- ----
3.3.3.3          1.1.1.1
10      VNI-RED     --       AC   xe48     --- Single Homed Port ---    1001 ----
----             ----
10      VNI-RED     --       AC   xe48     --- Single Homed Port ---    1002 ----
----             ----
20      VNI-BLUE    L2       NW   ----     ----                         ---- ----
3.3.3.3          2.2.2.2
20      VNI-BLUE    L2       NW   ----     ----                         ---- ----
3.3.3.3          1.1.1.1
20      VNI-BLUE    --       AC   xe48     --- Single Homed Port ---    3001 ----
----             ----

Total number of entries are 7

VTEP3#show nvo vxlan access-if brief

                Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
```

```
xe48       1002  ---   500001   10        up      up
xe48       1001  ---   500000   10        up      up
xe48       3001  ---   500002   20        up      up

Total number of entries are 3

VTEP3#show bgp l2vpn evpn summary
BGP router identifier 3.3.3.3, local AS number 500
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
1.1.1.1                 4   500  177       173      3      0      0  01:11:49
6      3      0      2      1      0
2.2.2.2                 4   500  177       171      2      0      0  01:11:59
6      3      0      2      1      0

Total number of neighbors 2

Total number of Established sessions 2

VTEP3#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status           Up/Down        Update
================================================================================
3.3.3.3          2.2.2.2          Installed        01:12:10       01:12:10
3.3.3.3          1.1.1.1          Installed        01:12:00       01:12:00

Total number of entries are 2

VTEP3#show bgp l2vpn evpn multihoming es-route

RD[1.1.1.1:1]
ESI                             PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   1.1.1.1         1.1.1.1         VXLAN

RD[2.2.2.2:1]
ESI                             PE IP-Address   Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   2.2.2.2         2.2.2.2         VXLAN

VTEP3#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[1.1.1.1:1]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   4294967295  0              1.1.1.1         VXLAN

RD[2.2.2.2:1]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   4294967295  0              2.2.2.2         VXLAN
```


© 2021 IP Infusion Inc. Proprietary

```
RD[3.3.3.3:11] VRF[VRF1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   4294967295  0              2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00   4294967295  0              1.1.1.1         VXLAN

RD[3.3.3.3:21] VRF[VRF2]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   4294967295  0              2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00   4294967295  0              1.1.1.1         VXLAN

VTEP3#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[1.1.1.1:11]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   10          10             1.1.1.1         VXLAN

RD[1.1.1.1:21]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   20          20             1.1.1.1         VXLAN

RD[2.2.2.2:11]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   10          10             2.2.2.2         VXLAN

RD[2.2.2.2:21]
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   20          20             2.2.2.2         VXLAN

RD[3.3.3.3:11] VRF[VRF1]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   10          10             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00   10          10             1.1.1.1         VXLAN

RD[3.3.3.3:21] VRF[VRF2]:
ESI                             Eth-Tag     VNID/LABEL     Nexthop IP      Encap
00:00:00:00:00:11:11:00:00:00   20          20             2.2.2.2         VXLAN
00:00:00:00:00:11:11:00:00:00   20          20             1.1.1.1         VXLAN

VTEP3#show bgp l2vpn evpn
BGP table version is 4, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
```

```
5 - Prefix Route

   Network          Next Hop            Metric    LocPrf      Weight     Path  Peer
Encap

RD[1.1.1.1:1]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                    1.1.1.1             0         100           0        i  1.1.1.1
VXLAN
*>i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,1.1.1.1]
                    1.1.1.1             0         100           0        i  1.1.1.1
VXLAN

RD[1.1.1.1:11]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                    1.1.1.1             0         100           0        i  1.1.1.1
VXLAN
*>i  [3]:[10]:[32,1.1.1.1]
                    1.1.1.1             0         100           0        i  1.1.1.1
VXLAN

RD[1.1.1.1:21]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                    1.1.1.1             0         100           0        i  1.1.1.1
VXLAN
*>i  [3]:[20]:[32,1.1.1.1]
                    1.1.1.1             0         100           0        i  1.1.1.1
VXLAN

RD[2.2.2.2:1]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                    2.2.2.2             0         100           0        i  2.2.2.2
VXLAN
*>i  [4]:[00:00:00:00:00:11:11:00:00:00]:[32,2.2.2.2]
                    2.2.2.2             0         100           0        i  2.2.2.2
VXLAN

RD[2.2.2.2:11]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                    2.2.2.2             0         100           0        i  2.2.2.2
VXLAN
*>i  [3]:[10]:[32,2.2.2.2]
                    2.2.2.2             0         100           0        i  2.2.2.2
VXLAN

RD[2.2.2.2:21]
*>i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                    2.2.2.2             0         100           0        i  2.2.2.2
VXLAN
*>i  [3]:[20]:[32,2.2.2.2]
                    2.2.2.2             0         100           0        i  2.2.2.2
VXLAN
```


© 2021 IP Infusion Inc. Proprietary

```
RD[3.3.3.3:11] VRF[VRF1]:
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[10]:[10]
                    2.2.2.2            0        100          0       i  2.2.2.2
VXLAN
* i                 1.1.1.1            0        100          0       i  1.1.1.1
VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                    2.2.2.2            0        100          0       i  2.2.2.2
VXLAN
* i                 1.1.1.1            0        100          0       i  1.1.1.1
VXLAN
* i  [3]:[10]:[32,1.1.1.1]
                    1.1.1.1            0        100          0       i  1.1.1.1
VXLAN
* i  [3]:[10]:[32,2.2.2.2]
                    2.2.2.2            0        100          0       i  2.2.2.2
VXLAN
*>   [3]:[10]:[32,3.3.3.3]
                      3.3.3.3              0         100           32768    i  -------
---      VXLAN

RD[3.3.3.3:21] VRF[VRF2]:
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[20]:[20]
                    2.2.2.2            0        100          0       i  2.2.2.2
VXLAN
* i                 1.1.1.1            0        100          0       i  1.1.1.1
VXLAN
* i  [1]:[00:00:00:00:00:11:11:00:00:00]:[4294967295]:[0]
                    2.2.2.2            0        100          0       i  2.2.2.2
VXLAN
* i                 1.1.1.1            0        100          0       i  1.1.1.1
VXLAN
* i  [3]:[20]:[32,1.1.1.1]
                    1.1.1.1            0        100          0       i  1.1.1.1
VXLAN
* i  [3]:[20]:[32,2.2.2.2]
                    2.2.2.2            0        100          0       i  2.2.2.2
VXLAN
*>   [3]:[20]:[32,3.3.3.3]
                      3.3.3.3              0         100           32768    i  -------
---      VXLAN

Total number of prefixes 22
```

Static MAC-IP advertise through Single Home and Multihomed VTEPs

Advertise static MAC IPv4 from MH1 and SH3.

MH1-VTEPs: VTEP1 & VTEP2- same MAC should be configured on both VTEPs under po access-port, configs should be symmetric between MH VTEPs

SH3-VTEP: VTEP3

VTEP1(MH1)

`#configure terminal`	Enter Configure mode.
`(config)# nvo vxlan access-if port-vlan po1 1001`	Enter into VxLAN MH po1 access-port with VLAN 1001
`(config-nvo-acc-if)#mac 0000.1111.1001 ip 11.11.10.1`	Configure static MAC IP
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-port config mode
`(config)#exit`	Exit from configuration mode

VTEP2(MH1)

`#configure terminal`	Enter Configure mode.
`(config)#nvo vxlan access-if port-vlan po1 1001`	Enter into VxLAN MH po1 access-port with vlan 1001
`(config-nvo-acc-if)# mac 0000.1111.1001 ip 11.11.10.1`	Configure static MAC IP
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-port config mode
`(config)#exit`	Exit from configuration mode

VTEP3(SH)

`#configure terminal`	Enter Configure mode.
`(config)# nvo vxlan access-if port-vlan xe48 1001`	Enter into single-homed access-port - xe48 with VLAN 1001
`(config-nvo-acc-if)#mac 0000.3333.1001 ip 11.11.10.2`	Configure static MAC IP
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-port config mode
`(config)#exit`	Exit from configuration mode

Validation

Verify MAC-table in MH VTEPs and Single Home VTEP, MAC will be advertised through ESI value which is advertised from VTEP1 and VTEP2 and VTEP IP from SH VTEP VTEP3.

Verify ARP-cache table in all VTEPs, VTEP1 and VTEP2 will learn VTEP3 IP.

Any ARP request comes for 11.11.10.2, VTEP1/VTEP2 will do proxy-ARP.

VTEP1

```
VTEP1#show nvo vxlan mac-table
================================================================================================
                                                    VXLAN MAC Entries
================================================================================================
```


© 2021 IP Infusion Inc. Proprietary

```
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type            Status     AccessPortDesc
_____________________________________________________________________________________________
_____________________________________________

10         po1       1001   ----         0000.1111.1001 00:00:00:00:00:11:11:00:00:00
Static Local    -------    -------
10         ----      ----   ----         0000.3333.1001 3.3.3.3
Static Remote   -------    -------

Total number of entries are : 2

VTEP1#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
10       11.11.10.1       0000.1111.1001 Static Local   ----
10       11.11.10.2       0000.3333.1001 Static Remote  ----
Total number of entries are 2
```

VTEP2

```
VTEP2#show nvo vxlan mac-table
=============================================================================================
====================================
                                                          VXLAN MAC Entries
=============================================================================================
====================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type            Status     AccessPortDesc
_____________________________________________________________________________________________
_________________________________________

10         po1       1001   ----         0000.1111.1001 00:00:00:00:00:11:11:00:00:00
Static Local    -------    -------
10         ----      ----   ----         0000.3333.1001 3.3.3.3
Static Remote   -------    -------

Total number of entries are : 2

VTEP2#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
10       11.11.10.1       0000.1111.1001 Static Local   ----
10       11.11.10.2       0000.3333.1001 Static Remote  ----
Total number of entries are 2
```

VTEP3

```
VTEP3#show nvo vxlan mac-table
================================================================================================
====================================
                                                                VXLAN MAC Entries
================================================================================================
====================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type            Status     AccessPortDesc

________________________________________________________________________________________________
_____________________________________

10         ----      1001   ----         0000.1111.1001 00:00:00:00:00:11:11:00:00:00
Static Remote   -------    -------
10         xe48      1001   ----         0000.3333.1001 3.3.3.3
Static Local    -------    -------

Total number of entries are : 2

VTEP3#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
============================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left

_____________________________________________________________________________
10       11.11.10.1       0000.1111.1001 Static Remote  ----
10       11.11.10.2       0000.3333.1001 Static Local   ----
Total number of entries are 2
```

Dynamic MAC advertise through Single Home and Multihomed VTEPs

Advertise 2 MAC's through CE1 connected IXIA, dynamic MAC entries and verify MAC-table in all VTEPs.

One MAC will be dynamic local in VTEP1 and same will be remote in VTEP2 and other be dynamic local in VTEP2 and same will be remote in VTEP1.

Both MAC's will be in remote in VTEP3.

VTEP1

```
VTEP1#show nvo vxlan mac-table
================================================================================================
====================================
                                                                VXLAN MAC Entries
================================================================================================
====================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type            Status     AccessPortDesc

________________________________________________________________________________________________
_____________________________________

10         po1       1001   ----         0000.1111.1002 00:00:00:00:00:11:11:00:00:00
Dynamic Local   -------    -------
```


© 2021 IP Infusion Inc. Proprietary

```
10         ----      1002   ----         0000.1111.1003 00:00:00:00:00:11:11:00:00:00
Dynamic Remote  -------    -------

Total number of entries are : 2

VTEP1#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
10       21.21.21.1       0000.1111.1002 Dynamic Local  ----
10       31.1.31.1        0000.1111.1003 Dynamic Remote ----
Total number of entries are 2
```

VTEP2

```
VTEP2#show nvo vxlan mac-table
================================================================================================
====================================
                                                        VXLAN MAC Entries
================================================================================================
====================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type            Status     AccessPortDesc
________________________________________________________________________________________________
_____________________________________

10         ----      1001   ----         0000.1111.1002 00:00:00:00:00:11:11:00:00:00
Dynamic Remote  -------    -------
10         po1       1002   ----         0000.1111.1003 00:00:00:00:00:11:11:00:00:00
Dynamic Local   -------    -------

Total number of entries are : 2

VTEP2#show nvo vxla arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
10       21.21.21.1       0000.1111.1002 Dynamic Remote ----
10       31.1.31.1        0000.1111.1003 Dynamic Local  ----
Total number of entries are 2
```

VTEP3

```
VTEP3#show nvo vxlan mac-table
================================================================================================
================================================
                                                        VXLAN MAC Entries
```

```
================================================================================================
================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type            Status     AccessPortDesc
________________________________________________________________________________________________
_____________________________________________________

10         ----      1001   ----         0000.1111.1002 00:00:00:00:00:11:11:00:00:00
Dynamic Remote  -------    -------
10         ----      1002   ----         0000.1111.1003 00:00:00:00:00:11:11:00:00:00
Dynamic Remote  -------    -------

Total number of entries are : 2

VTEP3#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
10       21.21.21.1       0000.1111.1002 Dynamic Remote ----
10       31.1.31.1        0000.1111.1003 Dynamic Remote ----
Total number of entries are 2
```

Note: When VTEP1 tunnel goes down, then traffic from VTEP3 will use VTEP2 for forwarding. But Traffic from Switch to VTEP1 will be lost in VTEP1 itself.

When DUT is rebooted, access-if will be in hold down state until ESI hold timer value expiry. After ESI hold timer expiry, access-if port will be up and started learning.

MAC Hold timer will not be applicable on ESI interface, because of mass-withdraw requirement.

A CE can connect to maximum two nodes for multihoming, more than two nodes in a multihoming group is not supported.

All configuration (shutdown, disable learning, disable arp/nd cache, disable arp/nd flood, map vnid, qos profiles, encapsulation) on a multihomed access port should be same on both VTEPs sharing the ESI for multihoming functionalities to work properly.

Multiple ESI values are supported on same VTEP.

© 2021 IP Infusion Inc. Proprietary

CHAPTER 7 VXLAN Quality of Service Configuration

This chapter contains the configurations for VXLAN Quality of Service (QoS) .

Overview

VXLAN enables multiple tenants to operate in a data center. Each tenant is assigned a priority group to prioritize their traffic. Cloud carriers want to use quality of service to differentiate different applications.

Data center networks are being increasingly used by telecommunications operators as well as by enterprises. Currently these networks are organized as one large Layer 2 network in a single building. In some cases such a network is extended geographically using Virtual Local Area Network (VLAN) technologies as an even larger Layer 2 network connecting the virtual machines (VM), each with its own MAC address.

Multiple tenants might want their own isolated network domain. In a data center hosting multiple tenants, each tenant may independently assign MAC addresses and VLAN IDs and this might lead to duplication.

Cloud carriers wish to categorize the traffic based on the application such as voice, video, etc. Based on the type of the application different traffic classes may be identified and different priority levels can be assigned to each. To do so, quality of service marking is needed in VXLAN.

This chapter shows how to mark packet headers with the VXLAN tunnel end point (VTEP) when the frames are introduced by the virtual machines. The (re)marking /setting of QoS field DSCP/TOS in the VXLAN IP header is done with the two modes which are set globally.

Topology

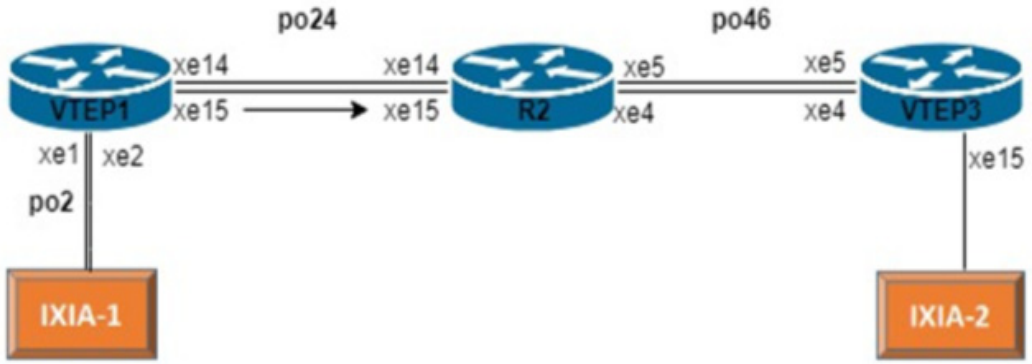


Figure 7-77: VXLAN QoS

COS-DSCP

RTR1/VTEP1

`VTEP1#configure terminal`	Enter Configure mode.
`(config)#mac vrf vrf1`	Create mac routing/forwarding instance with vrf1 name and enter into vrf mode
`(config-vrf)#rd 1.1.1.1:11`	Assign RD value
`(config-vrf)#route-target both 10.10.10.10:100`	Assign route-target value for import/export
`(config-vrf)#exit`	Exit from vrf mode
`(config)#qos enable`	Enable qos
`(config)#qos profile cos-to-queue COS-QUE`	Create qos profile for mapping traffic towards tunnel from access-if.
`(config-ingress-cos-map)#cos 2 queue 3`	Configure particular COS value to the queue value for configured profile.
`(config-ingress-cos-map)#exit`	Exit from qos profile config mode
`(config)#qos profile queue-color-to-dscp QUE-DSCP`	Create qos profile for attaching in vxlan tunnel egress.
`(config-egress-dscp-map)#queue 3 dscp 16`	Configure particular queue value to the dscp value for configured profile.
`(config-egress-dscp-encap-map)#exit`	Exit from qos profile config mode
`(config)#interface po2`	Create a port channel po2
`(config-if)#switchport`	Configure port as switchport
`(config-if)#load-interval 30`	Set load-interval
`(config-if)#interface po24`	Create a port channel po24
`(config-if)#load-interval 30`	Configure port as switchport
`(config-if)#ip address 24.1.1.1/30`	Set load-interval
`(config-if)#interface lo`	Enter in to loopback interface
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure ip address
`(config-if)#interface xe1`	Enter in to interface mode
`(config-if)#channel-group 2 mode active`	Map to channel-group
`(config-if)#interface xe2`	Enter in to interface mode
`(config-if)#channel-group 2 mode active`	Map to channel-group
`(config-if)#interface xe14`	Enter in to interface mode
`(config-if)#channel-group 24 mode ac-tive`	Map to channel-group
`(config-if)#interface xe15`	Enter in to interface mode
`(config-if)#channel-group 24 mode ac-tive`	Map to channel-group
`(config-if)#router ospf 1`	Create ospf instance
`(config-router)#ospf router-id 1.1.1.1`	Configure ospf router-id
`(config-router)#network 1.1.1.1/32 area 0.0.0.0`	Configure loopback network address in to ospf
`(config-router)#network 24.1.1.0/30 area 0.0.0.0`	Configure network address in to ospf

© 2021 IP Infusion Inc. Proprietary

(config-router)#router bgp 100	Enter into Router BGP mode
(config-router)#neighbor 6.6.6.6 re-mote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 6.6.6.6 up-date-source lo	Specify the neighbor to use loopback address as source
(config-router)#address-family l2vpn evpn	Enter into l2vpn evpn address-family
(config-router-af)#neighbor 6.6.6.6 activate	Activate the neighbor to address-family
(config-router)#nvo vxlan vtep-ip-global 1.1.1.1	Configure Source vtep-ip-global configuration
(config)#nvo vxlan tunnel qos-map-mode cos-dscp egress QUE-DSCP	Configure the mapping qos profile in to vxlan tunnel egress
(config)#nvo vxlan id 1 in-gress-replication inner-vid-disabled	Create vnid 1 and disable inner-vid
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#nvo vxlan access-if port-vlan po2 1001	Create vxlan access-if with vlan 1001
(config-nvo-acc-if)#no shutdown	No shut the vxlan access-if
(config-nvo-acc-if)#map vnid 1	Map vnid to the vxlan access-if
(config-nvo-acc-if)#map qos-profile cos-to-queue COS-QUE	Map qos profile for vxlan access-if ingress traffic from CE

RTR2

R2#configure terminal	Enter Configure mode.
(config)#interface po24	Create port channel
(config-if)#load-interval 30	Set load-interval
(config-if)#ip address 24.1.1.2/30	Assign ip address
(config-if)#interface po46	Create port channel
(config-if)#load-interval 30	Set load-interval
(config-if)#ip address 46.1.1.1/30	Assign ip address
(config-if)#interface lo	Enter in to loopback interface
(config-if)#ip address 4.4.4.4/32 sec-ondary	Assign secondary ip address
(config-if)#interface xe4	Enter into interface mode
(config-if)#channel-group 46 mode active	Map port channel to the interface
(config-if)#interface xe5	Enter into interface mode
(config-if)#channel-group 46 mode active	Map port channel to the interface
(config-if)#interface xe14	Enter into interface mode
(config-if)#channel-group 24 mode active	Map port channel to the interface
(config-if)#interface xe15	Enter into interface mode
(config-if)#channel-group 24 mode active	Map port channel to the interface
(config-if)#router ospf 1	Create ospf instance
(config-router)#ospf router-id 4.4.4.4	Configure ospf router-id

`(config-router)#network 4.4.4.4/32 area 0.0.0.0`	Configure ospf network address with respective area
`(config-router)#network 24.1.1.0/30 area 0.0.0.0`	Configure ospf network address with respective area
`(config-router)#network 46.1.1.0/30 area 0.0.0.0`	Configure ospf network address with respective area

© 2021 IP Infusion Inc. Proprietary

RTR3/VTEP2

VTEP2#configure terminal	Enter Configuration mode
(config)#mac vrf vrf1	Create mac routing/forwarding instance with vrf1 name and enter into vrf mode
(config-vrf)#rd 6.6.6.6:11	Assign RD value
(config-vrf)#route-target both 10.10.10.10:100	Assign route-target value for import/export
(config-vrf)#exit	Exit from vrf mode
(config)#qos enable	Enable QOS
(config)#qos statistics	Enable QOS statistics
(config-ingress-cos-map)#qos profile queue-color-to-cos QUE-COS	Create qos profile for mapping incoming traffic from tunnel to access-if.
(config-egress-cos-map)#queue 4 cos 5	Configure particular queue value to the cos value for configured profile.
(config-egress-cos-map)#qos profile dscp-to-queue DSCP-QUE	Create qos profile for attaching in vxlan tunnel ingress.
(config-ingress-dscp-map)#dscp 16 queue 4	Configure particular dscp value to the queue value for configured profile.
(config-egress-dscp-map)#interface po46	Create port channel
(config-if)#load-interval 30	Set load interval
(config-if)#ip address 46.1.1.2/30	Assign ip address
(config-if)#interface lo	Enter into loopback interface
(config-if)#ip address 6.6.6.6/32 secondary	Assign secondary ip address
(config-if)#interface xe4	Enter into interface mode
(config-if)#channel-group 46 mode active	Map channel group into the interface
(config-if)#interface xe5	Enter into interface mode
(config-if)#channel-group 46 mode active	Map channel group into the interface
(config-if)#interface xe15	Enter into interface mode
(config-if)#switchport	Make interface as L2 port
(config-if)#load-interval 30	Set load interval
(config-if)#router ospf 1	Create ospf instance
(config-router)#ospf router-id 6.6.6.6	Configure ospf router-id
(config-router)#network 6.6.6.6/32 area 0.0.0.0	Configure ospf network address with respective area
(config-router)#network 46.1.1.0/30 area 0.0.0.0	Configure ospf network address with respective area
(config-router)#router bgp 100	Enter into Router BGP mode
(config-router)#neighbor 1.1.1.1 re-mote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 1.1.1.1 up-date-source lo	Specify the neighbor to use loopback address as source
(config-router)#address-family l2vpn evpn	Enter into l2vpn evpn address-family
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor to address-family
(config)#nvo vxlan vtep-ip-global 6.6.6.6	Configure Source vtep-ip-global configuration

`(config)#nvo vxlan tunnel qos-map-mode cos-dscp ingress DSCP-QUE`	Configure the mapping qos profile in to vxlan tunnel ingress
`(config)#nvo vxlan id 1 in-gress-replication inner-vid-disabled`	Create vnid 1 and disable inner-vid
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1`	Assign vrf for evpn-bgp to carry EVPN route
`(config-nvo)#nvo vxlan access-if port-vlan xe15 1000`	Create vxlan access-if with vlan 1000
`(config-nvo-acc-if)#no shutdown`	No shut the vxlan access-if
`(config-nvo-acc-if)#map vnid 1`	Map vnid to the vxlan access-if
`(config-nvo-acc-if)#map qos-profile queue-color-to-cos QUE-COS`	Map qos profile for vxlan access-if egress traffic to CE

Validation

As per the qos configuration, when L2 traffic with cos value 2 sent to VTEP1 access-if, the packets forwarded to queue 3 and packets in queue 3 are mapped with overlay dscp value 16 while egress out of tunnel. At VTEP2, when packets with overlay dscp value 16 ingresses at tunnel, it is forwarded to queue 4 and packets of queue 4 are remarked with cos value 5.

RTR1/VTEP1

```
VTEP1#sh run nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 1.1.1.1
!
nvo vxlan tunnel qos-map-mode cos-dscp egress QUE-DSCP
!
nvo vxlan id 1 ingress-replication inner-vid-disabled
 vxlan host-reachability-protocol evpn-bgp vrf1
!
nvo vxlan access-if port-vlan po2 1001
 map vnid 1
 map qos-profile cos-to-queue COS-QUE
!
VTEP1#show run qos
qos enable
!
qos profile cos-to-queue COS-QUE
 cos 2 dei all queue 3
!
qos profile queue-color-to-dscp QUE-DSCP
 queue 3 color all dscp 16
!

VTEP1#show interface xe14 count queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
```


© 2021 IP Infusion Inc. Proprietary

```
+--------------------+--------+----------------+------------------+----------------
+------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts    |     Tx bytes     |  Dropped pkts   |
Dropped bytes   |
+--------------------+--------+----------------+------------------+----------------
+------------------+
q0                (E) 12517376 0                0                  0                 0
q1                (E) 12517376 0                0                  0                 0
q2                (E) 12517376 0                0                  0                 0
q3                (E) 12517376 205284588        188040683524       0                 0
q4                (E) 12517376 0                0                  0                 0
q5                (E) 12517376 0                0                  0                 0
q6                (E) 12517376 0                0                  0                 0
q7                (E) 12517376 7518             1007412            0                 0

VTEP1#show interface xe15 count queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+----------------+------------------+----------------
+------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts    |     Tx bytes     |  Dropped pkts   |
Dropped bytes   |
+--------------------+--------+----------------+------------------+----------------
+------------------+
q0                (E) 12517376 0                0                  0                 0
q1                (E) 12517376 0                0                  0                 0
q2                (E) 12517376 0                0                  0                 0
q3                (E) 12517376 205624494        188352040168       0                 0
q4                (E) 12517376 0                0                  0                 0
q5                (E) 12517376 0                0                  0                 0
q6                (E) 12517376 0                0                  0                 0
q7                (E) 12517376 9006             1136741            0                 0

VTEP1#
VTEP1#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID    VNI-Name     VNI-Type Type Interface ESI                           VLAN DF-Status
Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________
1       ----         L2       NW   ----      ----                          ---- ----
1.1.1.1          6.6.6.6
1       ----        AC   po2      --- Single Hommed port ---    1001 ----     ----
----

Total number of entries are 3
VTEP1#show nvo vxlan mac-table
=============================================================================
============================================================
```

```
                                                                    VXLAN MAC Entries
================================================================================================
================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
________________________________________________________________________________________________
________________________________________________________________

1         po2        1001   ----         0000.2000.9991 1.1.1.1
Dynamic Local        -------              -------

Total number of entries are : 1

VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source            Destination      Status          Up/Down        Update
================================================================================
1.1.1.1          6.6.6.6          Installed        00:11:29        00:11:29

Total number of entries are 2
VTEP1#
VTEP1#show qos-profile COS-QUE
profile name: COS-QUE
profile type: cos-to-queue
profile attached to 1 instances
configured mapping:
 cos 2 dei all queue 3
Detailed mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       3       green    |  2       1       3       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

VTEP1#
VTEP1#show qos-profile QUE-DSCP
profile name: QUE-DSCP
profile type: queue-color-to-dscp
profile attached to 1 instances
configured mapping:
 queue 3 color all dscp 16
Detailed mapping:
 ----------------+-------- | ----------------+-------- | ----------------+--------
```


© 2021 IP Infusion Inc. Proprietary

```
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      | OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+--------
  Queue | Color  | DSCP    |  Queue | Color  | DSCP    |  Queue | Color  | DSCP
 -------+--------+-------- | -------+--------+-------- | -------+--------+--------
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    10      |  1       yellow   12      |  1       red      14
  2       green    18      |  2       yellow   20      |  2       red      22
  3       green    16      |  3       yellow   16      |  3       red      16
  4       green    34      |  4       yellow   36      |  4       red      38
  5       green    40      |  5       yellow   40      |  5       red      40
  6       green    48      |  6       yellow   48      |  6       red      48
  7       green    56      |  7       yellow   56      |  7       red      56

VTEP1#
```

RTR3/VTEP3

```
VTEP3#show run nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 6.6.6.6
!
nvo vxlan tunnel qos-map-mode cos-dscp ingress DSCP-QUE
!
nvo vxlan id 1 ingress-replication inner-vid-disabled
 vxlan host-reachability-protocol evpn-bgp vrf1
!
nvo vxlan access-if port-vlan xe15 1000
 map vnid 1
 map qos-profile queue-color-to-cos QUE-COS
!
!
VTEP3#show run qos
qos enable
qos statistics
!
qos profile queue-color-to-cos QUE-COS
 queue 4 color all cos 5
!
qos profile dscp-to-queue DSCP-QUE
 dscp 16 queue 4
!
VTEP3#show nvo vxlan mac-table

================================================================================================
============================================================
                                                          VXLAN MAC Entries
```

```
================================================================================================
============================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
________________________________________________________________________________________________
_____________________________________________________________

1         ----       ----   ----         0000.2000.9991 1.1.1.1
Dynamic Remote       -------              -------

Total number of entries are : 1

VTEP3#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
6.6.6.6          1.1.1.1          Installed       00:09:39        00:09:39

Total number of entries are 2
VTEP3#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface ESI                          VLAN DF-Status
Src-Addr         Dst-Addr
________________________________________________________________________________________________
_____________________________________
1        ----         L2       NW   ----      ----                         ---- ----
6.6.6.6          1.1.1.1
1       ----        AC   xe15     --- Single Hommed port ---   1000 ----     ----
----

Total number of entries are 3
VTEP3#

VTEP3#show interface xe15 count queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+-----------------+-------------------+-----------------
+--------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts     |     Tx bytes      |  Dropped pkts   |
Dropped bytes   |
+--------------------+--------+-----------------+-------------------+-----------------
+--------------------+
q0                (E) 12517376 0                 0                   0                 0
q1                (E) 12517376 0                 0                   0                 0
q2                (E) 12517376 0                 0                   0                 0
q3                (E) 12517376 0                 0                   0                 0
q4                (E) 12517376 37895872          36455829826         0                 0
q5                (E) 12517376 0                 0                   0                 0
q6                (E) 12517376 0                 0                   0                 0
```


© 2021 IP Infusion Inc. Proprietary

```
q7                (E) 12517376 0                 0                   0                 0

VTEP3#
VTEP3#show qos-profile QUE-COS
profile name: QUE-COS
profile type: queue-color-to-cos
profile attached to 1 instances
configured mapping:
 queue 4 color all cos 5
Detailed mapping:
 ----------------+-------- | ----------------+-------- | ----------------+--------
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      | OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+--------
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+--------
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    5       |  4       yellow   5       |  4       red      5
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7

VTEP3#
VTEP3#show qos-profile DSCP-QUE
profile name: DSCP-QUE
profile type: dscp-to-queue
profile attached to 1 instances
configured mapping:
 dscp 16 queue 4
Detailed mapping:
 Ingress map for dscp to queue-color
 -------+----------------- | -------+----------------- | -------+----------------- | --
-----+-----------------
  INPUT |     OUTPUT       |  INPUT |     OUTPUT       |  INPUT |     OUTPUT       |
INPUT |     OUTPUT
 -------+----------------- | -------+----------------- | -------+----------------- | --
-----+-----------------
  DSCP  | Queue | Color    |  DSCP  | Queue | Color    |  DSCP  | Queue | Color    |  DSCP
| Queue | Color
 -------+-------+--------- | -------+-------+--------- | -------+-------+--------- | --
-----+-------+---------
  0       0       green    |  16      4       green    |  32      4       green    |  48
6       green
  1       0       green    |  17      2       green    |  33      4       green    |  49
6       green
  2       0       green    |  18      2       green    |  34      4       green    |  50
6       green
  3       0       green    |  19      2       green    |  35      4       green    |  51
6       green
  4       0       green    |  20      2       yellow   |  36      4       yellow   |  52
6       green
```

```
  5       0       green    |  21      2       green    |  37      4       green    |  53
6       green
  6       0       green    |  22      2       red      |  38      4       red      |  54
6       green
  7       0       green    |  23      2       green    |  39      4       green    |  55
6       green
  8       1       green    |  24      3       green    |  40      5       green    |  56
7       green
  9       1       green    |  25      3       green    |  41      5       green    |  57
7       green
  10      1       green    |  26      3       green    |  42      5       green    |  58
7       green
  11      1       green    |  27      3       green    |  43      5       green    |  59
7       green
  12      1       yellow   |  28      3       yellow   |  44      5       green    |  60
7       green
  13      1       green    |  29      3       green    |  45      5       green    |  61
7       green
  14      1       red      |  30      3       red      |  46      5       green    |  62
7       green
  15      1       green    |  31      3       green    |  47      5       green    |  63
7       green

VTEP3#
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 8 VXLAN Trunk Access Port

In VxLAN, most of the use cases demand to carry the complete traffic received on the access interface to another VTEP access-port. Hence, this support of accepting all tagged and untagged traffic received on the mapped physical port.

Topology

The configurations used in this section use the topology in Figure 8-78.

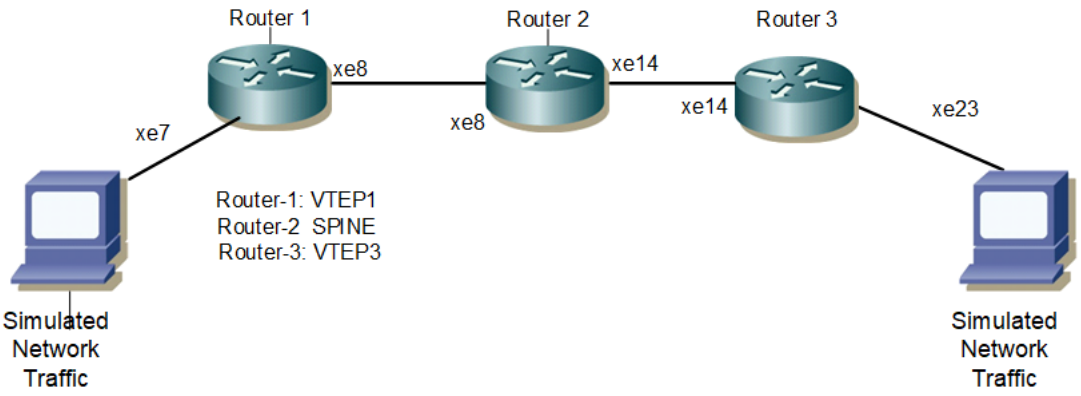


Figure 8-78: VXLAN Trunk Access Port

Base Configuration - L2 VXLAN

VTEP1

Hardware profile and generic configuration:

`#configure terminal`	Enter Configure mode.
`(config)#qos enable`	Enable qos
`(config)#commit`	Committing the configurations

Interface and loopback configuration:

`(config)#interface xe7`	Enter Interface mode for xe7
`(config-if)#switchport`	Make it L2 interface
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe8`	Enter Interface mode for xe8
`(config-if)#ip add 10.10.10.1/24`	Configuring the ip address in the network side
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface lo`	Enter Interface mode for lo
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure loopback ip address as 1.1.1.1 for VTEP1

© 2021 IP Infusion Inc. Proprietary

`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#commit`	Committing the interface configurations

OSPF configuration:

`(config)#router ospf 1`	Enter into router OSPF mode
`(config-router)#ospf router-id 1.1.1.1`	Configure router-id as 1.1.1.1 (lo ip address)
`(config-router)#network 1.1.1.1/32 area 0.0.0.0`	Add 1.1.1.1 (lo ip address) network into area 0
`(config-router)#network 10.10.10.0/24 area 0.0.0.0`	Add 10.10.10.0(Spine) network into area 0
`(config-router)#bfd all-interfaces`	Enabling bfd on all ospf interface for fast convergence
`(config-router)#exit`	Exit Interface mode and return to Configure mode.
`(config)#commit`	Committing the ospf configurations

BGP configuration:

`(config)#router bgp 1`	Enter into Router BGP mode
`(config-router)#bgp router-id 1.1.1.1`	Configure router-id as 1.1.1.1 (lo ip address)
`(config-router)#neighbor 2.2.2.2 remote-as 1`	Specify a VTEP2 loopback ip address and remote-as defined
`(config-router)#neighbor 2.2.2.2 update-source lo`	Configure update as loopback for VTEP2
`(config-router)#neighbor 2.2.2.2 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for VTEP2
`(config-router)#address-family l2vpn evpn`	Enter into l2vpn EVPN address family mode
`(config-router-af)#neighbor 2.2.2.2 activate`	Activate 2.2.2.2(VTEP2) into l2vpn evpn address family mode
`(config-router-af)#exit-address-family`	Exit from l2vpn address family mode
`(config-router)#exit`	Exit from Router BGP mode and enter into config mode
`(config)#commit`	Committing the bgp configurations

L2 MAC VRF Configuration:

`(config)#mac vrf L2VRF1`	Create mac routing/forwarding instance with L2VRF1 name and enter into vrf mode
`(config-vrf)#rd 1.1.1.1:1`	Assign RD value
`(config-vrf)#route-target both 1:1`	Assign route-target value for same for import and export. Should be same on all node for L2VRF1
`(config-vrf)#exit`	Exit from vrf mode
`(config)#commit`	Committing the vrf configurations

L2 VXLAN configuration:

`(config)#nvo vxlan enable`	Enable VXLAN
`(config)#nvo vxlan vtep-ip-global 1.1.1.1`	Configure Source vtep-ip-global configuration - Use loopback ip address

© 2021 IP Infusion Inc. Proprietary

(config)#nvo vxlan id 100 ingress-replication	Configure VXLAN Network identifier without inner-vid-disabled configured for vxlan trunk access port and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp L2VRF1	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#commit	Committing the vxlan configurations

VTEP2

Hardware profile and generic configuration:

#configure terminal	Enter Configure mode.
(config)#qos enable	Enable qos
(config)#commit	Committing the configurations

Interface and loopback configuration:

(config)#interface xe23	Enter Interface mode for xe23
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe14	Enter Interface mode for xe14
(config-if)#ip add 20.20.20.1/24	Configuring the ip address in the network side
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface lo	Enter Interface mode for lo
(config-if)#ip address 2.2.2.2/32 secondary	Configure loopback ip address as 2.2.2.2 for VTEP2
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#commit	Committing the interface configurations

OSPF configuration:

(config)#router ospf 1	Enter into router OSPF mode
(config-router)#ospf router-id 2.2.2.2	Configure router-id as 2.2.2.2 (lo ip address)
(config-router)#network 2.2.2.2/32 area 0.0.0.0	Add 2.2.2.2 (lo ip address) network into area 0
(config-router)#network 20.20.20.0/24 area 0.0.0.0	Add 20.20.20.0(Spine) network into area 0
(config-router)#bfd all-interfaces	Enabling bfd on all ospf interface for fast convergence
(config-router)#exit	Exit Interface mode and return to Configure mode.
(config)#commit	Committing the ospf configurations

BGP configuration:

`(config)#router bgp 1`	Enter into Router BGP mode
`(config-router)#bgp router-id 2.2.2.2`	Configure router-id as 2.2.2.2 (lo ip address)
`(config-router)#neighbor 1.1.1.1 remote-as 1`	Specify a VTEP1 loopback ip address and remote-as defined
`(config-router)#neighbor 1.1.1.1 update-source lo`	Configure update as loopback for VTEP2
`(config-router)#neighbor 1.1.1.1 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for VTEP1
`(config-router)#address-family l2vpn evpn`	Enter into l2vpn EVPN address family mode
`(config-router-af)#neighbor 1.1.1.1 activate`	Activate 1.1.1.1(VTEP1) into l2vpn evpn address family mode
`(config-router-af)#exit-address-family`	Exit from l2vpn address family mode
`(config-router)#exit`	Exit from Router BGP mode and enter into config mode
`(config)#commit`	Committing the bgp configurations

L2 MAC VRF Configuration:

`(config)#mac vrf L2VRF1`	Create mac routing/forwarding instance with L2VRF1 name and enter into vrf mode
`(config-vrf)#rd 2.2.2.2:1`	Assign RD value
`(config-vrf)#route-target both 1:1`	Assign route-target value for same for import and export. Should be same on all node for L2VRF1
`(config-vrf)#exit`	Exit from vrf mode
`(config)#commit`	Committing the vrf configurations

L2 VXLAN configuration:

`(config)#nvo vxlan enable`	Enable VXLAN
`(config)#nvo vxlan vtep-ip-global 2.2.2.2`	Configure Source vtep-ip-global configuration - Use loopback ip address
`(config)#nvo vxlan id 100 ingress-replication`	Configure VXLAN Network identifier without inner-vid-disabled configured for vxlan trunk access port and enter into VXLAN tenant mode
`(config-nvo)#vxlan host-reachability-protocol evpn-bgp L2VRF1`	Assign vrf for evpn-bgp to carry EVPN route
`(config-nvo)#exit`	Exit from VXLAN tenant mode and enter into configuration mode.
`(config)#commit`	Committing the vxlan configurations

SPINE

Spine node where all VTEPs are connected.

© 2021 IP Infusion Inc. Proprietary

Generic configuration:

`#configure terminal`	Enter Configure mode.
`(config)#qos enable`	Enabling qos
`(config)#commit`	Committing the configuration

Interface configuration:

`(config)#interface xe8`	Enter Interface mode for xe8
`(config-if)#ip address 10.10.10.2/24`	Configure ip address as 10.10.10.2 on network side of VTEP1
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config) interface xe14`	Enter into ce5/1 interface mode
`(config-if)#ip address 20.20.20.2/24`	Configure ip address as 20.20.20.2 on network side of VTEP2
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config) commit`	Committing the configuration

OSPF configuration:

`(config)#router ospf 1`	Enter into router OSPF mode
`(config-router)#ospf router-id 3.3.3.3`	Configure router-id as 3.3.3.3
`(config-router)#network 10.10.10.0/24 area 0.0.0.0`	Add 10.10.10.0 (VTEP1) network into area 0
`(config-router)#network 20.20.20.0/24 area 0.0.0.0`	Add 20.20.20.0 (VTEP2) network into area 0
`(config-router)#bfd all-interfaces`	Enabling bfd on all ospf interface for fast convergence
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)commit`	Committing the ospf configuration

VxLAN Trunk Access port as default

In VxLAN, most of the use cases demand to carry the complete traffic received on the access interface to another VTEP access-port. Hence this support of accepting all tagged and untagged traffic received on the mapped physical port.

VTEP1

(config)#nvo vxlan access-if port xe7 default	Configuring the vxlan access port as default to receive untagged, single and double tagged traffic
(config-nvo-acc-if)#map vnid 100	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#arp-cache disable	Disable arp-cache - mandatory
(config-nvo-acc-if)#nd-cache disable	Disable nd-cache - mandatory
(config-nvo-acc-if)# mac 0000.1111.0001	Configure static mac-only
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#commit	Committing the vxlan configuration

VTEP2

(config)#nvo vxlan access-if port xe23 default	Configuring the vxlan access port as default to receive untagged, single and double tagged traffic
(config-nvo-acc-if)#map vnid 100	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#arp-cache disable	Disable arp-cache - mandatory
(config-nvo-acc-if)#nd-cache disable	Disable nd-cache - mandatory
(config-nvo-acc-if)# mac 0000.2222.0001	Configure static mac-only
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#commit	Committing the vxlan configuration

Validation

VTEP1

```
VTEP1#sh run nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 1.1.1.1
!
nvo vxlan id 100 ingress-replication
 vxlan host-reachability-protocol evpn-bgp L2VRF1
!
nvo vxlan access-if port xe7 default
 map vnid 100
 arp-cache disable
 nd-cache disable
 mac 0000.1111.0001
!
```


© 2021 IP Infusion Inc. Proprietary

```
!
VTEP1#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status           Up/Down        Update
================================================================================
1.1.1.1          2.2.2.2          Installed        00:02:49       00:02:49

Total number of entries are 1
VTEP1#sh nvo vxlan mac-table
================================================================================================
================================================
                                                          VXLAN MAC Entries
================================================================================================
================================================
VNID     Interface VlanId Vlan-RangeId Inner-VlanId Mac-Addr     VTEP-Ip/ESI
Type             Status     AccessPortDesc
________________________________________________________________________________________________
________________________________________________

100      xe7      ----   ----       ----       0000.1111.0001 1.1.1.1
Static Local    -------    -------
100        ----      ----   ----         0000.2222.0001 2.2.2.2
Static Remote   -------    -------
100      xe7      ----   ----       ----       b0da.1d10.6496 1.1.1.1
Dynamic Local   -------    -------

Total number of entries are : 3

VTEP1#sh nvo vxlan mac-table hardware
================================================================================================
================================================
                                                          VXLAN MAC Entries
================================================================================================
================================================
VNID     Interface VlanId Vlan-RangeId Inner-VlanId Mac-Addr     VTEP-Ip/ESI
Type             Status     Time-out AccessPortDesc
________________________________________________________________________________________________
________________________________________________

100        xe7       ----   ----         0000.1111.0001 1.1.1.1
Static Local    -------    ---      -------
100        ---       ----   ----         0000.2222.0001 2.2.2.2
Remote          -------    ---      -------
100        xe7       ----   ----         b0da.1d10.6496 1.1.1.1
Dynamic Local   -------    300      -------

Total number of entries are 3
VTEP1#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
```

```
VNID     VNI-Name     VNI-Type Type Interface ESI                          VLAN DF-Status
Src-Addr          Dst-Addr
_____________________________________________________________________________________________
_____________________________________
100      ----         L2       NW   ----      ----                         ---- ----
1.1.1.1           2.2.2.2
100      ----         --       AC   xe7       --- Single Homed Port ---     ---- ----
----              ----

Total number of entries are 2
VTEP1#sh nvo vxlan route-count
VXLAN Active route count information
==================================
Max route count   : 32768
Active route count: 3

---------------------------------------------
 VNID     Total    MACONLY  MACIPv4  MACIPv6
---------------------------------------------
 100      3        3        0        0

Total number of entries are 1
VTEP1#sh nvo vxlan access-if-config
nvo vxlan access-if port xe7 default
 map vnid 100
 arp-cache disable
 nd-cache disable
 mac 0000.1111.0001
!
VTEP1#sh nvo vxlan access-if brief

                 Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
xe7        ---   ---   500000   100       up      up

Total number of entries are 1
VTEP1#sh bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 1
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
2.2.2.2                 4    1   15        17      2     0     0  00:04:52
2      0      1      1      0      0

Total number of neighbors 1

Total number of Established sessions 1
VTEP1#sh bgp l2vpn evpn
```


© 2021 IP Infusion Inc. Proprietary

```
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, a add-path, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

   Network          Next Hop            Metric    LocPrf      Weight     Path  Peer
Encap

RD[1.1.1.1:1] VRF[L2VRF1]:
*>   [2]:[0]:[100]:[48,0000:1111:0001]:[0]:[100]
                      1.1.1.1              0        100       32768  i  ----------
VXLAN
* i  [2]:[0]:[100]:[48,0000:2222:0001]:[0]:[100]
                     2.2.2.2              0        100       0    i  2.2.2.2        VXLAN
*>   [2]:[0]:[100]:[48,b0da:1d10:6496]:[0]:[100]
                      1.1.1.1              0        100       32768  i  ----------
VXLAN
*>   [3]:[100]:[32,1.1.1.1]
                      1.1.1.1              0        100       32768  i  ----------
VXLAN
* i  [3]:[100]:[32,2.2.2.2]
                     2.2.2.2              0        100       0    i  2.2.2.2        VXLAN

RD[2.2.2.2:1]
*>i  [2]:[0]:[100]:[48,0000:2222:0001]:[0]:[100]
                     2.2.2.2              0        100       0    i  2.2.2.2        VXLAN
*>i  [3]:[100]:[32,2.2.2.2]
                     2.2.2.2              0        100       0    i  2.2.2.2        VXLAN

Total number of prefixes 7
VTEP1#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
============================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left

_____________________________________________________________________________
Total number of entries are 0
VTEP1#sh nvo vxlan nd-cache
VXLAN ND-CACHE Information
============================
VNID     Ip-Addr                                 Mac-Addr       Type         Age-Out
Retries-Left

_____________________________________________________________________________
_____________
Total number of entries are 0
```

```
VTEP1#
```

VTEP2

```
VTEP2#sh run nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 2.2.2.2
!
nvo vxlan id 100 ingress-replication
 vxlan host-reachability-protocol evpn-bgp L2VRF1
!
nvo vxlan access-if port xe23 default
 map vnid 100
 arp-cache disable
 nd-cache disable
 mac 0000.2222.0001
!
!
VTEP2#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
Source            Destination      Status           Up/Down        Update
================================================================================
2.2.2.2           1.1.1.1          Installed        00:05:47       00:05:47

Total number of entries are 1
VTEP2#sh nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface ESI                            VLAN DF-Status
Src-Addr          Dst-Addr
_____________________________________________________________________________________________
_____________________________________
100      ----         L2       NW   ----      ----                           ---- ----
2.2.2.2           1.1.1.1
100      ----         --       AC   xe23      --- Single Homed Port ---      ---- ----
----              ----

Total number of entries are 2
VTEP2#sh nvo vxlan mac-table
================================================================================
================================================
                                                        VXLAN MAC Entries
================================================================================
================================================
```


© 2021 IP Infusion Inc. Proprietary

```
VNID     Interface VlanId Vlan-RangeId Inner-VlanId Mac-Addr     VTEP-Ip/ESI
Type             Status     AccessPortDesc
_____________________________________________________________________________________________
_____________________________________________________

100        ----      ----   ----         0000.1111.0001 1.1.1.1
Static Remote   -------    -------
100      xe23     ----   ----       ----       0000.2222.0001 2.2.2.2
Static Local    -------    -------
100        ----      ----   ----         b0da.1d10.6496 1.1.1.1
Dynamic Remote  -------    -------

Total number of entries are : 3

VTEP2#sh nvo vxlan mac-table hardware
=============================================================================================
=================================================
                                                                VXLAN MAC Entries
=============================================================================================
=================================================
VNID     Interface VlanId Vlan-RangeId Inner-VlanId Mac-Addr     VTEP-Ip/ESI
Type             Status     Time-out AccessPortDesc
_____________________________________________________________________________________________
_____________________________________________________

100        ---       ----   ----         0000.1111.0001 1.1.1.1
Remote          -------    ---      -------
100        xe23      ----   ----         0000.2222.0001 2.2.2.2
Static Local    -------    ---      -------
100        ---       ----   ----         b0da.1d10.6496 1.1.1.1
Remote          -------    ---      -------

Total number of entries are 3
VTEP2#sh nvo vxlan route-count
VXLAN Active route count information
==================================
Max route count   : 32768
Active route count: 3

-------------------------------------------
 VNID     Total    MACONLY  MACIPv4  MACIPv6
-------------------------------------------
 100      3        3        0        0

Total number of entries are 1
VTEP2#sh nvo vxlan access-if br

                 Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
xe23       ---   ---   500000   100       up      up

Total number of entries are 1
```

```
VTEP2#sh nvo vxlan access-if-config
nvo vxlan access-if port xe23 default
 map vnid 100
 arp-cache disable
 nd-cache disable
 mac 0000.2222.0001
!
VTEP2#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left

_____________________________________________________________________________
Total number of entries are 0
VTEP2#sh nvo vxlan nd-cache
VXLAN ND-CACHE Information
===========================
VNID     Ip-Addr                                  Mac-Addr       Type         Age-Out
Retries-Left

_____________________________________________________________________________________________
_____________
Total number of entries are 0

VTEP2#
VTEP2#sh bgp l2vpn evpn summary
BGP router identifier 2.2.2.2, local AS number 1
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
1.1.1.1                 4     1   27        27      1     0     0  00:09:54
3      0      2      1      0      0

Total number of neighbors 1

Total number of Established sessions 1
VTEP2#sh bgp l2vpn evpn
BGP table version is 2, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, a add-path, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route
```


© 2021 IP Infusion Inc. Proprietary

```
   Network          Next Hop            Metric    LocPrf      Weight     Path  Peer
Encap

RD[1.1.1.1:1]
*>i  [2]:[0]:[100]:[48,0000:1111:0001]:[0]:[100]
                     1.1.1.1             0        100       0    i  1.1.1.1         VXLAN
*>i  [2]:[0]:[100]:[48,b0da:1d10:6496]:[0]:[100]
                     1.1.1.1             0        100       0    i  1.1.1.1         VXLAN
*>i  [3]:[100]:[32,1.1.1.1]
                     1.1.1.1             0        100       0    i  1.1.1.1         VXLAN

RD[2.2.2.2:1] VRF[L2VRF1]:
* i  [2]:[0]:[100]:[48,0000:1111:0001]:[0]:[100]
                     1.1.1.1             0        100       0    i  1.1.1.1         VXLAN
*>   [2]:[0]:[100]:[48,0000:2222:0001]:[0]:[100]
                      2.2.2.2              0        100       32768  i  ----------
VXLAN
* i  [2]:[0]:[100]:[48,b0da:1d10:6496]:[0]:[100]
                     1.1.1.1             0        100       0    i  1.1.1.1         VXLAN
* i  [3]:[100]:[32,1.1.1.1]
                     1.1.1.1             0        100       0    i  1.1.1.1         VXLAN
*>   [3]:[100]:[32,2.2.2.2]
                      2.2.2.2              0        100       32768  i  ----------
VXLAN

Total number of prefixes 8
VTEP2#
```

VxLAN Trunk access port with vlan range

When access port with a specific vlan range configured, all the traffic in that specific range are accepted and forwaded.

VTEP1

`(config)#nvo vxlan access-if port-vlan xe7 2-100`	Configuring the vxlan access port with vlan range 2-100 where traffic in the vlan range 2-100 are accepted
`(config-nvo-acc-if)#map vnid 100`	Map VXLAN Identified to access-port for VXLAN
`(config-nvo-acc-if)#arp-cache disable`	Disable arp-cache - mandatory
`(config-nvo-acc-if)#nd-cache disable`	Disable nd-cache - mandatory
`(config-nvo-acc-if)# mac 0000.1111.0001`	Configure static mac-only
`(config-nvo-acc-if)#exit`	Exit from VXLAN access-interface mode and enter into configuration mode
`(config)#commit`	Committing the vxlan configuration

VTEP2

(config)#nvo vxlan access-if port-vlan xe23 2-100	Configuring the vxlan access port with vlan range 2-100 where traffic in the vlan range 2-100 are accepted
(config-nvo-acc-if)#map vnid 100	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#arp-cache disable	Disable arp-cache - mandatory
(config-nvo-acc-if)#nd-cache disable	Disable nd-cache - mandatory
(config-nvo-acc-if)# mac 0000.2222.0001	Configure static mac-only
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#commit	Committing the vxlan configuration

Validations

VTEP1

```
VTEP1#sh run nvo vx
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 1.1.1.1
!
nvo vxlan id 100 ingress-replication
 vxlan host-reachability-protocol evpn-bgp L2VRF1
!
nvo vxlan access-if port-vlan xe7 2-100
 map vnid 100
 arp-cache disable
 nd-cache disable
 mac 0000.1111.0001
!
!
VTEP1#
VTEP1#sh nvo vxlan tunnel summary

Total number of entries: 1 [Installed: 1, Resolved: 0, Unresolved: 0]

Total number of entries are 1
VTEP1#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status           Up/Down        Update
================================================================================
1.1.1.1          2.2.2.2          Installed        00:20:10       00:20:10

Total number of entries are 1
VTEP1#sh nvo vx
VXLAN Information
=================
```


© 2021 IP Infusion Inc. Proprietary

```
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID    VNI-Name    VNI-Type Type Interface ESI                          VLAN DF-Status
Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________
100     ----        L2       NW   ----     ----                         ---- ----
1.1.1.1          2.2.2.2
100     ----        --       AC   xe7      --- Single Homed Port ---     2    ----
----             ----

Total number of entries are 2
VTEP1#sh nvo vxlan mac-table
=====================================================================================
================================================
                                                          VXLAN MAC Entries
=====================================================================================
================================================
VNID    Interface VlanId Vlan-RangeId Inner-VlanId Mac-Addr     VTEP-Ip/ESI
Type            Status     AccessPortDesc
_____________________________________________________________________________________
_____________________________________________

100      xe7     -----      2-100 ----       0000.1111.0001 1.1.1.1
Static Local    -------    -------
100       ----      ----   ----         0000.2222.0001 2.2.2.2
Static Remote   -------    -------
100      xe7     -----      2-100 ----       b0da.1d10.6496 1.1.1.1
Dynamic Local   -------    -------

Total number of entries are : 3

VTEP1#sh nvo vxlan mac-table hardware
=====================================================================================
================================================
                                                          VXLAN MAC Entries
=====================================================================================
================================================
VNID    Interface VlanId Vlan-RangeId Inner-VlanId Mac-Addr     VTEP-Ip/ESI
Type            Status     Time-out AccessPortDesc
_____________________________________________________________________________________
_____________________________________________

100      xe7     -----      2-100 ----       0000.1111.0001 1.1.1.1
Static Local    -------    ---      -------
100       ---       ----   ----         0000.2222.0001 2.2.2.2
Remote          -------    ---      -------
100      xe7     -----      2-100 ----       b0da.1d10.6496 1.1.1.1
Dynamic Local   -------    300      -------

Total number of entries are 3
VTEP1#sh nvo vxlan arp-cache
```

```
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
Total number of entries are 0
VTEP1#sh nvo vxlan nd-cache
VXLAN ND-CACHE Information
===========================
VNID     Ip-Addr                                  Mac-Addr       Type         Age-Out
Retries-Left
_____________________________________________________________________________
_____________
Total number of entries are 0
VTEP1#sh nvo vxlan access-if-config
nvo vxlan access-if port-vlan xe7 2-100
 map vnid 100
 arp-cache disable
 nd-cache disable
 mac 0000.1111.0001
!
VTEP1#sh nvo vxlan access-if brief

                 Inner                     Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
xe7        2     ---   500000   100       up      up

Total number of entries are 1
VTEP1#
VTEP1#sh nvo vxlan route-count
VXLAN Active route count information
====================================
Max route count   : 32768
Active route count: 3

-----------------------------------------
 VNID     Total    MACONLY  MACIPv4  MACIPv6
-----------------------------------------
 100      3        3        0        0

Total number of entries are 1
VTEP1#sh bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 1
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
2.2.2.2                 4    1   58        61      5     0     0  00:22:05
2      0      1      1      0      0
```


© 2021 IP Infusion Inc. Proprietary

```
Total number of neighbors 1

Total number of Established sessions 1
VTEP1#sh bgp l2vpn evpn
BGP table version is 5, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, a add-path, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

   Network         Next Hop           Metric    LocPrf      Weight     Path  Peer
Encap

RD[1.1.1.1:1] VRF[L2VRF1]:
*>   [2]:[0]:[100]:[48,0000:1111:0001]:[0]:[100]
                      1.1.1.1              0        100       32768  i  ----------
VXLAN
* i  [2]:[0]:[100]:[48,0000:2222:0001]:[0]:[100]
                     2.2.2.2              0        100       0    i  2.2.2.2        VXLAN
*>   [2]:[0]:[100]:[48,b0da:1d10:6496]:[0]:[100]
                      1.1.1.1              0        100       32768  i  ----------
VXLAN
*>   [3]:[100]:[32,1.1.1.1]
                      1.1.1.1              0        100       32768  i  ----------
VXLAN
* i  [3]:[100]:[32,2.2.2.2]
                     2.2.2.2              0        100       0    i  2.2.2.2        VXLAN

RD[2.2.2.2:1]
*>i  [2]:[0]:[100]:[48,0000:2222:0001]:[0]:[100]
                     2.2.2.2              0        100       0    i  2.2.2.2        VXLAN
*>i  [3]:[100]:[32,2.2.2.2]
                     2.2.2.2              0        100       0    i  2.2.2.2        VXLAN

Total number of prefixes 7
```

VTEP2

```
VTEP2#sh run nvo vxlan
!
nvo vxlan enable
!
nvo vxlan vtep-ip-global 2.2.2.2
```

```
!
nvo vxlan id 100 ingress-replication
 vxlan host-reachability-protocol evpn-bgp L2VRF1
!
nvo vxlan access-if port-vlan xe23 2-100
 map vnid 100
 arp-cache disable
 nd-cache disable
 mac 0000.2222.0001
!
!
VTEP2#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status           Up/Down        Update
================================================================================
2.2.2.2          1.1.1.1          Installed        00:19:28       00:19:28

Total number of entries are 1
VTEP2#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status           Up/Down        Update
================================================================================
2.2.2.2          1.1.1.1          Installed        00:21:06       00:21:06

Total number of entries are 1
VTEP2#sh nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
           AC - Access Port
          (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface ESI                            VLAN DF-Status
Src-Addr         Dst-Addr
_____________________________________________________________________________________________
_____________________________________
100      ----         L2       NW   ----      ----                           ---- ----
2.2.2.2          1.1.1.1
100      ----         --       AC   xe23      --- Single Homed Port ---     2    ----
----             ----

Total number of entries are 2
VTEP2#sh nvo vxlan mac-table
================================================================================================
================================================
                                                                VXLAN MAC Entries
================================================================================================
================================================
VNID     Interface VlanId Vlan-RangeId Inner-VlanId Mac-Addr     VTEP-Ip/ESI
Type             Status     AccessPortDesc
_____________________________________________________________________________________________
_____________________________________________
```


© 2021 IP Infusion Inc. Proprietary

```
100        ----      ----   ----         0000.1111.0001 1.1.1.1
Static Remote   -------    -------
100       xe23     -----       2-100 ----       0000.2222.0001 2.2.2.2
Static Local    -------    -------
100        ----      ----   ----         b0da.1d10.6496 1.1.1.1
Dynamic Remote  -------    -------

Total number of entries are : 3

VTEP2#sh nvo vxlan mac-table hardware
================================================================================
================================================
                                                          VXLAN MAC Entries
================================================================================================
================================================
VNID     Interface VlanId Vlan-RangeId Inner-VlanId Mac-Addr     VTEP-Ip/ESI
Type             Status     Time-out AccessPortDesc
________________________________________________________________________________________________
_____________________________________________

100        ---       ----   ----         0000.1111.0001 1.1.1.1
Remote          -------    ---      -------
100       xe23     -----       2-100 ----       0000.2222.0001 2.2.2.2
Static Local    -------    ---      -------
100        ---       ----   ----         b0da.1d10.6496 1.1.1.1
Remote          -------    ---      -------

Total number of entries are 3
VTEP2#sh nvo vxlan route-count
VXLAN Active route count information
====================================
Max route count   : 32768
Active route count: 3

-------------------------------------------
 VNID     Total    MACONLY  MACIPv4  MACIPv6
-------------------------------------------
 100      3        3        0        0

Total number of entries are 1
VTEP2#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
Total number of entries are 0
VTEP2#sh nvo vxlan nd-cache
VXLAN ND-CACHE Information
===========================
VNID     Ip-Addr                                  Mac-Addr       Type         Age-Out
Retries-Left
```

```
_____________________________________________________________________________________
_____________
Total number of entries are 0
VTEP2#
VTEP2#
VTEP2#sh nvo vxlan access-if brief

                 Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
xe23       2     ---   500000   100       up      up

Total number of entries are 1
VTEP2#sh nvo vxlan access-if-config
nvo vxlan access-if port-vlan xe23 2-100
 map vnid 100
 arp-cache disable
 nd-cache disable
 mac 0000.2222.0001
!
VTEP2#sh bgp l2vpn evpn summary
BGP router identifier 2.2.2.2, local AS number 1
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
1.1.1.1                 4    1   59        57      3     0     0  00:21:48
3      0      2      1      0      0

Total number of neighbors 1

Total number of Established sessions 1
VTEP2#sh bgp l2vpn evpn
BGP table version is 4, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, a add-path, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

   Network         Next Hop           Metric    LocPrf      Weight     Path  Peer
Encap
```


© 2021 IP Infusion Inc. Proprietary

```
RD[1.1.1.1:1]
*>i  [2]:[0]:[100]:[48,0000:1111:0001]:[0]:[100]
                     1.1.1.1             0       100       0    i  1.1.1.1         VXLAN
*>i  [2]:[0]:[100]:[48,b0da:1d10:6496]:[0]:[100]
                     1.1.1.1             0       100       0    i  1.1.1.1         VXLAN
*>i  [3]:[100]:[32,1.1.1.1]
                     1.1.1.1             0       100       0    i  1.1.1.1         VXLAN

RD[2.2.2.2:1] VRF[L2VRF1]:
* i  [2]:[0]:[100]:[48,0000:1111:0001]:[0]:[100]
                     1.1.1.1             0       100       0    i  1.1.1.1         VXLAN
*>   [2]:[0]:[100]:[48,0000:2222:0001]:[0]:[100]
                      2.2.2.2              0        100       32768  i  ----------
VXLAN
* i  [2]:[0]:[100]:[48,b0da:1d10:6496]:[0]:[100]
                     1.1.1.1             0       100       0    i  1.1.1.1         VXLAN
* i  [3]:[100]:[32,1.1.1.1]
                     1.1.1.1             0       100       0    i  1.1.1.1         VXLAN
*>   [3]:[100]:[32,2.2.2.2]
                      2.2.2.2              0        100       32768  i  ----------
VXLAN

Total number of prefixes 8
VTEP2#
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 9 VXLAN Tunnel Over SVI

This chapter contains the configurations for VXLAN Tunnel Over SVI.

Overview

VxLAN EVPN solution is envisioned to simplify the topology and configurations in Data Centers (DC). In Data Centers, CLOS topology was used, which makes network side pure L3 and uses EBGP as IGP.

VxLAN solution is required for Service Providers (SP) as well to run few of the services or all services in their network over VxLAN. When they choose to run few services over VxLAN, then on the network side there will be a need to run VxLAN over SVI.

Topology

The Topology shown below contains the 3 VTEPS i.e VTEP1 ,VTEP2 and VTEP3 and 3 core nodes P1 ,P2 and P3. Vxlan tunnel will be established between VTEPS over SVI interfaces. OSPF as IGP will be running between VTEPS and the core node to provide the end to end connectivity. Switch is connected between host and VTEP-1, VTEP-2 via dynamic LAG.

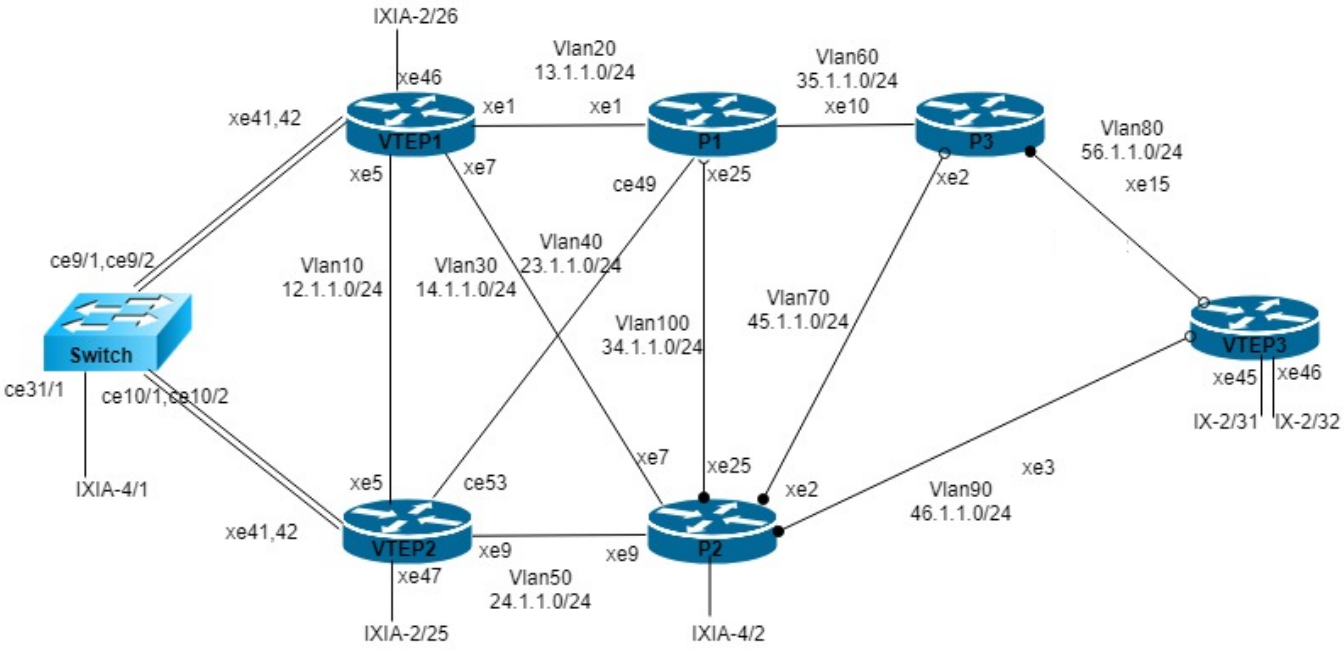


Figure 9-79: VXLAN over SVI

RTR1/VTEP1

`VTEP1#configure terminal`	Enter configuration terminal
`VTEP1(config)#hostname VTEP1`	Configure hostname

`VTEP1(config)#mac vrf vrf1`	Configure MAC vrf vrf1
`VTEP1(config-vrf)#rd 1.1.1.1:11`	Configure RD for vrf1
`VTEP1(config-vrf)#route-target both 10.10.10.10:100`	Configure RT for vrf1
`VTEP1(config-vrf)#mac vrf vrf2`	Configure MAC vrf vrf2
`VTEP1(config-vrf)#rd 1.1.1.1:12`	Configure RD for vrf2
`VTEP1(config-vrf)#route-target both 10.10.10.10:102`	Configure RT for vrf2
`VTEP1(config-vrf)#bfd interval 3 minrx 3 multiplier 3`	Configure BFD interval globally
`VTEP1(config)#evpn vxlan multihoming enable`	Enable EVPN VXLAN multihoming
`VTEP1(config)#nvo vxlan enable`	Enable VXLAN
`VTEP1(config)#qos enable`	Enable qos
`VTEP1(config)#qos statistics`	Enable qos statistics
`VTEP1(config)#bridge 1 protocol ieee vlan-bridge`	Configure IEEE VLAN bridge
`VTEP1(config)#no bridge 1 spanning-tree enable`	Disable spanning tree in bridge 1 globally
`VTEP1(config)#no igmp snooping`	Disable igmp snooping messages globally
`VTEP1(config)#vlan database`	Enter into the VLAN database
`VTEP1(config-vlan)#vlan 10-200 bridge 1 state enable`	Configure VLAN 10-200 and associate with bridge 1
`VTEP1(config-vlan)#vlan 4000 bridge 1 state enable`	Configure VLAN 4000 and associate with bridge 1
`VTEP1(config-vlan)#interface po1`	Enter interface mode
`VTEP1(config-if)#switchport`	Set the interface as Layer2 port
`VTEP1(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP1(config-if)#evpn multi-homed system-mac aa22.3344.5566`	Configure EVPN system-MAC
`VTEP1(config-if)#interface lo`	Enter lo interface mode
`VTEP1(config-if)#ip address 1.1.1.1/32 secondary`	Assign loopback IP
`VTEP1(config-if)#interface vlan1.10`	Specify interface VLAN1.10 to be configured.
`VTEP1(config-if)#ip address 12.1.1.1/24`	Assign IP address
`VTEP1(config-if)#ip ospf cost 1`	Change OSPF cost of the link
`VTEP1(config-if)#interface vlan1.20`	Specify interface VLAN1.20 to be configured.
`VTEP1(config-if)#ip address 13.1.1.1/24`	Assign IP address
`VTEP1(config-if)#ip ospf cost 1`	Change OSPF cost of the link
`VTEP1(config-if)#interface vlan1.30`	Specify interface VLAN1.30 to be configured.
`VTEP1(config-if)#ip address 14.1.1.1/24`	Assign IP address
`VTEP1(config-if)#ip ospf cost 1`	Change OSPF cost of the link
`VTEP1(config-if)#interface xe1`	Enter interface mode
`VTEP1(config-if)#switchport`	Set the interface as Layer2 port

© 2021 IP Infusion Inc. Proprietary

VTEP1(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
VTEP1(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
VTEP1(config-if)#switchport trunk allowed vlan add 20,29	Enable VLAN's allowed on this interface.
VTEP1(config-if)#switchport trunk native vlan 29	Configure native VLAN
VTEP1(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
VTEP1(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
VTEP1(config-if)#interface xe5	Enter interface mode
VTEP1(config-if)#switchport	Set the interface as Layer2 port
VTEP1(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
VTEP1(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
VTEP1(config-if)#switchport trunk allowed vlan add 10,19	Enable VLAN's allowed on this interface.
VTEP1(config-if)#switchport trunk native vlan 19	Configure native VLAN
VTEP1(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
VTEP1(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
VTEP1(config-if)#interface xe7	Enter interface mode
VTEP1(config-if)#switchport	Set the interface as Layer2 port
VTEP1(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
VTEP1(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
VTEP1(config-if)#switchport trunk allowed vlan add 30,39	Enable VLAN's allowed on this interface.
VTEP1(config-if)#switchport trunk native vlan 39	Configure native VLAN
VTEP1(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
VTEP1(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
VTEP1(config-if)#interface xe41	Enter interface mode
VTEP1(config-if)#channel-group 1 mode active	Map this interface to po1
VTEP1(config-if)#interface xe42	Enter interface mode
VTEP1(config-if)#channel-group 1 mode active	Map this interface to po1
VTEP1(config-if)#interface xe46	Enter interface mode
VTEP1(config-if)#switchport	Map this interface to po1
VTEP1(config-if)#router ospf 1	Enter OSPF configuration mode
VTEP1(config-router)#ospf router-id 1.1.1.1	Configure OSPF router id
VTEP1(config-router)#bfd all-interfaces	Enable BFD in all OSPF interfaces
VTEP1(config-router)#network 1.1.1.1/32 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.

`VTEP1(config-router)#network 12.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP1(config-router)#network 13.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP1(config-router)#network 14.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP1(config-router)#router bgp 100`	Enter Router BGP mode and define the AS number 100.
`VTEP1(config-router)#address-family ipv4 unicast`	Enter address-family IPv4 unicast mode
`VTEP1(config-router)#network 1.1.1.1/32`	Add the lo network to BGP route
`VTEP1(config-router-af)#neighbor 2.2.2.2 activate`	Activate neigbors
`VTEP1(config-router-af)#neighbor 6.6.6.6 activate`	Activate neigbors
`VTEP1(config-router-af)#exit-address-family`	Exit address-family mode.
`VTEP1(config-router)#neighbor 2.2.2.2 remote-as 100`	Configure BGP remote-as 100 with neighbor IP
`VTEP1(config-router)#neighbor 2.2.2.2 update-source lo`	Define BGP neighbors, to update the source routes with lo
`VTEP1(config-router)#neighbor 2.2.2.2 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for VTEP2
`VTEP1(config-router)#neighbor 6.6.6.6 remote-as 100`	Configure BGP remote-as 100 with neighbor IP
`VTEP1(config-router)#neighbor 6.6.6.6 update-source lo`	Define BGP neighbors, to update the source routes with lo
`VTEP1(config-router)#neighbor 6.6.6.6 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for VTEP3
`VTEP1(config-router)#address-family l2vpn evpn`	Enter in to BGP L2VPN EVPN address-family
`VTEP1(config-router-af)#neighbor 2.2.2.2 activate`	Activate neigbors
`VTEP1(config-router-af)#neighbor 6.6.6.6 activate`	Activate neigbors
`VTEP1(config-router-af)#exit-address-family`	Exit from BGP L2VPN EVPN address-family
`VTEP1(config-router)#nvo vxlan vtep-ip-global 1.1.1.1`	Configure VXLAN global IP
`VTEP1(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled`	Create VNID 1
`VTEP1(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1`	Associate VNID with EVPN and vrf1
`VTEP1(config-nvo)#nvo vxlan id 1000 ingress-replication inner-vid-disabled`	Create VNID 1000
`VTEP1(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf2`	Associate VNID with EVPN and vrf2
`VTEP1(config-nvo-acc-if)#nvo vxlan access-if port-vlan po1 2000`	Create VXLAN access port port-vlan
`VTEP1(config-nvo-acc-if)#no shutdown`	Unshut the access interface
`VTEP1(config-nvo-acc-if)#map vnid 1000`	Map the VNID to access-if

© 2021 IP Infusion Inc. Proprietary

VTEP1(config-nvo)#nvo vxlan access-if port xe46	Create VXLAN access port
VTEP1(config-nvo-acc-if)#no shutdown	Unshut the access interface
VTEP1(config-nvo-acc-if)#map vnid 1	Map the VNID to access-if
VTEP1(config-nvo-acc-if)#nvo vxlan access-if port-vlan po1 1000	Create VXLAN access port port-vlan
VTEP1(config-nvo-acc-if)#no shutdown	Unshut the access interface
VTEP1(config-nvo-acc-if)#map vnid 1	Map the VNID to access-if
VTEP1(config-nvo-acc-if)#mac 0000.1111.1111 ip 100.1.1.100	Configure static MAC IP
VTEP1(config-nvo-acc-if)#mac 0000.1111.1112	Configure static MAC
VTEP1(config-nvo-acc-if)#mac 0000.1111.1113	Configure static MAC
VTEP1(config-nvo-acc-if)#mac 0000.1111.1114	Configure static MAC
VTEP1(config-nvo-acc-if)#mac 0000.1111.1115	Configure static MAC

VTEP2

VTEP2#configure terminal	Enter configuration terminal
VTEP2(config)#hostname VTEP2	Configure hostname
VTEP2(config)#mac vrf vrf1	Configure MAC VRF vrf1
VTEP2(config-vrf)#rd 2.2.2.2:11	Configure RD for vrf1
VTEP2(config-vrf)#route-target both 10.10.10.10:100	Configure RT for vrf1
VTEP2(config-vrf)#mac vrf vrf2	Configure MAC VRF vrf2
VTEP2(config-vrf)#rd 2.2.2.2:12	Configure RD for vrf2
VTEP2(config-vrf)#route-target both 10.10.10.10:102	Configure RT for vrf2
VTEP2(config)#nvo vxlan enable	Enable VXLAN
VTEP2(config)#evpn vxlan multihoming enable	Enable EVPN VXLAN multihoming
VTEP2(config)#qos enable	Enable QOS
VTEP2(config)#qos statistics	Enable QOS statistics
VTEP2(config)#bridge 1 protocol ieee vlan-bridge	Configure IEEE VLAN bridge
VTEP2(config)#no bridge 1 spanning-tree enable	Disable spanning tree in bridge 1 globally
VTEP2(config)#vlan database	Enter into the VLAN database
VTEP2(config-vlan)#vlan 10-200 bridge 1 state enable	Configure VLAN 10-200 and associate with bridge 1
VTEP2(config-vlan)#interface po2	Enter interface mode
VTEP2(config-if)#switchport	Set the interface as Layer2 port
VTEP2(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
VTEP2(config-if)#evpn multi-homed system-mac aa22.3344.5566	Configure EVPN system-MAC
VTEP2(config-if)#interface lo	Enter interface mode

`VTEP2(config-if)#ip address 2.2.2.2/32 secondary`	Configure loopback IP
`VTEP2(config-if)#interface vlan1.10`	Specify interface VLAN1.10 to be configured.
`VTEP2(config-if)#ip address 12.1.1.2/24`	Assign IP address
`VTEP2(config-if)#interface vlan1.40`	Specify interface VLAN1.40 to be configured.
`VTEP2(config-if)#ip address 23.1.1.1/24`	Assign IP address
`VTEP2(config-if)#ip ospf cost 1`	Change OSPF cost of the link
`VTEP2(config-if)#interface vlan1.50`	Specify interface VLAN1.50 to be configured.
`VTEP2(config-if)#ip address 24.1.1.1/24`	Assign IP address
`VTEP2(config-if)#interface ce53`	Enter interface mode
`VTEP2(config-if)#switchport`	Set the interface as Layer2 port
`VTEP2(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`VTEP2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`VTEP2(config-if)#switchport trunk allowed vlan add 40,49`	Enable VLAN's allowed on this interface.
`VTEP2(config-if)#switchport trunk native vlan 49`	Configure native VLAN
`VTEP2(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP2(config-if)#spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`VTEP2(config-if)#interface xe5`	Enter interface mode
`VTEP2(config-if)#switchport`	Set the interface as Layer2 port
`VTEP2(config-if)#bridge-group 1 spanningtree disable`	Associate the interface with bridge group 1 and disable spanning tree
`VTEP2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode
`VTEP2(config-if)#switchport trunk allowed vlan add 10,19`	Enable VLAN's allowed on this interface
`VTEP2(config-if)#switchport trunk native vlan 19`	Configure native VLAN
`VTEP2(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP2(config-if)#spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`VTEP2(config-if)#interface xe9`	Enter interface mode
`VTEP2(config-if)#switchport`	Set the interface as Layer2 port
`VTEP2(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`VTEP2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`VTEP2(config-if)#switchport trunk allowed vlan add 50,59`	Enable VLAN's allowed on this interface.
`VTEP2(config-if)#switchport trunk native vlan 59`	Configure native VLAN
`VTEP2(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP2(config-if)#spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions

© 2021 IP Infusion Inc. Proprietary

`VTEP2(config-if)#interface xe41`	Enter interface mode
`VTEP2(config-if)#channel-group 1 mode active`	Map the interface to po1
`VTEP2(config-if)#interface xe42`	Enter interface mode
`VTEP2(config-if)#channel-group 1 mode active`	Map the interface to po1
`VTEP2(config-if)#interface xe47`	Enter interface mode
`VTEP2(config-if)#switchport`	Set the interface as Layer2 port
`VTEP2(config-if)#router ospf 1`	Enter OSPF configuration mode
`VTEP2(config-router)#ospf router-id 2.2.2.2`	Configure OSPF router id
`VTEP2(config-router)#network 2.2.2.2/32 area 0.0.0.0`	Enable BFD in all ospf interfaces
`VTEP2(config-router)#network 12.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP2(config-router)#network 23.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP2(config-router)#network 24.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP2(config-router)#network 25.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP2(config-router)#router bgp 100`	Enter Router BGP mode and define the AS number 100.
`VTEP2(config-router)#address-family ipv4 unicast`	Enter address-family IPv4 unicast mode
`VTEP2(config-router)#network 2.2.2.2/32`	Add the lo network to BGP route
`VTEP2(config-router-af)#neighbor 1.1.1.1 activate`	Activate neigbors
`VTEP2(config-router-af)#neighbor 6.6.6.6 activate`	Activate neigbors
`VTEP2(config-router-af)#exit-address-family`	Exit address-family mode.
`VTEP2(config-router)#neighbor 1.1.1.1 remote-as 100`	Configure BGP remote-as 100 with neighbor IP
`(config-router)#neighbor 1.1.1.1 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for VTEP1
`VTEP2(config-router)#neighbor 1.1.1.1 update-source lo`	Define BGP neighbors, to update the source routes with lo
`VTEP2(config-router)#neighbor 6.6.6.6 remote-as 100`	Configure BGP remote-as 100 with neighbor IP
`(config-router)#neighbor 6.6.6.6 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for VTEP3
`VTEP2(config-router)#neighbor 6.6.6.6 update-source lo`	Define BGP neighbors, to update the source routes with lo
`VTEP2(config-router)#address-family l2vpn evpn`	Enter in to BGP L2VPN EVPN address-family
`VTEP2(config-router-af)#neighbor 1.1.1.1 activate`	Activate neigbors
`VTEP2(config-router-af)#neighbor 6.6.6.6 activate`	Activate neigbors
`VTEP2(config-router-af)#exit-address-family`	Exit from BGP L2VPN EVPN address-family

`VTEP2(config-router)#nvo vxlan vtep-ip-global 2.2.2.2`	Configure VXLAN global IP
`VTEP2(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled`	Create VNID 1
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1`	Associate VNID with EVPN and vrf1
`VTEP2(config-nvo)#nvo vxlan id 1000 ingress-replication inner-vid-disabled`	Create VNID 1000
`VTEP2(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf2`	Associate VNID with EVPN and vrf2
`VTEP2(config-nvo)#nvo vxlan access-if port xe47`	Create VXLAN access port
`VTEP2(config-nvo-acc-if)#no shutdown`	Unshut the access interface
`VTEP2(config-nvo-acc-if)#map vnid 1`	Map the VNID to access-if
`VTEP2(config-nvo-acc-if)#nvo vxlan access-if port-vlan po1 2001`	Create VXLAN access port
`VTEP2(config-nvo-acc-if)#no shutdown`	Unshut the access interface
`VTEP2(config-nvo-acc-if)#map vnid 1000`	Map the VNID to access-if
`VTEP2(config-nvo-acc-if)#nvo vxlan access-if port-vlan po1 2000`	Create VXLAN access port
`VTEP2(config-nvo-acc-if)#no shutdown`	Unshut the access interface
`VTEP2(config-nvo-acc-if)#map vnid 1000`	Map the VNID to access-if
`VTEP2(config-nvo-acc-if)#end`	Exit from config mode

P1

`P1#configure terminal`	Enter configuration terminal
`P1(config)#hostname P1`	Configure hostname
`P1(config)#bfd interval 3 minrx 3 multiplier 3`	Configure BFD interval globally
`P1(config)#qos enable`	Enable qos
`P1(config)#bridge 1 protocol ieee vlan-bridge`	Configure IEEE VLAN bridge
`P1(config)#no bridge 1 spanning-tree enable`	Disable spanning tree in bridge 1 globally
`P1(config)#no igmp snooping`	Disable igmp snooping messages globally
`P1(config)#vlan database`	Enter into the VLAN database
`P1(config-vlan)#vlan 10-200 bridge 1 state enable`	Configure VLAN 10-200 and associate with bridge 1
`P1(config-if)#interface lo`	Enter loopback interface mode
`P1(config-if)#ip address 3.3.3.3/32 secondary`	Assign loopback IP
`P1(config-if)#interface vlan1.20`	Specify interface VLAN1.20 to be configured.
`P1(config-if)#ip address 13.1.1.2/24`	Assign IP address
`P1(config-if)#ip ospf cost 1`	Change OSPF cost of the link
`P1(config-if)#interface vlan1.40`	Specify interface VLAN1.40 to be configured.
`P1(config-if)#ip address 23.1.1.2/24`	Assign IP address

© 2021 IP Infusion Inc. Proprietary

P1(config-if)#interface vlan1.60	Specify interface VLAN1.60 to be configured.
P1(config-if)#ip address 35.1.1.1/24	Assign IP address
P1(config-if)#ip ospf cost 1	Change OSPF cost of the link
P1(config-if)#interface vlan1.100	Specify interface VLAN1.100 to be configured.
P1(config-if)#ip address 34.1.1.1/24	Assign IP address
P1(config-if)#ip ospf cost 1	Change OSPF cost of the link
P1(config-vlan)#interface ce49	Enter interface mode
P1(config-if)#switchport	Set the interface as Layer2 port
P1(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P1(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P1(config-if)#switchport trunk allowed vlan add 40,49	Enable VLAN's allowed on this interface.
P1(config-if)#switchport trunk native vlan 49	Configure native VLAN
P1(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
P1(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P1(config-if)#interface xe1	Enter interface mode
P1(config-if)#switchport	Set the interface as Layer2 port
P1(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P1(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P1(config-if)#switchport trunk allowed vlan add 20,29	Enable VLAN's allowed on this interface.
P1(config-if)#switchport trunk native vlan 29	Configure native VLAN
P1(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
P1(config-if)#mtu 1600	Change the interface mtu value
P1(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P1(config-if)#interface xe10	Enter interface mode
P1(config-if)#switchport	Set the interface as Layer2 port
P1(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P1(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P1(config-if)#switchport trunk allowed vlan add 60,69	Enable VLAN's allowed on this interface.
P1(config-if)#switchport trunk native vlan 69	Configure native VLAN
P1(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
P1(config-if)#mtu 1600	Change the interface mtu value
P1(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P1(config-if)#interface xe25	Enter interface mode

`P1(config-if)#switchport`	Set the interface as Layer2 port
`P1(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P1(config-if)#switchport trunk allowed vlan add 100,109`	Enable VLAN's allowed on this interface.
`P1(config-if)#switchport trunk native vlan 109`	Configure native VLAN
`P1(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`P1(config-if)#spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P1(config-if)#router ospf 1`	Enter OSPF configuration mode
`P1(config-router)#ospf router-id 3.3.3.3`	Configure OSPF router id
`P1(config-router)#bfd all-interfaces`	Enable BFD in all OSPF interfaces
`P1(config-router)#network 3.3.3.3/32 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P1(config-router)#network 10.10.10.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P1(config-router)#network 13.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P1(config-router)#network 23.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P1(config-router)#network 34.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P1(config-router)#network 35.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P1(config-router)#end`	Exit from config mode

P2

`P2#configure terminal`	Enter configuration terminal
`P2(config)#bfd interval 3 minrx 3 multiplier 3`	Configure BFD interval globally
`P2(config)#qos enable`	Enable qos
`P2(config)#hostname P2`	Configure hostname
`P2(config)#bridge 1 protocol ieee vlan-bridge`	Configure IEEE VLAN bridge
`P2(config)#no bridge 1 spanning-tree enable`	Disable spanning tree in bridge 1 globally
`P2(config)#no igmp snooping`	Disable igmp snooping messages globally
`P2(config)#vlan database`	Enter into the VLAN database
`P2(config-vlan)#vlan 10-200 bridge 1 state enable`	Configure VLAN 10-200 and associate with bridge 1
`P2(config-vlan)#interface lo`	Enter lo interface mode
`P2(config-if)#ip address 4.4.4.4/32 secondary`	Assign loopback IP
`P2(config-if)#interface vlan1.30`	Specify interface VLAN1.30 to be configured.

© 2021 IP Infusion Inc. Proprietary

P2(config-if)#ip address 14.1.1.2/24	Assign IP address
P2(config-if)#ip ospf cost 1	Change OSPF cost of the link
P2(config-if)#interface vlan1.50	Specify interface VLAN1.50 to be configured.
P2(config-if)#ip address 24.1.1.2/24	Assign IP address
P2(config-if)#interface vlan1.70	Specify interface VLAN1.70 to be configured.
P2(config-if)#ip address 45.1.1.1/24	Assign IP address
P2(config-if)#ip ospf cost 1	Change OSPF cost of the link
P2(config-if)#interface vlan1.90	Specify interface VLAN1.90 to be configured.
P2(config-if)#ip address 46.1.1.1/24	Assign IP address
P2(config-if)#ip ospf cost 1	Change OSPF cost of the link
P2(config-if)#interface vlan1.100	Specify interface VLAN1.100 to be configured.
P2(config-if)#ip address 34.1.1.2/24	Assign IP address
P2(config-if)#ip ospf cost 1	Change OSPF cost of the link
P2(config-if)#interface xe2	Enter interface mode
P2(config-if)#switchport	Set the interface as Layer2 port
P2(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P2(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P2(config-if)#switchport trunk allowed vlan add 70,79	Enable VLAN's allowed on this interface.
P2(config-if)#switchport trunk native vlan 79	Configure native VLAN
P2(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
P2(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P2(config-if)#interface xe3	Enter interface mode
P2(config-if)#switchport	Set the interface as Layer2 port
P2(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P2(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P2(config-if)#switchport trunk allowed vlan add 90,99	Enable VLAN's allowed on this interface.
P2(config-if)#switchport trunk native vlan 99	Configure native VLAN
P2(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
P2(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P2(config-if)#interface xe7	Enter interface mode
P2(config-if)#switchport	Set the interface as Layer2 port
P2(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P2(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P2(config-if)#switchport trunk allowed vlan add 30,39	Enable VLAN's allowed on this interface.

`P2(config-if)#switchport trunk native vlan 39`	Configure native VLAN
`P2(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`P2(config-if)#spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P2(config-if)#interface xe9`	Enter interface mode
`P2(config-if)#switchport`	Set the interface as Layer2 port
`P2(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P2(config-if)#switchport trunk allowed vlan add 50,59`	Enable VLAN's allowed on this interface.
`P2(config-if)#switchport trunk native vlan 59`	Configure native VLAN
`P2(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`P2(config-if)#spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P2(config-if)#interface xe25`	Enter interface mode
`P2(config-if)#switchport`	Set the interface as Layer2 port
`P2(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`P2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`P2(config-if)#switchport trunk allowed vlan add 100,109`	Enable VLAN's allowed on this interface.
`P2(config-if)#switchport trunk native vlan 109`	Configure native VLAN
`P2(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`P2(config-if)#spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`P2(config-if)#router ospf 1`	Enter OSPF configuration mode
`P2(config-router)#ospf router-id 4.4.4.4`	Configure OSPF router id
`P2(config-router)#bfd all-interfaces`	Enable BFD in all OSPF interfaces
`P2(config-router)#network 4.4.4.4/32 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P2(config-router)#network 14.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P2(config-router)#network 24.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P2(config-router)#network 34.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P2(config-router)#network 45.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P2(config-router)#network 46.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`P2(config)#end`	Exit config mode

© 2021 IP Infusion Inc. Proprietary

P3

P3(config)#hostname P3	Configure hostname
P3(config)#bfd interval 3 minrx 3 multiplier 3	Configure BFD interval globally
P3(config)#qos enable	Enable qos
P3(config)#bridge 1 protocol ieee vlan-bridge	Configure IEEE VLAN bridge
P3(config)#no bridge 1 spanning-tree enable	Disable spanning tree in bridge 1 globally
P3(config)#no igmp snooping	Disable igmp snooping messages globally
P3(config)#vlan database	Enter into the VLAN database
P3(config-vlan)#vlan 10-200 bridge 1 state enable	Configure VLAN 10-200 and associate with bridge 1
P3(config-vlan)#interface lo	Enter lo interface mode
P3(config-if)#ip address 5.5.5.5/32 secondary	Assign loopback IP
P3(config-if)#interface vlan1.60	Specify interface VLAN1.60 to be configured.
P3(config-if)#ip address 35.1.1.2/24	Assign IP address
P3(config-if)#ip ospf cost 1	Change OSPF cost of the link
P3(config-if)#interface vlan1.70	Specify interface VLAN1.70 to be configured.
P3(config-if)#ip address 45.1.1.2/24	Assign IP address
P3(config-if)#ip ospf cost 1	Change OSPF cost of the link
P3(config-if)#interface vlan1.80	Specify interface VLAN1.80 to be configured.
P3(config-if)#ip address 56.1.1.1/24	Assign IP address
P3(config-if)#ip ospf cost 1	Change OSPF cost of the link
P3(config-if)#interface vlan1.110	Specify interface VLAN1.1100 to be configured.
P3(config-if)#ip address 15.1.1.2/24	Assign IP address
P3(config-if)#ip ospf cost 1	Change OSPF cost of the link
P3(config-if)#interface vlan1.160	Specify interface VLAN1.160 to be configured.
P3(config-if)#ip address 25.1.1.2/24	Assign IP address
P3(config-if)#ip ospf cost 1	Change OSPF cost of the link
P3(config-if)#interface xe2	Enter interface mode
P3(config-if)#switchport	Set the interface as Layer2 port
P3(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P3(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P3(config-if)#switchport trunk allowed vlan add 70,79	Enable VLAN's allowed on this interface.
P3(config-if)#switchport trunk native vlan 79	Configure native VLAN
P3(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
P3(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P3(config-if)#interface xe10	Enter interface mode

P3(config-if)#switchport	Set the interface as Layer2 port
P3(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P3(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P3(config-if)#switchport trunk allowed vlan add 60,69	Enable VLAN's allowed on this interface.
P3(config-if)#switchport trunk native vlan 69	Configure native VLAN
P3(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
P3(config-if)#mtu 1600	Change interface mtu value
P3(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P3(config-if)#interface xe15	Enter interface mode
P3(config-if)#switchport	Set the interface as Layer2 port
P3(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
P3(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
P3(config-if)#switchport trunk allowed vlan add 80,89	Enable VLAN's allowed on this interface.
P3(config-if)#switchport trunk native vlan 89	Configure native VLAN
P3(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
P3(config-if)#mtu 1600	Change interface mtu value
P3(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions
P3(config-if)#router ospf 1	Enter OSPF configuration mode
P3(config-router)#ospf router-id 5.5.5.5	Configure OSPF router id
P3(config-router)#bfd all-interfaces	Enable BFD in all ospf interfaces
P3(config-router)#network 5.5.5.5/32 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)#network 15.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)#network 25.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)#network 35.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)#network 45.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)#network 56.1.1.0/24 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
P3(config-router)#end	Exit config mode

VTEP3

VTEP3#configure terminal	Enter configuration terminal
VTEP3(config)#hostname VTEP3	Configure hostname

© 2021 IP Infusion Inc. Proprietary

VTEP3(config)#mac vrf vrf1	Configure MAC vrf vrf1
VTEP3(config-vrf)#rd 6.6.6.6:11	Configure RD for vrf1
VTEP3(config-vrf)#route-target both 10.10.10.10:100	Configure RT for vrf1
VTEP3(config-vrf)#mac vrf vrf2	Configure MAC vrf vrf2
VTEP3(config-vrf)#rd 6.6.6.6:12	Configure RD for vrf2
VTEP3(config-vrf)#route-target both 10.10.10.10:101	Configure RT for vrf2
VTEP3(config-vrf)#route-target both 10.10.10.10:102	Configure RT for vrf2
VTEP3(config-vrf)#bfd interval 3 minrx 3 multiplier 3	Enable EVPN VXLAN multihoming
VTEP3(config)#evpn vxlan multihoming enable	Enable statistics on VXLAN tunnel interface
VTEP3(config)#nvo vxlan enable	Enable VXLAN
VTEP3(config)#qos enable	Enable qos
VTEP3(config)#qos statistics	Enable qos statistics
VTEP3(config)#bridge 1 protocol ieee vlan-bridge	Configure IEEE VLAN bridge
VTEP3(config)#no bridge 1 spanning-tree enable	Disable spanning tree in bridge 1 globally
VTEP3(config)#no igmp snooping	Disable igmp snooping messages globally
VTEP3(config)#vlan database	Enter into the VLAN database
VTEP3(config-vlan)#vlan 10-200 bridge 1 state enable	Configure VLAN 10-200 and associate with bridge 1
VTEP3(config-vlan)#interface lo	Enter lo interface mode
VTEP3(config-if)#ip address 6.6.6.6/32 secondary	Assign loopback IP
VTEP3(config-if)#interface vlan1.80	Specify interface VLAN1.80 to be configured.
VTEP3(config-if)#ip address 56.1.1.2/24	Assign IP address
VTEP3(config-if)#ip ospf cost 1	Change OSPF cost of the link
VTEP3(config-if)#interface vlan1.90	Specify interface VLAN1.90 to be configured.
VTEP3(config-if)#ip address 46.1.1.2/24	Assign IP address
VTEP3(config-if)#ip ospf cost 1	Change OSPF cost of the link
VTEP3(config-if)#interface xe3	Enter interface mode
VTEP3(config-if)#switchport	Set the interface as Layer2 port
VTEP3(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1 and disable spanning tree
VTEP3(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
VTEP3(config-if)#switchport trunk allowed vlan add 90,99	Enable VLAN's allowed on this interface.
VTEP3(config-if)#switchport trunk native vlan 99	Configure native VLAN
VTEP3(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
VTEP3(config-if)#spanning-tree edgeport	Set the port as an edge-port to enable rapid transitions

`VTEP3(config-if)#interface xe15`	Enter interface mode
`VTEP3(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1 and disable spanning tree
`VTEP3(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`VTEP3(config-if)#switchport trunk allowed vlan add 80,89`	Enable VLAN's allowed on this interface.
`VTEP3(config-if)#switchport trunk native vlan 89`	Configure native VLAN
`VTEP3(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP3(config-if)#mtu 1600`	Change interface mtu value
`VTEP3(config-if)#spanning-tree edgeport`	Set the port as an edge-port to enable rapid transitions
`VTEP3(config-if)#interface xe45`	Enter interface mode
`VTEP3(config-if)#switchport`	Set the interface as Layer2 port
`VTEP3(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP3(config-if)#interface xe46`	Enter interface mode
`VTEP3(config-if)#switchport`	Set the interface as Layer2 port
`VTEP3(config-if)#load-interval 30`	Configure load period in multiple of 30 seconds
`VTEP3(config-if)#router ospf 1`	Enter OSPF configuration mode
`VTEP3(config-router)#ospf router-id 6.6.6.6`	Configure OSPF router id
`VTEP3(config-router)#bfd all-interfaces`	Enable BFD in all OSPF interfaces
`VTEP3(config-router)#network 6.6.6.6/32 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP3(config-router)#network 46.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP3(config-router)#network 56.1.1.0/24 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`VTEP3(config-router)#router bgp 100`	Enter address-family IPv4 unicast mode
`VTEP3(config-router)#address-family ipv4 unicast`	Add the lo network to BGP route
`VTEP3(config-router)#network 6.6.6.6/32`	Activate neighbors
`VTEP3(config-router-af)#neighbor 1.1.1.1 activate`	Activate neigbors
`VTEP3(config-router-af)#neighbor 2.2.2.2 activate`	Exit address-family mode.
`VTEP3(config-router-af)#exit-address-family`	Enter Router BGP mode and define the AS number 100.
`VTEP3(config-router)#neighbor 1.1.1.1 remote-as 100`	Configure BGP remote-as 100 with neighbor IP
`VTEP3(config-router)#neighbor 1.1.1.1 update-source lo`	Define BGP neighbors, to update the source routes with lo
`VTEP3(config-router)#neighbor 2.2.2.2 remote-as 100`	Configure BGP remote-as 100 with neighbor IP
`VTEP3(config-router)#neighbor 2.2.2.2 update-source lo`	Configure advertisement-interval as 0 for fast convergence for VTEP2
`(config-router)#neighbor 2.2.2.2 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for VTEP1

© 2021 IP Infusion Inc. Proprietary

(config-router)#neighbor 1.1.1.1 advertisement-interval 0	Define BGP neighbors, to update the source routes with lo
VTEP3(config-router)#address-family l2vpn evpn	Enter in to BGP L2VPN EVPN address-family
VTEP3(config-router-af)#neighbor 1.1.1.1 activate	Activate neigbors
VTEP3(config-router-af)#neighbor 2.2.2.2 activate	Activate neigbors
VTEP3(config-router-af)#exit-address-family	Exit from BGP L2VPN EVPN address-family
VTEP3(config-router)#nvo vxlan vtep-ip-global 6.6.6.6	Configure VXLAN global IP
VTEP3(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled	Create VNID 1
VTEP3(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Associate VNID with EVPN and vrf1
VTEP3(config-nvo)#nvo vxlan id 1000 ingress-replication inner-vid-disabled	Create VNID 1000
VTEP3(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf2	Associate VNID with EVPN and vrf2
VTEP3(config-nvo)#nvo vxlan access-if port-vlan xe45 3001	Create VXLAN access port port-VLAN
VTEP3(config-nvo-acc-if)#no shutdown	Unshut the access interface
VTEP3(config-nvo-acc-if)#map vnid 1	Map the VNID to access-if
VTEP3(config-nvo-acc-if)#nvo vxlan access-if port xe46	Create VXLAN access port
VTEP3(config-nvo-acc-if)#no shutdown	Unshut the access interface
VTEP3(config-nvo-acc-if)#map vnid 1000	Map the VNID to access-if
VTEP3(config-nvo-acc-if)#end	Enter configuration terminal

SWITCH

SWITCH#configure terminal	Enter configuration terminal
SWITCH#(config-vlan)#interface po1	Enter interface mode
SWITCH#(config-if)#switchport	Set the interface as Layer2 port
SWITCH#(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
SWITCH#(config-if)#interface ce9/1	Enter interface mode
SWITCH#(config-if)#channel-group 1 mode active	Map this interface to po1
SWITCH#(config-if)#interface ce9/2	Enter interface mode
SWITCH#(config-if)#channel-group 1 mode active	Map this interface to po1
SWITCH#(config-if)#load-interval 30	Configure load period in multiple of 30 seconds
SWITCH#(config-if)#interface ce10/1	Enter interface mode
SWITCH#(config-if)#channel-group 1 mode active	Map this interface to po1
SWITCH#(config-if)#interface ce10/2	Enter interface mode

© 2021 IP Infusion Inc. Proprietary

SWITCH#(config-if)#channel-group 1 mode active	Map this interface to po1
SWITCH#(config-if)#interface ce31/1	Set the port as an edge-port to enable rapid transitions
SWITCH#(config-if)#switchport	Enter interface mode
SWITCH#(config-if)#bridge-group 1 spanning-tree disable	Set the interface as Layer2 port
SWITCH#(config-if)#switchport mode trunk	Associate the interface with bridge group 1 and disable spanning tree
SWITCH#(config-if)#switchport trunk allowed vlan all	Set the switching characteristics of this interface to trunk mode.
SWITCH#(config-if)#load-interval 30	Configure native VLAN

Validation

```
VTEP1#sh ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
2.2.2.2           1   Full/DR         00:00:30    12.1.1.2        vlan1.10              0
3.3.3.3           1   Full/DR         00:00:31    13.1.1.2        vlan1.20              0
4.4.4.4           1   Full/DR         00:00:33    14.1.1.2        vlan1.30              0


VTEP2#sh ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/Backup      00:00:38    12.1.1.1        vlan1.10
0
3.3.3.3           1   Full/DR         00:00:39    23.1.1.2        vlan1.40              0
4.4.4.4           1   Full/DR         00:00:39    24.1.1.2        vlan1.50              0
P1#sh ip ospf neighbor

Total number of full neighbors: 4
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/Backup      00:00:39    13.1.1.1        vlan1.20
0
2.2.2.2           1   Full/Backup      00:00:38    23.1.1.1        vlan1.40
0
4.4.4.4           1   Full/DR         00:00:40    34.1.1.2        vlan1.100             0
5.5.5.5           1   Full/DR         00:00:36    35.1.1.2        vlan1.60              0

P2#sh ip ospf neighbor
```


© 2021 IP Infusion Inc. Proprietary

```
Total number of full neighbors: 5
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/Backup     00:00:30    14.1.1.1        vlan1.30
0
2.2.2.2           1   Full/Backup     00:00:38    24.1.1.1        vlan1.50
0
3.3.3.3           1   Full/Backup     00:00:33    34.1.1.1        vlan1.100
0
5.5.5.5           1   Full/DR         00:00:30    45.1.1.2        vlan1.70              0
6.6.6.6           1   Full/DR         00:00:34    46.1.1.2        vlan1.90              0
P2#
P3#sh ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
3.3.3.3           1   Full/Backup     00:00:34    35.1.1.1        vlan1.60
0
4.4.4.4           1   Full/Backup     00:00:34    45.1.1.1        vlan1.70
0
6.6.6.6           1   Full/DR         00:00:33    56.1.1.2        vlan1.80              0
P3#

VTEP1#sh bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
2.2.2.2                 4   100   23        22      4      0      0  00:07:34
2      0      0      2      0      0
6.6.6.6                 4   100   21        22      4      0      0  00:07:34
2      0      0      2      0      0

Total number of neighbors 2

Total number of Established sessions 2
VTEP1#
VTEP2#sh bgp l2vpn evpn summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
1.1.1.1                 4   100   22        24      5      0      0  00:07:41
2      0      0      2      0      0
```

```
6.6.6.6                 4   100   24        27      5     0     0  00:08:51
2      0      0      2      0      0

Total number of neighbors 2

Total number of Established sessions 2
VTEP2#
VTEP3#sh bgp l2vpn evpn summary
BGP router identifier 6.6.6.6, local AS number 100
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
1.1.1.1                 4   100   23        21      5     0     0  00:07:44
2      0      0      2      0      0
2.2.2.2                 4   100   26        24      5     0     0  00:08:54
2      0      0      2      0      0

Total number of neighbors 2

Total number of Established sessions 2
VTEP3#

VTEP1#show nvo vxlan mac-table
================================================================================================
============================================================
                                                                VXLAN MAC Entries
================================================================================================
============================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                Status              AccessPortDesc
________________________________________________________________________________________________
____________________________________________________________

1         po1        1000   ----         0000.1111.1111 00:aa:22:33:44:55:66:00:00:00
Static Local         -------              -------
1         po1        1000   ----         0000.1111.1112 00:aa:22:33:44:55:66:00:00:00
Static Local         -------              -------
1         po1        1000   ----         0000.1111.1113 00:aa:22:33:44:55:66:00:00:00
Static Local         -------              -------
1         po1        1000   ----         0000.1111.1114 00:aa:22:33:44:55:66:00:00:00
Static Local         -------              -------
1         po1        1000   ----         0000.1111.1115 00:aa:22:33:44:55:66:00:00:00
Static Local         -------              -------
1         po1        1000   ----         a82b.b57c.4470 00:aa:22:33:44:55:66:00:00:00
Dynamic Local        -------              -------
1000      ----       ----   ----         a82b.b57c.4476 00:aa:22:33:44:55:66:00:00:00
Dynamic Remote       -------              -------

Total number of entries are : 7

VTEP1#
```


© 2021 IP Infusion Inc. Proprietary

```
VTEP2#sh nvo vxlan mac-table
================================================================================================
================================================================
                                                                    VXLAN MAC Entries
================================================================================================
================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc

________________________________________________________________________________________________
________________________________________________________________

1         ----       ----   ----         0000.1111.1111 00:aa:22:33:44:55:66:00:00:00
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1112 00:aa:22:33:44:55:66:00:00:00
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1113 00:aa:22:33:44:55:66:00:00:00
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1114 00:aa:22:33:44:55:66:00:00:00
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1115 00:aa:22:33:44:55:66:00:00:00
Static Remote        -------             -------
1         ----       ----   ----         a82b.b57c.4470 00:aa:22:33:44:55:66:00:00:00
Dynamic Remote       -------             -------
1000      po1        2000   ----         a82b.b57c.4476 00:aa:22:33:44:55:66:00:00:00
Dynamic Local        -------             -------

Total number of entries are : 7

VTEP2#
VTEP3#sh nvo vxlan mac-table
================================================================================================
================================================================
                                                                    VXLAN MAC Entries
================================================================================================
================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc

________________________________________________________________________________________________
________________________________________________________________

1         ----       ----   ----         0000.1111.1111 00:aa:22:33:44:55:66:00:00:00
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1112 00:aa:22:33:44:55:66:00:00:00
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1113 00:aa:22:33:44:55:66:00:00:00
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1114 00:aa:22:33:44:55:66:00:00:00
Static Remote        -------             -------
1         ----       ----   ----         0000.1111.1115 00:aa:22:33:44:55:66:00:00:00
Static Remote        -------             -------
1         ----       ----   ----         a82b.b57c.4470 00:aa:22:33:44:55:66:00:00:00
Dynamic Remote       -------             -------
1000      ----       ----   ----         a82b.b57c.4476 00:aa:22:33:44:55:66:00:00:00
Dynamic Remote       -------             -------
```

```
Total number of entries are : 7

VTEP3#
VTEP1#show nvo vxlan access-if brief

                 Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
xe46       ---   ---   500000   1         up      up
po1        2000  ---   500001   1000      up      up
po1        2001  ---   500002   1000      up      up


Total number of entries are 2
VTEP1#
VTEP2#show nvo vxlan access-if brief

                 Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
xe47       ---   ---   500000   1         up      up
po1        2001  ---   500001   1000      up      up
po1        2000  ---   500002   1000      up      up

Total number of entries are 3
VTEP2#
VTEP3#show nvo vxlan access-if brief

                 Inner                    Admin   Link
Interface  Vlan  vlan  Ifindex  Vnid      status  status
-----------------------------------------------------------
xe45       3001  ---   500000   1         up      up
xe46       ---   ---   500001   1000      up      up

Total number of entries are 2
VTEP3#
VTEP1#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
1.1.1.1          6.6.6.6          Installed        00:03:59        00:03:59
1.1.1.1          2.2.2.2          Installed        00:03:59        00:03:59

Total number of entries are 2
VTEP1#sh nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
```


© 2021 IP Infusion Inc. Proprietary

```
VNID     VNI-Name     VNI-Type Type Interface ESI                                VLAN DF-
Status Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________
1        ----         L2       NW   ----      ----                                ---- --
--      1.1.1.1          6.6.6.6
1        ----         L2       NW   ----      ----                                ---- --
--      1.1.1.1          2.2.2.2
1000     ----       --      AC   po1      --- 00:aa:22:33:44:55:66:00:00:00 2000 DF
----             ----
1000     ----       --      AC   po1      --- 00:aa:22:33:44:55:66:00:00:00 2001 DF
----             ----
1000     ----         L2       NW   ----      ----                                ---- -
---      1.1.1.1          6.6.6.6
1000     ----         L2       NW   ----      ----                                ---- -
---      1.1.1.1          2.2.2.2
1000     ----         --       AC   xe46      --- Single Homed Port ---           ---- -
---      ----             ----

Total number of entries are 10
VTEP1#

VTEP2#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
2.2.2.2          1.1.1.1          Installed       00:03:59        00:03:59
2.2.2.2          6.6.6.6          Installed       00:05:09        00:05:09

Total number of entries are 2
VTEP2#sh nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
          (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface ESI                                VLAN DF-
Status Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________
1        ----         L2       NW   ----      ----                                ---- --
--      2.2.2.2          1.1.1.1
1        ----         L2       NW   ----      ----                                ---- --
--      2.2.2.2          6.6.6.6
1        ----         --       AC   xe47      --- Single Homed Port ---           ---- --
--      ----             ----
1000     ----         L2       NW   ----      ----                                ---- --
--      2.2.2.2          1.1.1.1
1000     ----         L2       NW   ----      ----                                ---- --
--      2.2.2.2          6.6.6.6
1000     ----       --       AC   po1       --- 00:aa:22:33:44:55:66:00:00:00 2001 NON-
DF       ----             ----
```

```
1000     ----         --       AC   po1       --- 00:aa:22:33:44:55:66:00:00:00 2000 NON-
DF       ----              ----

Total number of entries are 11
VTEP2#

VTEP3#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
6.6.6.6          1.1.1.1          Installed       00:03:58        00:03:58
6.6.6.6          2.2.2.2          Installed       00:05:08        00:04:03

Total number of entries are 2
VTEP3#sh nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     VNI-Name     VNI-Type Type Interface ESI                           VLAN DF-Status
Src-Addr         Dst-Addr
_____________________________________________________________________________________
_____________________________________
1        ----         L2       NW   ----      ----                          ---- ----
6.6.6.6          1.1.1.1
1        ----         L2       NW   ----      ----                          ---- ----
6.6.6.6          2.2.2.2
1        ----         --       AC   xe45      --- Single Hommed port ---    3001 ----
----             ----
1000     ----         L2       NW   ----      ----                          ---- ----
6.6.6.6          1.1.1.1
1000     ----         L2       NW   ----      ----                          ---- ----
6.6.6.6          2.2.2.2
1000     ----         --       AC   xe46      --- Single Homed Port ---     ---- ----
----             ----

Total number of entries are 10
VTEP3#
```


© 2021 IP Infusion Inc. Proprietary

Virtual eXtensible Local Area Network Command Reference

Contents

This document contains these chapters and appendices:

- Chapter 1, *VXLAN Commands*
- Chapter 2, *VXLAN Quality of Service Commands*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 VXLAN Commands

This chapter describes the VXLAN commands:

- arp-cache disable
- arp-nd flood-suppress
- arp-nd refresh timer
- clear mac address table dynamic vxlan
- clear nvo vxlan counters
- clear nvo vxlan tunnels
- clear nvo vxlan mac-stale-entries
- description
- dynamic-learning disable
- encapsulation
- evpn esi holdtime
- evpn vxlan multi-homing enable
- evpn multi-homed
- evpn-vlan-service
- garp-gna enable
- load-balance rtag7 vxlan inner-l2
- load-balance rtag7 vxlan inner-l3
- mac
- mac vrf
- mac-holdtime
- map vnid
- nd-cache disable
- no nvo vxlan
- nvo vxlan
- nvo vxlan access-if
- nvo vxlan mac-ageing-time
- nvo vxlan mac-ageing-time
- nvo vxlan max-cache-disable
- nvo vxlan vtep-ip-global
- show bgp l2vpn evpn
- show bgp l2vpn evpn summary
- show nvo vxlan
- show nvo vxlan access-if-config

© 2021 IP Infusion Inc. Proprietary

- show nvo vxlan arp-cache
- show nvo vxlan counters access-port
- show nvo vxlan counters network-port
- show nvo vxlan mac-table
- show nvo vxlan nd-cache
- show nvo vxlan static host state
- show nvo vxlan tunnel
- show running-config nvo vxlan
- show evpn multi-homing all
- show evpn multihoming-status
- show nvo vxlan route-count
- show nvo vxlan vni-name
- shutdown
- vxlan host-reachability-protocol evpn-bgp

© 2021 IP Infusion Inc. Proprietary

arp-cache disable

Use this command to disable the ARP cache for MAC/IP.

When the ARP cache is disabled on a VxLAN access port, OcNOS does not reply to any ARP arriving on this port from the cache. OcNOS withdraws all MAC/IPs configured/learned on this access port and removes the MAC/IP entry for this access port from the local ARP cache.

OcNOS also makes sure that on withdrawing the MAC/IP route, the MAC does not become unknown. If all routes for this MAC are being withdrawn because of this command, then OcNOS advertises a MAC-only route. This is done so that the MAC does not become unknown and only the cache functionality becomes disabled.

See also nvo vxlan max-cache-disable.

Use the `no` form of this command to enable ARP cache for MAC/IP.

Note: On enabling the cache, an IP will be in conflict, then the cache enable will fail. The conflict has to be manually removed and then the cache enabled.

Command Syntax

```
arp-cache disable
```

```
no arp-cache disable
```

Parameters

None

Default

By default, the arp-cache option is enabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#arp-cache disable
(config-nvo-acc-if)#exit
```

arp-nd flood-suppress

Use this command to *completely* restrict the flood of ARP/ND packets towards remote VTEPs or other access ports.

This command applies only when the ARP cache and ND cache are enabled. When the ARP cache is disabled, ARP flooding is not suppressed even if this command is given. When the ND cache is disabled, ND flooding is not disabled, even if this command is given.

Use the `no` form of this command to not restrict the flood of ARP/ND packets.

Command Syntax

```
arp-nd flood-suppress
```

```
no arp-nd flood-suppress
```

Parameters

None

Default

By default, the arp-nd flood-suppress option is disabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#arp-nd flood-suppress
(config-nvo-acc-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

arp-nd refresh timer

Use this command to configure aging out the arp-cache and nd-cache entries for given time multiplied by 3 in secs

Use the no form of this command to remove the configuration

Command Syntax

```
nvo vxlan arp-nd refresh-timer <3-190>
no nvo vxlan arp-nd refresh-timer
```

Parameters

`<3-190>` refresh time in seconds

Command Mode

Config mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config mode
(config)#nvo vxlan arp-nd refresh-timer 100
(config)#no nvo vxlan arp-nd refresh-timer
```

clear mac address table dynamic vxlan

Use this command to clear dynamically learned MACs.

Command Syntax

```
clear mac address table dynamic vxlan
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear mac address table dynamic vxlan
```


© 2021 IP Infusion Inc. Proprietary

clear nvo vxlan counters

Use this command to clear the counters of access ports or network ports.

Command Syntax

```
clear nvo vxlan counters((access-port (port IFNAME | port-vlan IFNAME (VLAN_ID |
  outer-vlan) | all)) | (network-port (dst A.B.C.D | all)))
```

Parameters

`port`	Port
`IFNAME`	Interface name
`port-vlan`	VLAN port
`IFNAME`	Interface name
`VLAN_ID`	VLAN identifier
`Outer-vlan`	Outer Vlan
`A.B.C.D`	Tunnel destination IPv4 address
`all`	All access or network ports

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Example for clearing a VLAN port counter:

```
#clear nvo vxlan counters access-port port-vlan xe1 2
```

Example for clearing all access port counters:

```
#clear nvo vxlan counters access-port all
```

Example for clearing network port counters:

```
#clear nvo vxlan counters network-port dst 1.1.1.1
```

Example for clearing all network port counters:

```
#clear nvo vxlan counters network-port all
```

clear nvo vxlan tunnels

Use this command to clear the nvo vxlan tunnels to re-establish the tunnel after mapping/un-mapping the QoS profile to vxlan tunnel.

Command Syntax

```
clear nvo vxlan tunnels (|dst-ip A.B.C.D)
```

Parameters

`dst-ip`	VXLAN tunnel destination
`A.B.C.D`	destination IPv4 address

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Example

```
#clear nvo vxlan tunnels dst-ip 2.2.2.2
```

Note: `clear nvo vxlan tunnels` This command will clear all the VXLAN tunnels destination.

`clear nvo vxlan tunnels dst-ip A.B.C.D -` This command to clear individual tunnel destination(i.e A.B.C.D).

© 2021 IP Infusion Inc. Proprietary

clear nvo vxlan mac-stale-entries

Use this command to clear MAC entries that are in discard state in the forwarding database.

Command Syntax

```
clear nvo vxlan mac-stale-entries (vnid <1-16777215> |)
```

Parameters

<1-16777215>	VXLAN network identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear nvo vxlan mac-stale-entries vnid 100
```

description

Use this command to set a description for a port.

Use the `no` form of this command to remove the description for a port.

Command Syntax

```
description LINE
no description
```

Parameters

`LINE`	Maximum 32 characters describing this port.

Default

No default value is specified for description LINE commands.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#description member-port xe1 with vlan 2
(config-nvo-acc-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

dynamic-learning disable

Use this command to disable dynamic learning of MACs at the access port. This command also disables dynamic learning of MAC/IP from ARP/ND messages received on this access port.

Use the `no` form of this command to enable dynamic learning of MACs at the access port.

Command Syntax

```
dynamic-learning disable
```

```
no dynamic-learning disable
```

Parameters

None

Default

By default, the dynamic-learning option is enabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#dynamic-learning disable
(config-nvo-acc-if)#exit
```

encapsulation

Use this command to assign a Tag Protocol Identifier (TPID) to an access port.

Use the `no` form of this command to set the default TPID (0x8100: IEEE 802.1Q VLAN-tagged frame) to an access port.

Command Syntax

```
encapsulation TPID
no encapsulation
```

Parameters

`TPID`	Tag Protocol Identifier: Ox88A8: IEEE 802.1ad Provider Bridging Ox9100: IEEE 802.1Q VLAN-tagged frame with double tagging

Default

The encapsulation TPID default is 0X8100.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#encapsulation 0x9100
(config-nvo-acc-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

evpn esi holdtime

Use this command to allow some time for the tunnels to come at the time of vxlan initialization before making the esi up. This avoids traffic to be black-holed when a new PE is added and connected to an already running CE for multi-homing.

Use the no form of this command to make the esi up immediately when configuring the access-if cli.

Command Syntax

```
evpn esi holdtime <10-300>
no evpn esi holdtime <10-300>
```

Parameters

<10-300>	Hold time in seconds

Default

Default value is 0.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)# evpn esi holdtime 100
(config)# exit
```

evpn vxlan multi-homing enable

Use this command to enable evpn vxlan multi-homing

Use the no form of this command to disable evpn vxlan multi-homing.

Note: Node will have to be restarted for this to be applicable. If there are some nodes in topology which have multi-homed CEs, then nodes which do not have multi-homed CEs should also enable multihoming so, that they can load share traffic to the multi-homed CEs.

Command Syntax

```
evpn vxlan multihoming enable
```

```
no evpn vxlan multihoming enable
```

Parameters

None

Default

By Default Multi-homing will be d]isabled

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#(config)# evpn vxlan multihoming enable
#(config)# exit
```


© 2021 IP Infusion Inc. Proprietary

evpn multi-homed

Use this command to configure interfaces as multi-homed and configure esi-value in case of physical and static lag and system-mac in case of Dynamic lag.

Use the no parameter of this command to unconfigure multi-homed on the interface.

Command Syntax

```
evpn multi-homed (esi XX:XX:XX:XX:XX:XX:XX:XX:XX | system-mac (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)
no evpn multi-homed (esi | system-mac)
```

Parameters

`XX:XX:XX:XX:XX:XX:XX:XX:XX`	ESI value in HH:HH:HH:HH:HH:HH:HH:HH:HH - 9 octet format
`XX-XX-XX-XX-XX-XX`	Host MAC address (Option 1)
`XX:XX:XX:XX:XX:XX`	Host MAC address (Option 2)
`XXXX.XXXX.XXXX`	Host MAC address (Option 3)

Default

Default value is 0.

Command Mode

Interface Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)# interface xe1
(config)# evpn multi-homed esi 00:11:22:33:44:55:66:77:88
(config)# exit

configure terminal
(config)# interface po1
(config)# evpn multi-homed system-mac 0000.0000.1111
(config)# exit
```

© 2021 IP Infusion Inc. Proprietary

evpn-vlan-service

Use this command to configure VLAN-based EVPN-Service type.

Use the `no` form of this command to delete the evpn vlan service.

Note: If access port mappings to vnid exists already and vlan service is configured later and mapped to tenant then we should not allow the mapping, user should either remove and reconfigure the access port mappings.

Command Syntax

```
evpn-vlan-service vlan-based
no evpn-vlan-service
```

Parameters

`vlan-based`	VLAN-based EVPN-Service type

Command Mode

MAC vrf mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mac vrf vrf1
(config-vrf)# evpn-vlan-service vlan-based
(config-vrf)# no evpn-vlan-service vlan-based
```


© 2021 IP Infusion Inc. Proprietary

garp-gna enable

Use this command to enable GARP/GNA packets per vxlan on the outgoing access interfaces where it is configured.

Use the no form this command to disable GARP/GNA packets on the outgoing access interfaces.

By default it will be disable

Command Syntax

```
garp-gna enable
```

```
garp-gna enable
```

Parameters

```
None
```

Command Mode

config-nvo-acc-if mode

Applicability

This command is introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 10
config-nvo-acc-if)#garp-gna enable
```

load-balance rtag7 vxlan inner-l2

Use this command to enable RTAG7 load balancing for VxLAN for inner-L2 packets on the access side for load sharing of traffic on tunnel paths. This command also enables random UDP source port generation for the VxLAN UDP tunnels based on the L2 frame being received on the VxLAN access port.

Use the `no` parameter of this command to disable load balance for RTAG7 for VxLAN for inner-L2 frames.

Command Syntax

```
load-balance rtag7 vxlan inner-l2 (dest-mac | src-mac)
no load-balance rtag7 vxlan inner-l2 (dest-mac | src-mac)
```

Parameter

`dest-mac`	Destination MAC Address.
`src-mac`	Source MAC Address.

Default

By default, the load-balance rtag7 vxlan inner-l2 default is src-mac.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#load-balance rtag7 vxlan inner-l2 dest-mac

(config)#no load-balance rtag7 vxlan inner-l2 dest-mac
```


© 2021 IP Infusion Inc. Proprietary

load-balance rtag7 vxlan inner-l3

Use this command to enable RTAG7 load balancing for VxLAN for inner-L3 IPv4 and IPv6 packets on the access side for load sharing of traffic on tunnel paths. This command also enables random UDP source port generation for the VxLAN UDP tunnels based on the L3 frame being received on the VxLAN access port.

Use the `no` parameter of this command to disable load balance for RTAG7 for VxLAN for inner-L3 IPv4 and IPv6 frames.

Command Syntax

```
load-balance rtag7 vxlan inner-l3 (dest-ip | destl4-port | protocol-id | src-ip |
  srcl4-port)
no load-balance rtag7 vxlan inner-l3 (dest-ip | destl4-port | protocol-id | src-ip
  | srcl4-port)
```

Parameter

`dest-ip`	Destination IP.
`destl4-port`	Destination l4 port.
`protocol-id`	Protocol (IPv4).
`src-ip`	Source IP.
`srcl4-port`	Source l4 port.

Default

By default, the load-balance rtag7 vxlan inner-l3 default is src-ip.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#load-balance rtag7 vxlan inner-l3 dest-ip

(config)#no load-balance rtag7 vxlan inner-l3 dest-ip
```

mac

Use this command to associate a static MAC address and a static IPv4 or IPv6 address on an access interface.

Use the `no` form of this command to disassociate a static MAC address and an IPv4 or IPv6 address for an access interface.

Note: When a static host is configured on an access port which is in the down state, its state is Inactive.

Note: The same static mac configuration is not allowed on a different access port as then there will be a chance of conflict. However, if a dynamic packet is sent at another access port which is up and running with the same MAC, it learns as usual. As soon as the port on which the static MAC is configured comes up, static learning is given precedence and the dynamically learned MAC is moved to the port where it is configured statically.

Command Syntax

```
mac XXXX.XXXX.XXXX
mac XXXX.XXXX.XXXX (ip A.B.C.D | ipv6 X:X::X:X)
no mac XXXX.XXXX.XXXX (ip A.B.C.D | ipv6 X:X::X:X)
```

Parameters

`XXXX.XXXX.XXXX`	Static MAC address. The following formats are supported:
	XX-XX-XX-XX-XX-XX Source MAC address (Option 1)
	XX:XX:XX:XX:XX:XX Source MAC address (Option 2)
	XXXX.XXXX.XXXX Source MAC address (Option 3)
`A.B.C.D`	Static IPv4 address.
`X:X::X:X`	Static IPv6 address.

Default

No default value is specified for mac command.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#mac 0000.0000.aaaa ip 10.10.10.1
(config-nvo-acc-if)#mac 0000.0000.aaaa ipv6 1201::1
(config-nvo-acc-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

mac vrf

Use this command to create a MAC VRF to use in EVPN routes.

See also vxlan host-reachability-protocol evpn-bgp.

Use the `no` parameter of this command to delete the MAC VRF.

Command Syntax

```
mac vrf WORD
no mac vrf WORD
```

Parameter

`WORD`	MAC routing or forwarding instance name.

Default

No default value is specified for mac vrf WORD command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mac vrf vrf1

(config)#no mac vrf vrf1
```

mac-holdtime

Use this command to set the MAC hold time for a MAC/IP or MAC.

The feature holds the MAC in hardware until BGP has withdrawn from the neighbors. This helps to reduce flooding to other access ports.

This setting applies when the access port is shut down, the physical port on which the access port is down, or the access port is removed from the VNID using the `no` form of the map vnid command.

When the MAC hold time is configured as -1, then the MAC is not removed from the hardware and is also not withdrawn from EVPN BGP.

Use the `no` form of this command to remove the MAC hold time for the MAC/IP or MAC.

Note: When a MAC is moved to discard state, traffic to and from this MAC is discarded. This is applicable only on statically configured MAC/MAC-IPs.

Command Syntax

```
mac-holdtime <-1-300>
no mac-holdtime
```

Parameters

`<-1-300>`	MAC hold time in seconds. Specify -1 to “never expire”.

Default

The default holdtime for mac is 3 seconds.

Command Mode

NVO mode and NVO_ACC_IF_MODE mode

Note: When configured in both modes, then the NVO_ACC_IF_MODE value takes preference for that access port.

Applicability

This command was introduced before OcNOS version 1.3.

This command in NVO_ACC_IF_MODE mode is introduced in OcNOS version 1.3.4.

Example

```
#configure terminal
(config)#nvo vxlan id 3 ingress-replication inner-vid-disabled
(config-nvo)#mac-holdtime -1
(config-nvo)#exit
```


© 2021 IP Infusion Inc. Proprietary

map vnid

Use this command to map a tenant to an access-port.

Use the `no` form of this command to remove the tenant from an access-port

Command Syntax

```
map vnid <1-16777215>
no map vnid <1-16777215>
```

Parameters

`<1-16777215>`	VxLAN network identifier.

Default

No default value is specified for map vnid command.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#map vnid 100
(config-nvo-acc-if)#exit
```

nd-cache disable

Use this command to disable ND cache for MAC/IPv6.

When the ND cache is disabled on a VxLAN access port, OcNOS does not reply to any ND arriving on this port from the cache. OcNOS withdraws all MAC/IPs configured/learned on this access port and removes the MAC/IP entry for this access port from the local ND cache.

OcNOS also makes sure that on withdrawing the MAC/IP route, the MAC does not become unknown. If all routes for this MAC are being withdrawn because of this command, then OcNOS advertises a MAC-only route. This is done so that the MAC does not become unknown and only the cache functionality becomes disabled.

See also arp-cache disable.

Use the `no` form of this command to enable ND cache for MAC/IPv6.

Note: On enabling the cache, an IP will be in conflict, then the cache enable will fail. The conflict has to be manually removed and then the cache enabled.

Command Syntax

```
nd-cache disable
```

```
no nd-cache disable
```

Parameters

None

Default

By default, the nd-cache option is enabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#nd-cache disable
(config-nvo-acc-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

no nvo vxlan

Use this command to delete a given tenant or all tenants/VPNs.

Command Syntax

```
no nvo vxlan (id <1-16777215>|all-vnids)
```

Parameters

`<1-16777215>`	VXLAN Network Identifier.
`all-vnids`	Delete all VxLAN network identifiers.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#no nvo vxlan id 100
```

nvo vxlan

Use this command to enable or disable VxLAN.

Command Syntax

```
nvo vxlan (enable | disable)
```

Parameters

None

Default

By default, the nvo vxlan option is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan enable

(config)#nvo vxlan disable
```


© 2021 IP Infusion Inc. Proprietary

nvo vxlan access-if

Use this command to map a complete interface or a VLAN or VLAN range on an interface to identify the tenant traffic and to enter NVO access interface mode.

The command "nvo vxlan access-if port <if_name> default" accepts all tagged, double tagged and untagged traffic received on the mapped physical port.

Use the `no` form of this command to unmap an interface or a VLAN.

Note: When a VxLAN access interface configured as a port VLAN as vlan-range or port as default, then arp-cache and nd-cache should be disabled and only VNID with inner-vid-enable is mapped.

Note: Inner-vid-enable is one-to-one mapping. VNID is mapped to only on one access-port.

Note: Vlan Range not allowed to be configured for Vxlan stacked access-port.

Command Syntax

```
nvo vxlan access-if (port IFNAME (| default) | port-vlan IFNAME VLAN_RANGE (|
  inner-vlan <2-4094>))
no nvo vxlan access-if (port IFNAME | port-vlan IFNAME VLAN_RANGE(| inner-vlan <2-
  4094>))
```

Parameters

`port`	A physical port.
`IFNAME`	Interface name (Physical/Static lag/Dynamic lag)
`default`	Default access interface
`port-vlan`	The physical port on which VLANs are configured
`IFNAME`	Interface name (Physical/Static lag/Dynamic lag)
`VLAN_RANGE`	Configure VlanId or Vlan-Range for outer vlan
`Inner-vlan`	Inner-vlan id
`<2-4094>`	VLAN id

Default

By default, the nvo vxlan access-if option is port VLAN ID and VLAN_RANGE option is introduced in OcNOS-SP version 5.0..

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2-10
(config-nvo-acc-if)#exit

#configure terminal
```

```
(config)#nvo vxlan access-if port xe1
(config-nvo-acc-if)#exit

#configure terminal
(config)#nvo vxlan access-if port xe1 default
(config-nvo-acc-if)#exit

#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2 inner-vlan 10
(config-nvo-acc-if)#exit
```


© 2021 IP Infusion Inc. Proprietary

nvo vxlan mac-ageing-time

Use this command to set the dynamically learned MAC aging time.

Use the `no` form of this command to set the age out the MACs in hardware to its default (300 seconds).

Command Syntax

```
nvo vxlan mac-ageing-time <10-572>
no nvo vxlan mac-ageing-time
```

Parameters

`<10-572>`	Ageing time in seconds.

Default

The default age out time is 300 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan mac-ageing-time 10
```

nvo vxlan max-cache-disable

Use this command to configure the maximum number of ARP and ND cache disables on access ports configured with the port+VLAN options. This command does not limit the ARP and ND cache disables on access ports created with only the port option.

Use the `no` form of this command to set the maximum number of ARP and ND cache disables to its default (0).

Note: If any mac is in conflict when the max cache disable is being unconfigured, then the corresponding caches will not be enabled. This can be enabled after manually, removing the conflict. Caches where there is no conflict, will be enabled.

Command Syntax

```
nvo vxlan max-cache-disable <1-200>
no nvo vxlan max-cache-disable
```

Parameters

`<-1-200>`	Number of ARP/ND cache disable allowed

Default

The default maximum number of ARP and ND cache disables is 0.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan max-cache-disable 10
(config-nvo)#exit
```


© 2021 IP Infusion Inc. Proprietary

nvo vxlan vtep-ip-global

Use this command to set the source IP address of the VxLAN tunnels.

Use the `no` form of this command to remove the source IP address of the VxLAN tunnels.

Command Syntax

```
nvo vxlan vtep-ip-global A.B.C.D
no nvo vxlan vtep-ip-global A.B.C.D
```

Parameters

`A.B.C.D`	Source VTEP IP address of the global configuration

Default

No default value is specified for nvo vxlan vtep-ip-global command.

Command Mode

NVO mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config-nvo)#nvo vxlan vtep-ip-global 10.10.11.1
```

show bgp l2vpn evpn

Use this command to display details about Layer 2 Virtual Private Network (L2VPN) Ethernet Virtual Private Network (EVPN) routes.

Note: A BGP EVPN route update received for an unreachable IP address is also listed by this command and as a best route. This is because the next hop tracking feature is not supported for the EVPN address family. However, the tunnel to this IP address is shown in unresolved state by the show nvo vxlan tunnel output.

Note: An E-tag (Ethernet tag) can have the value of zero/VID/VNID based on the use case. An E-tag can go up to 32 bits and no restrictions are noted in the RFC. Since an E-tag can have different values, it should not be compared with the label/VNID.

Command Syntax

```
show bgp l2vpn evpn ((vrf WORD)|(rd WORD)| time|)
show bgp l2vpn evpn mac-ip ((vrf WORD)|(rd WORD)|)
show bgp l2vpn evpn mcast
show bgp l2vpn evpn multihoming es-route <(rd WORD)|(vrf WORD)>
show bgp l2vpn evpn multihoming ethernet-ad-per-evi <(rd WORD)|(vrf WORD)>
show bgp l2vpn evpn multihoming ethernet-ad-per-es <(rd WORD)|(vrf WORD)>
```

Parameters

`vrf`	Virtual Routing and Forwarding instance
`WORD`	VRF name
`rd`	Route distinguisher
`WORD`	Route distinguisher: ASN:nn or IP:nn
`time`	Display learned time for EVPN routes
`mac-ip`	MAC/IP routes (EVPN type 2)
`mcast`	Multicast routes (EVPN type 3)

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp l2vpn evpn

BGP table version is 25, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
```


© 2021 IP Infusion Inc. Proprietary

```
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route

    Network          Next Hop            Metric    LocPrf       Weight Path  Peer

RD[1.1.1.1:1] VRF[vrfblue]:
*>   [2]:[0]:[100]:[48,0000.00aa.aaaa]:[32,10.1.1.2]:[100]
                      1.1.1.1             0         100            32768    i
*>i  [2]:[0]:[100]:[48,0000.00bb.bbbb]:[32,10.1.1.3]:[100]
                      4.4.4.4             0         100            0        i  10.1.1.1
*>   [3]:[100]:[32,1.1.1.1]
                      1.1.1.1             0         100            32768    i
*>i  [3]:[100]:[32,4.4.4.4]
                      4.4.4.4             0         100            0        i  10.1.1.1
*>   [3]:[101]:[32,1.1.1.1]
                      1.1.1.1             0         100            32768    i
*>i  [3]:[101]:[32,4.4.4.4]
                      4.4.4.4             0         100            0        i  10.1.1.1

RD[2.2.2.2:1]
*>i  [2]:[0]:[100]:[48,0000.00bb.bbbb]:[32,10.1.1.3]:[100]
                     4.4.4.4              0         100            0        i  10.1.1.1
*>i  [3]:[100]:[32,4.4.4.4]
                      4.4.4.4             0         100            0        i  10.1.1.1
*>i  [3]:[101]:[32,4.4.4.4]
                      4.4.4.4             0         100            0        i  10.1.1.1

Total number of prefixes 9
```

Table 1-236 shows the status codes displayed at the start of a route entry.

Table 1-236: status codes

Status code	Description	Comments
s	suppressed	Whether the route is suppressed and is not advertised to neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The selected route to be installed in the kernel routing table.
i	internal	The prefix was learned from an iBGP peer.
l	labeled	BGP Labeled Unicast advertises route information between inter region routers.

Table 1-237 shows the codes at the end of each route entry that indicate where the route originated.

Table 1-237: origin codes

Origin Code	Description	Comments
i	IGP	The route is from an Interior Gateway Protocol.
e	EGP	The route is from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an IGP.

Table 1-238 explains the fields for each route.

Table 1-238: route entry fields

Field	Description
RD	Route distinguisher: AS number or IP address.
VRF	Name of the VRF.
Network	EVPN route information. The route type indicates the type of routing information advertised by the EVPN control plane: 2 MAC/IP Route: Endpoint reachability information, including MAC and IP addresses of the endpoints. 3 Inclusive Multicast Route: Information about how to forward Broadcast, Unknown Unicast and Multicast (BUM) traffic. The other fields included depend on the route type: Type 2: [ESI]:[E-Tag]:[Length, Host MAC address]:[Length, Host IP address]:[Label/VNID] Type 3: [E-Tag]:[Length, PE IP address] ESI (Ethernet Segment Identifier): a unique non-zero identifier that identifies an Ethernet segment, which is a set of links that connects a network or device to one or more PEs. ESI 0 denotes a single-homed site. E-Tag (Ethernet tag): identifies a particular broadcast domain such as a VLAN or VNID in the VxLAN case. An EVPN instance consists of one or more broadcast domains. VNID (VXLAN network identifier): identifies Layer 2 segments and maintains Layer 2 isolation between the segments, allowing the addressing of up to 16 million logical networks in the same administrative domain. The status codes are explained in Table 1-236.
Next Hop	IP address of the nexthop for this route.
Metric	Multiple-Exit Discriminator (MED). If there are multiple paths to the same destination from a single routing protocol, then the multiple paths have the same administrative distance and the best path is selected based on this metric. The path with the lowest metric is selected as the optimal path and installed in the routing table.
LocPrf	Local preference set with the `set local-preference` command. This value is used only with iBGP sessions within the local autonomous system to determine if a route towards a destination is the “best” one. The path with the highest local preference is preferred.
Weight	This field applies only to routes within an individual router. If a route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.

© 2021 IP Infusion Inc. Proprietary

Table 1-238: route entry fields (Continued)

Field	Description
Path	The autonomous systems through which the prefix advertisement passed. The origin codes are explained in Table 1-237.
Peer	Neighbor address.
Total number of prefixes	The total number of prefixes listed.

show bgp l2vpn evpn summary

Use this command to display a summary of BGP EVPN neighbor status.

Command Syntax

```
show bgp l2vpn evpn summary
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 17
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/PfxRcd     AD  MACIP  MCAST    ESI
8.8.8.8                  4   100  111        112      17      0      0  00:53:03              3      0      0      3      0
9.9.9.9                  4   100  110        110      17      0      0  00:52:10             15      0     13      2      0
13.13.13.13              4   100  132        109      17      0      0  00:51:57              4      0      2      2      0

Total number of neighbors 3

Total number of Established sessions 3
```

The start of the output shows:

- The BGP router identifier and the local router AS number.
- The BGP table version tracks the local BGP table version. Any time the BGP best path algorithm executes, the table version increments.
- BGP AS-PATH entry and community entries.

Table 1-239 explains the fields for each neighbor entry.

Table 1-239: neighbor fields

Field	Description
Neighbor	IP address of peer.
V	BGP version of peer.
AS	Autonomous system number of peer.
MsgRcvd	Messages received since the BGP connection was established.
MsgSent	Messages sent since the BGP connection was established.

© 2021 IP Infusion Inc. Proprietary

Table 1-239: neighbor fields (Continued)

Field	Description
TblVer	Last version of the local router's BGP database advertised to the peer.
InQ	Received messages waiting in the input queue for further processing.
OutQ	Messages waiting in the output queue to be sent.
Up/Down	Connection up time in the interface.
State/PfxRcd	If the TCP session is up and the BGP peers have formed an adjacency, this field shows how many prefixes have been received from the remote neighbor. Other states: Idle: The local router has not allocated resources for the peer connection, so incoming connection requests are refused Idle (Admin): The peer has shut down Idle (PfxCt): Prefix overflow Idle (G-shut): Graceful shutdown Connect: BGP is waiting for the TCP connection to complete Active: the local router is trying to establish a TCP connection to the remote peer. You might see this if the local peer has been configured, but the remote peer is unreachable or has not been configured. OpenSent: BGP is waiting for an open message from its peer OpenConfirm: BGP received an open message from the peer and is now waiting for a keepalive or notification message. If BGP receives a keep alive message from the peer, the state changes to established. If the message is a notification, the state changes to idle. Established: BGP is ready to exchange update, notification, and keep alive messages with its peer Invalid: The session state is invalid.
AD	Number of EVPN type 1 Ethernet Auto-discovery routes: Only originated for multi-homed sites. Type 1 routes allow fast convergence where PE devices can change the next-hop adjacencies for all MAC addresses associated with a particular Ethernet Segment and aliasing where traffic can be balanced across multiple egress points
MACIP	Number of EVPN type 2 MAC/IP routes: Endpoint reachability information, including MAC and IP addresses of the endpoints.
MCAST	Number of EVPN type 3 Inclusive Multicast routes: Broadcast, Unknown Unicast and Multicast (BUM) traffic.
ESI	Number of EVPN type 4 Ethernet Segment Routes: Used in multi-homing for Designated Forwarder Election. The Designated Forwarder sends BUM traffic to the CE on a particular Ethernet Segment.

show nvo vxlan

Use this command to display VXLAN information.

Command Syntax

```
show nvo vxlan (vnid <1-16777215>|)
```

Parameters

<1-16777215>	VXLAN network identifier.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh nvo vxlan
VXLAN Information
================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID     Vni-name     Type Interface ESI                             Vlan DF-
Status Src-addr         Dst-addr
_____________________________________________________________________________
_____________________________________
10       ----         NW   ----      ----                            ---- ----
      1.1.1.1          3.3.3.3
10       ----         NW   ----      ----                            ---- ----
      1.1.1.1          2.2.2.2
10       ----         AC   ce21/1    00:00:11:22:33:44:55:66:77:88 2
DF        ----             ----
20       ----         NW   ----      ----                            ---- ----
      1.1.1.1          3.3.3.3
20       ----         NW   ----      ----                            ---- ----
      1.1.1.1          2.2.2.2
20       ----         AC   ce21/1    00:00:11:22:33:44:55:66:77:88 3    NON-
DF    ----             ----

Total number of entries are 6
```

Table 1-240 explains the fields in the output.

Table 1-240: VxLAN fields

Field	Description
VNID	VXLAN network identifier.
Type	NW - Network Port: VxLAN tunnel AC - Access Port: Host connection

© 2021 IP Infusion Inc. Proprietary

Table 1-240: VxLAN fields

Field	Description
Interface	Name of the Interface.
Vlan	VLAN identifier
Src-addr	Source address in the interface.
Dst-addr	Destination address in the interface.
Total number of entries	The total number of entries listed.

show nvo vxlan access-if-config

Use this command to display the current running configuration of the access interface.

Command Syntax

```
show nvo vxlan access-if-config (LINE|)
```

Parameters

LINE	Access port description.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3,

Added new cli "garp-gna enable" under access-if cli in OcNOS version 1.3.6.

Example

```
#show nvo vxlan access-if-config
nvo vxlan access-if port-vlan xe1 2
map vnid 100
garp-gna enable
access-if-description member-port with xe1 as vlan 2
dynamic-learning disable
arp-nd flood-suppress
arp-cache disable
nd-cache disable
shutdown
mac 0000.0000.1111
mac 0000.0000.aaaa  ip 12.12.12.1
mac 0000.0000.bbbb  ipv6 1201::1
map qos-profile ingress 100
cos 2 egress
     !
      nvo vxlan access-if port-vlan po1 6 inner-vlan 5
      encapsulation 0x9100
      no shutdown
      map vnid 100
     !
```


© 2021 IP Infusion Inc. Proprietary

show nvo vxlan arp-cache

Use this command to display the ARP cache information.

Command Syntax

```
show nvo vxlan arp-cache (vnid <1-16777215>|summary|)
```

Parameters

`<1-16777215>` VXLAN network identifier.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3, modified to include new fields – Age-Out and Retries-Left in OcNOS version 1.3.5.

Remote Static and Dynamic keyword got changed to Static and Dynamic Remote in MAC table in OcNOS version 1.3.6.

Example

```
#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
ND Timeout :  300 sec   Random-Jitter-Max : 640

VNID     Ip-Addr          Mac-Addr       Type         Age-Out    Retries-Left
_____________________________________________________________________________
10       11.11.11.2       0000.0000.bbbb Dynamic Local  224      2
10       11.11.11.1       0000.0000.aaaa Dynamic Remote----
Total number of entries are 2
```

Table 1-245 explains the output fields.

Table 1-241: ARP cache fields

Field	Description
VNID	VXLAN network identifier
Ip-Addr	IP address of the vxlan
Mac-Addr	Device MAC address
Type	How a host learns a MAC/IP pair: Dynamic: Learned by data plane source learning Evpn: Learned by EVPN Type 2 (MAC/IP) routes Static Remote: Statically configured for remote; used only for static VxLAN, not with EVPN Static Local: Configured on local VTEP

Table 1-241: ARP cache fields

Field	Description
Age=Out	ARP entry expire time
Total number of entries	The total number of entries listed.

© 2021 IP Infusion Inc. Proprietary

show nvo vxlan counters access-port

Use this command to display the receive and transmit counters of an access port including ARP, ND and GARP counters in the same command.

Note: Due to a limitation in the hardware, the transmit packet counters includes the BUM traffic received on that port.

Command Syntax

```
show nvo vxlan counters access-port (port IFNAME | port-vlan IFNAME VLAN_ID)
```

Parameters

port	Port Mapping
IFNAME	Access port name
port-vlan	Port-vlan Mapping
IFNAME	Access port name
VLAN_ID_RANGE	Vlan Id or Vlan Range <2-4094>
INNER_VLAN_ID	Inner-Vlan Id
all	All ports and VLANs

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3 and added Control packet (ARP, ND and GARP) counters in OcNOS version 1.3.5. The VLAN_RANGE option is introduced in OcNOS-SP version 5.0.

Example

```
#show nvo vxlan counters access-port port-vlan xe1 2
     Data packets:
      *If ARP/ND cache is enabled, TX doesn't count ARP/ND replies
     from  ARP/ND cache and ARP/ND forwarded after uplifting to
     the control plane.
      RX:  packets  : 2774939
           bytes    : 210553516
      TX:  packets  : 4322274
           bytes    : 326026474

     Control Packets:
      *ARP/ND uplifted and sent/replied from control plane:
     Rx Vxlan Arp discard count           : 0
     Rx Vxlan Nd discard count            : 2
     Tx Vxlan Arp discard count           : 0
     Tx Vxlan Nd discard count            : 0
     Rx Vxlan Arp Request count           : 2
     Tx Vxlan Arp Request count           : 0
     Rx Vxlan Arp Reply count             : 5
     Tx Vxlan Arp Reply count             : 1
     Rx Vxlan Neighbor Solicitation count : 6
     Tx Vxlan Neighbor Solicitation count : 0
```

```
 Rx Vxlan Neighbor Advertisement count: 0
 Tx Vxlan Neighbor Advertisement count: 4
 Rx Vxlan Gratuitous ARP count        : 0
 Tx Vxlan Gratuitous ARP count        : 0
 Rx Vxlan Gratuitous Neighbor Advertisement count: 3
 Tx Vxlan Gratuitous Neighbor Advertisement count: 0
#
```

Table 1-242 explains the fields in the output.

Table 1-242: access port counters

Field	Description
RX: packets	Number of packets received.
RX: bytes	Number of bytes received.
TX: packets	Number of packets transmitted.
TX: bytes	Number of bytes transmitted.
Rx Vxlan Nd discard count	Number of discarded ND that is received from neighbor.
Tx Vxlan Arp discard count	Number of discarded Arp that is transmitted to peer.
Rx Vxlan Nd discard count	Number of discarded ND that is transmitted to peer.
Rx Vxlan Arp Request count	Number of request ARP that is received from neighbor.
Tx Vxlan Arp Request count	Number of request ARP that is transmitted to peer.
Rx Vxlan Arp Reply count	Number of replied ARP that is received from neighbor.
Tx Vxlan Arp Reply count	Number of replied ARP which is transmitted to peer.
Rx Vxlan Neighbor Solicitation count	Number of request ND that is received from neighbor.
Tx Vxlan Neighbor Solicitation count	Number of replied ND that is transmitted to peer.
Rx Vxlan Neighbor Advertisement count	Number of Neighbor Advertisement that is received from neighbor.

© 2021 IP Infusion Inc. Proprietary

Table 1-242: access port counters (Continued)

Field	Description
Tx Vxlan Neighbor Advertisement count	Number of Neighbor Advertisement that is transmitted to peer
Rx Vxlan Gratuitous ARP count	Number of Gratuitous ARP that is received from neighbor.
Tx Vxlan Gratuitous ARP count	Number of Gratuitous ARP which is transmitted to peer.
Rx Vxlan Gratuitous Neighbor Advertisement count	Number of Gratuitous Neighbor Advertisement that is received from neighbor.
Tx Vxlan Neighbor Gratuitous Advertisement count	Number of Gratuitous Neighbor Advertisement which is transmitted to peer.

show nvo vxlan counters network-port

Use this command to display the receive and transmit counters of a network port including ARP, ND and GARP counters in the same command.

Command Syntax

```
show nvo vxlan counters network-port dst A.B.C.D
```

Parameters

A.B.C.D	Tunnel IPv4 address

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3 and added control packets (ARP, ND, and GARP) counters in OcNOS version 1.3.5.

Example

```
VTEP1#sh nvo vxlan counters network-port dst 100.2.2.2

Data packets:
   *If ARP/ND cache is enabled, TX doesn't count ARP/ND replies
 from  ARP/ND cache and ARP/ND forwarded after uplifting to
 the control plane.
   RX:  packets  : 814327
        bytes    : 92833544
   TX:  packets  : 1508023
        bytes    : 171914622

Control Packets:
 *ARP/ND uplifted and sent/replied from control plane:
  TX VXLAN Arp discard count           : 0
  TX VXLAN ND discard count            : 0
  Tx Vxlan Arp Request count           : 0
  Tx Vxlan Arp Reply count             : 0
  Tx Vxlan Neighbor Solicitation count : 0
  Tx Vxlan Neighbor Advertisement count: 0
  Rx Vxlan Gratuitous ARP count: 0
  Tx Vxlan Gratuitous ARP count: 0
  Rx Vxlan Gratuitous Neighbor Advertisement count: 0
  Tx Vxlan Gratuitous Neighbor Advertisement count: 0
```

Table 1-243 explains each network entry fields.

© 2021 IP Infusion Inc. Proprietary

Table 1-243: show nvo vxlan counters network-port output fields

Field	Description
RX: packets	Number of hello packets received from neighbor.
RX: bytes	Number of hello packets received from neighbor in bytes received.
TX: packets	Number of hello packets transmitted to neighbor.
TX: bytes	Number of hello packets transmitted to neighbor in bytes transmitted.
Rx Vxlan Nd discard count	Number of discarded ND that is received from neighbor.
Tx Vxlan Arp discard count	Number of discarded Arp that is transmitted to peer.
Rx Vxlan Nd discard count	Number of discarded ND that is transmitted to peer.
Rx Vxlan Arp Request count	Number of request ARP that is received from neighbor.
Tx Vxlan Arp Request count	Number of request ARP that is transmitted to peer.
Rx Vxlan Arp Reply count	Number of replied ARP that is received from neighbor.
Tx Vxlan Arp Reply count	Number of replied ARP which is transmitted to peer.
Rx Vxlan Neighbor Solicitation count	Number of request ND that is received from neighbor.
Tx Vxlan Neighbor Solicitation count	Number of replied ND that is transmitted to peer.
Rx Vxlan Neighbor Advertisement count	Number of Neighbor Advertisement that is received from neighbor.
Tx Vxlan Neighbor Advertisement count	Number of Neighbor Advertisement that is transmitted to peer.
Rx Vxlan Gratuitous ARP count	Number of Gratuitous ARP that is received from neighbor.
Tx Vxlan Gratuitous ARP count	Number of Gratuitous ARP which is transmitted to peer.
Rx Vxlan Gratuitous Neighbor Advertisement count	Number of Gratuitous Neighbor Advertisement that is received from neighbor.
Tx Vxlan Neighbor Gratuitous Advertisement count	Number of Gratuitous Neighbor Advertisement which is transmitted to peer.

show nvo vxlan mac-table

Use this command to display the host MAC address table. Use the `hardware` option to see the age out time for dynamically learned macs.

Command Syntax

```
show nvo vxlan mac-table (vnid <1-16777215>|) (summary | hardware |)
```

Parameters

`<1-16777215>`	VXLAN network identifier.
`summary`	Count the MAC addresses.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Remote Static and Dynamic keyword got changed to Static and Dynamic Remote in MAC table in OcNOS version 1.3.6.

Example

```
#show nvo vxlan mac-table
================================================================================
================================================================
                      VXLAN MAC Entries
================================================================================
================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/
ESI                    Type                 Status              AccessPortDesc
________________________________________________________________________________
________________________________________________________________

10        ce21/1     2      ----         0000.0000.1111
1.1.1.1                      Static Local         -------
partner-port
10        ----       ----   ----         0000.0000.2222
3.3.3.3                      Static Remote        -------             ------
-
20        ce21/1     3      ----         0000.0000.cccc
1.1.1.1                      Static Local         Discard             ------
-
20        ----       ----   ----         0000.0000.dddd
3.3.3.3                      Static Remote        -------             ------
-

Total number of entries are : 4

#show nvo vxlan mac-table hardware
================================================================================
================================================================
                        VXLAN MAC Entries
================================================================================
================================================================
```


© 2021 IP Infusion Inc. Proprietary

```
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/
ESI                    Type                 Status            Time-out
AccessPortDesc
_____________________________________________________________________________
_____________________________________________________________________________

10         ce21/1    2      ---          0000.0000.1111
1.1.1.1                      Static Local         -----             ---
partner-port
10         ---       ---    ---          0000.0000.2222
3.3.3.3                      Static Remote               -----             -
--
10         ---       ---    ---          0000.0000.aa11
3.3.3.3                      Static Remote               -----             -
--
10         ce21/1    2      ---          0000.0000.bb11
1.1.1.1                      Dynamic Local        -----             300
partner-port
10         ce21/1    2      ---          0000.0000.bb12
1.1.1.1                      Dynamic Local        -----             277
partner-port
20         ce21/1    ---    ---          0000.0000.cccc
1.1.1.1                      Static Local         Discard           ---
20         ---       ---    ---          0000.0000.dddd
3.3.3.3                      Static Remote               -----             -
--

Total number of entries are 7
```

Table 1-244 explains the fields in the output.

Table 1-244: MAC table fields

Field	Description
VNID	VXLAN network identifier
Interface	Interface name
VlanId	VLAN identifier
Mac-Addr	MAC address
VTEP-Ip	VTEP identifier/Ethernet Segment Identifier
Type	How a host learns a MAC/IP pair: Remote: Statically configured for remote; used only for static VxLAN, not with EVPN Static Local: Configured on local VTEP Dynamic Local: Learned by data plane source learning
Status	Max Move conflict: When a MAC has moved too many times (5 or more times in 180 seconds). This is according to the procedures defined in RFC 7432, Section 15.1. Discard: If a MAC hold time is configured, then if the VxLAN access port goes down (admin or operational), the MAC is moved to the discard state for the period of the hold time. The MAC is also moved to the discard state if the VNID is unmapped from the port. In dynamically learned cases, the MAC is also moved to discard when learning is disabled.
Time-out	Age timeout for dynamically learned MACs.

Table 1-244: MAC table fields (Continued)

Field	Description
AccessPortDesc	Access port description.
Total number of entries	The total number of entries listed.

© 2021 IP Infusion Inc. Proprietary

show nvo vxlan nd-cache

Use this command to display the Neighbor Discovery cache.

Command Syntax

```
show nvo vxlan nd-cache (vnid <1-16777215>|summary|)
```

Parameters

<1-16777215>	VXLAN network identifier.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3, modified to include new fields – Age-Out and Retries-Left in OcNOS version 1.3.5.

Remote Static and Dynamic keyword got changed to Static and Dynamic Remote in ND table in OcNOS version 1.3.6.

Example

```
#show nvo vxlan nd-cache
VXLAN ND-CACHE Information
==========================
ND Timeout :  300 sec   Random-Jitter-Max : 640

VNID     Ip-Addr          Mac-Addr       Type          Age-Out    Retries-Left
_____________________________________________________________________________
10       2001::1       0000.0000.1111   Dynamic Local   274           2
10       2001::2       0000.0000.2222   Dynamic Remote  ----
Total number of entries are 2
```

Table 1-245 explains the output fields.

Table 1-245: ND cache fields

Field	Description
VNID	VXLAN network identifier
Ip-Addr	IP address
Mac-Addr	MAC address
Type	How a host learns a MAC/IP pair: Static Remote: Statically configured for remote; used only for static VxLAN, not with EVPN Static Local: Configured on local VTEP Dynamic: Learned by data plane source learning Evpn: Learned by EVPN Type 2 (MAC/IP) routes

Table 1-245: ND cache fields

Field	Description
Age-Out	ND entry expire Time
Total number of entries	The total number of entries listed.

© 2021 IP Infusion Inc. Proprietary

show nvo vxlan static host state

Use this command to display the state of the host which is configured statically.

Command Syntax

```
show nvo vxlan static host state
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh nvo vxlan static host state
VNID Ifname    Vlan      Ip-Addr        Mac-Addr         Status
_____________________________________________________________________
100      xe1          2      12.12.12.1       0000.0000.aaaa      Inactive
100      xe2          2      1201::1          0000.0000.bbbb      Conflict
100      xe3          2      120.120.120.1    0000.0000.bb11      Active
```

Table 1-246 explains the output fields.

Table 1-246: Static host fields

Field	Description
VNID	VXLAN network identifier
Ifname	Interface name
Vlan	VLAN name
Ip-Addr	IP address

Table 1-246: Static host fields

Field	Description
Mac-Addr	MAC address
Status	Status of the MAC/IP on the host: Conflict: When a MAC/IP was configured, the conflict was not known as the VNID was not mapped to the access port. After the VNID is mapped, if the same MAC/IP is present statically on some other port on the same VNID, then it is in conflict state. Learnt Conflict: When a MAC/IP was configured, the conflict was not known. However, it is now in conflict because the same MAC/IP is configured on an access port on VTEP1 and on an access port on VTEP2. Because the BGP session/tunnel was not up, the MAC/IP was not known to the other VTEP and the configuration was allowed. When the BGP session/tunnel comes up and it finds such a conflicted route, it marks the state as Learnt Conflict. Inactive: Configured but not operating, such as when the port is not mapped to any VNID. The port is down and the ARP/ND cache is disabled. Active: Operating host MAC/IP.

© 2021 IP Infusion Inc. Proprietary

show nvo vxlan tunnel

Use this command to view the source, destination, and status of the VxLAN tunnel entries.

Command Syntax

```
show nvo vxlan tunnel
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show nvo vxlan tunnel` command.

```
#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source Destination      Status Up/Down Update
=====================================================
1.1.1.1 2.2.2.2          Installed 00:00:20 00:00:20
Total number of entries are 1
#
```

Table 1-247 explains the output fields.

Table 1-247: VxLAN tunnel fields

Field	Description
Source	Tunnel source IP address.
Destination	Tunnel destination IP address.
Status	Installed: Tunnel Installed in the hardware and operating. Resolved: Tunnel destination IP is reachable, but VxLAN tunnel not installed in hardware. Therefore, not operating. Unresolved: Tunnel destination IP not reachable because L3 route is down.
Up/Down	When the tunnel came up or went down
Update	When the tunnel was last updated
Total number of entries	The total number of entries listed.

show running-config nvo vxlan

Use this command to display the current running configuration of VxLANs.

Command Syntax

```
show running-config nvo vxlan
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in a version before OcNOS version 1.3 and added few CLIs for IRB and ARP-ND refresh timer for OcNOS version 1.3.5.

Example

```
#show running-config nvo vxlan
!
     nvo vxlan multihoming enable
!
     nvo vxlan enable
     !
     nvo vxlan vtep-ip-global 1.1.1.1
     !
     nvo vxlan max-cache-disable 10
     !
     nvo vxlan tunnel qos-map-mode cos-dscp ingress QUE_DSCP
     !
     nvo vxlan tunnel qos-map-mode cos-dscp egress DSCP_QUE
     !
     nvo vxlan id 100 ingress-replication inner-vid-disabled
      vxlan host-reachability-protocol evpn-bgp vrf1
      mac-holdtime 20
     !
     nvo vxlan access-if port-vlan xe1 2
      map vnid 100
access-if-description member-port with xe1 as vlan 2
dynamic-learning disable
arp-nd flood-suppress
arp-cache disable
nd-cache disable
shutdown
mac 0000.0000.1111
mac 0000.0000.aaaa  ip 12.12.12.1
mac 0000.0000.bbbb  ipv6 1201::1
map qos-profile cos-to-queue COS_QUE
map qos-profile queue-color-to-cos QUE_COS
     !
     nvo vxlan access-if port-vlan po1 6 inner-vlan 5
      encapsulation 0x9100
```

 © 2021 IP Infusion Inc. Proprietary

```
 no shutdown
 map vnid 100
!
```

show evpn multi-homing all

Use this command to display the multi-homed VTEP details.

Command Syntax

```
show evpn multi-homing (all |)
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show evpn multi-homing all
ESI                             Access-IF    PE-IP-ADDRESS
============================================================
00:00:11:22:33:44:55:66:77:88   ce21/1       1.1.1.1
00:00:11:22:33:44:55:66:77:88   ----         2.2.2.2
Total number of entries are 2
```

Table 1-248 explains the output fields.

Table 1-248: show evpn multi-homing all output details

Field	Description
ESI	An Ethernet segment has an unique nonzero identifier, called the Ethernet segment identifier (ESI). The ESI is encoded as a 10-octet integer that identifies this segment. When manually configuring an ESI value, the most significant octet, known as the type byte, must be 00. When a single-homed CE device is attached to an Ethernet segment, the entire ESI value is zero.
Access-IF	Map the access port ce21/1 for evpn.
PE-IP-ADDRESS	Address of the provider edge router in the interface.

© 2021 IP Infusion Inc. Proprietary

show evpn multihoming-status

Use this command to display the status of multihoming on a VTEP.

Command Syntax

```
show evpn multihoming-status
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show evpn multihoming-status
Multihoming is ACTIVE in Hardware
```

show nvo vxlan route-count

Use this command to display the vxlan active route (MAC-IP.MAC-IPv6 and MAC-only) count information.

Command Syntax

```
show nvo vxlan route-count (|vnid <1-16777215>)
```

Parameters

`<1-16777215>`	Range supported for VNID.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3 and modified to include new fields – GW-IPv4, GW_IPv6, Prefix IPv4 and Prefix IPv6 in OcNOS version 1.3.5.

Example

```
#show nvo vxlan route-count
VXLAN Active route count information
====================================
Max route count   : 32768
Active route count: 7

Note: Prefix count refers only local routes
      It does not include evpn prefix routes

-------------------------------------------------------------------------------
----------
 VNID     Total    MACONLY  MACIPv4  MACIPv6  GW         GW         Prefix
Prefix
                                              MACIPv4    MACIPv6    IPv4
IPv6
-------------------------------------------------------------------------------
----------
 2000     3        1        1        1        0          0          0
0
 1000     0        0        0        0        0          0          0
0
 10002    4        0        0        0        1          1          1
1

Total number of entries are 3
```

Table 1-249 explains the output fields.

Table 1-249: show nvo vxlan route-count output details

Field	Description
Max route count	Maximum number of route count in vxlan.
Active route count	Number of active route count in the interface.

© 2021 IP Infusion Inc. Proprietary

Table 1-249: show nvo vxlan route-count output details

Field	Description
VNID	VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.
Total	Total number of entries for the interface.
MACONLY	The MAC-only route for the local interface appears in the VXLAN instance route table.
MACIPv4	IPv4 media access control (MAC) address for a default virtual gateway.
MACIPv6	IPv6 media access control (MAC) address for a default virtual gateway.

show nvo vxlan vni-name

Use this command to display the vxlan results bashed on vni-name.

Command Syntax

```
show nvo vxlan vni-name (WORD)
```

Parameters

WORD	VNI name of max size 10 character and should not be only numeric.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show nvo vxlan vni-name SITEA-PRO
VXLAN Information
=================
Codes: NW - Network Port
AC - Access Port
(u) - Untagged
VNID Vni-name Type Interface ESI Vlan DF-Status Src-addr Dst-addr
_____________________________________________________________________________________
_____________________________
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.6.8
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.6.9
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.3.1
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.1.2
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.5.1
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.2.2
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.2.1
1 SITEA-PRO AC xe7 — Single Hommed port — 2 ------ ---- ----
1 SITEA-PRO AC xe1 — Single Hommed port — 1010 ------ ---- ----
1 SITEA-PRO AC xe1 — Single Hommed port — 100 ------ ---- ----
1 SITEA-PRO AC xe1 — Single Hommed port — 2020 ------ ---- ----
1 SITEA-PRO AC po1 — Single Hommed port — 100 ------ ---- ----
1 SITEA-PRO AC po1 — Single Hommed port — 2 ------ ---- ----
1 SITEA-PRO AC po1 — Single Hommed port — 200 ------ ---- ----
1 SITEA-PRO AC xe8 — Single Hommed port — ---- ------ ---- ----
1 SITEA-PRO AC po2 — Single Hommed port — ---- ------ ---- ----
Total number of entries are 16
```


© 2021 IP Infusion Inc. Proprietary

shutdown

Use this command to administratively shut down an NVO access interface.

Use the `no` form of this command to start an NVO access interface.

Command Syntax

```
shutdown
no shutdown
```

Parameters

None

Default

The NVO access interface is running by default.

Command Mode

NVO access interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#shutdown
(config-nvo-acc-if)#exit
```

vxlan host-reachability-protocol evpn-bgp

Use this command to set the host reachable protocol to Ethernet-VPN over BGP. This defines BGP as the mechanism for host reachability advertisement.

Use use the no form of this command to remove Ethernet-VPN as the host reachable protocol.

Command Syntax

```
vxlan host-reachability-protocol evpn-bgp NAME
no vxlan host-reachability-protocol evpn-bgp
```

Parameters

NAME	Name of the VRF to carry VNID routes.

Default

No default value is specified for vxlan host-reachability-protocol command.

Command Mode

NVO mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#nvo vxlan id 3
(config-nvo)#vxlan host-reachability-protocol evpn-bgp Blue
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 VXLAN Quality of Service Commands

This chapter describes the VXLAN commands for QoS (Quality of Service):

- clear nvo vxlan tunnels
- cos queue
- dscp queue
- map qos-profile cos-to-queue
- map qos-profile queue-color-to-cos
- nvo vxlan tunnel qos-map-mode cos-dscp
- qos profile cos-to-queue
- qos profile dscp-to-queue
- qos profile queue-color-to-cos
- qos profile queue-color-to-dscp
- queue cos
- queue dscp

© 2021 IP Infusion Inc. Proprietary

clear nvo vxlan tunnels

Use this command to clear the nvo vxlan tunnels to re-establish the tunnel after mapping/un-mapping the QoS profile to vxlan tunnel.

Command Syntax

```
clear nvo vxlan tunnels (|dst-ip A.B.C.D)
```

Parameters

`dst-ip`	VXLAN tunnel destination
`A.B.C.D`	destination IPv4 address

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
#clear nvo vxlan tunnels dst-ip 2.2.2.2
```

Note: `clear nvo vxlan tunnels` This command will clear all the VXLAN tunnels destination.

`clear nvo vxlan tunnels dst-ip A.B.C.D -` This command to clear individual tunnel destination(i.e A.B.C.D).

© 2021 IP Infusion Inc. Proprietary

cos queue

Use this command to configure user defined mapping for cos and queue.

Use the `no` form of this command to remove the mapping.

Command Syntax

```
cos <0-7> queue <0-7>
no cos <0-7>
```

Parameters

`<0-7>`	COS and Queue ranger

Default

Default cos and queue value is one-one default mapping if it is not configured.

Command Mode

QoS config mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
(config)#qos profile cos-to-queue ac_port_ingress
(config-ingress-cos-map)#cos 1 queue 7
(config-ingress-cos-map)#no cos  1
```

dscp queue

Use this command to configure user defined mapping for DSCP to queue. This will be mapped with nvo VXLAN tunnel of remote VTEP.

Use the `no` form of this command to delete the mapping.

Command Syntax

```
dscp <0-63> queue <0-7> (color (green|yellow|red)|) (dscp <0-63>|)
no dscp <0-63>
```

Parameters

`<0-63>`	DSCP
`<0-7>`	Queue number
`color`	Color to map
`green`	Set mapping for green packets
`red`	Set mapping for red packets
`yellow`	Set mapping for yellow packets
`<0-63>`	out DSCP value

Default

Default queue and cos value is one-one default mapping if it is not configured.

Command Mode

Ingress-dscp-map mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
(config)#qos profile dscp-to-queue nw_profile
(config-ingress-dscp-map)#dscp 50 queue 1
(config-ingress-dscp-map)#no dscp 50
```


© 2021 IP Infusion Inc. Proprietary

map qos-profile cos-to-queue

Use this command to map the cos-to-queue profile to vxlan access port on the local VTEP.

Use the `no` form of the command to remove the mapping.

Command Syntax

```
map qos-profile cos-to-queue NAME
no map qos-profile cos-to-queue NAME
```

Parameters

`NAME`	Profile name

Default

None

Command Mode

NVO access interface mode

Applicability

This command was introduced in OcNOS DC version 4.2.

Example

```
(config)#nvo vxlan access-if port-vlan xe1 10
(config-nvo-acc-if)#map qos-profile cos-to-queue ac_port_ingress
(config-nvo-acc-if)#no map qos-profile cos-to-queue ac_port_ingress
```

© 2021 IP Infusion Inc. Proprietary

map qos-profile queue-color-to-cos

Use this command to map the queue-color-to-cos profile to vxlan access port on the remote VTEP.

Use the `no` form of the command to remove the mapping.

Command Syntax

```
map qos-profile queue-color-to-cos NAME
no map qos-profile queue-color-to-cos NAME
```

Parameters

`NAME`	Profile name

Default

None

Command Mode

NVO access interface mode

Applicability

This command was introduced in OcNOS DC version 4.2.

Example

```
(config)#nvo vxlan access-if port-vlan xe2 10
(config-nvo-acc-if)#map qos-profile queue-color-to-cos ac_profile
(config-nvo-acc-if)#no map qos-profile queue-color-to-cos ac_profile
```


© 2021 IP Infusion Inc. Proprietary

nvo vxlan tunnel qos-map-mode cos-dscp

Use this command to map QoS profile for network side to nvo vxlan tunnel. For outgoing/incoming traffic, you need to provide the direction with the keyword `egress`/`ingress`.

Use the `no` form of this command to delete the mapping.

You must give the clear nvo vxlan tunnels command to do the network port setting for QoS profile mapped.

Command Syntax

```
nvo vxlan tunnel qos-map-mode cos-dscp (ingress|egress) NAME
no nvo vxlan tunnel qos-map-mode cos-dscp (ingress|egress)
```

Parameters

`NAME`	Profile name
`ingress`	Ingress direction
`egress`	Egress direction

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
(config)#nvo vxlan tunnel qos-map-mode cos-dscp egress nw_profile
(config)#no nvo vxlan tunnel qos-map-mode cos-dscp egress
(config)#nvo vxlan tunnel qos-map-mode cos-dscp ingress nw_profile
(config)#no nvo vxlan tunnel qos-map-mode cos-dscp ingress
```

© 2021 IP Infusion Inc. Proprietary

qos profile cos-to-queue

Use this command to configure cos-to-queue profile. This profile has to be mapped to VXLAN access port on the local VTEP.

Use the `no` form of this command to delete the qos profile.

Command Syntax

```
qos profile cos-to-queue (NAME|default)
no qos profile cos-to-queue NAME
```

Parameters

`NAME`	QoS profile name for cos-to-queue
`default`	Default name

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
(config)#qos profile cos-to-queue ac_port_ingress
(config)#no qos profile cos-to-queue ac_port_ingress
```


© 2021 IP Infusion Inc. Proprietary

qos profile dscp-to-queue

Use this command to configure QoS profile for DSCP to Queue mapping. This profile will be mapped to nvo vxlan tunnel of remote VTEP. The created profile will support remarking of the data packets.

Use the `no` form of this command to delete the QoS profile

Command Syntax

```
qos profile dscp-to-queue (NAME|default}
no qos profile dscp-to-queue NAME
```

Parameters

`NAME`	Profile name
`default`	Default name

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
(config)#qos profile dscp-to-queue nw_profile
(config-ingress-dscp-map)#exit
(config)#no qos profile dscp-to-queue nw_profile
(config)#
```

qos profile queue-color-to-cos

Use this command to configure queue-color-to-cos profile. This profile has to be mapped to VXLAN access port on remote VTEP.

Use the `no` form of this command to delete the qos profile.

Command Syntax

```
qos profile queue-color-to-cos (NAME|default)
no qos profile queue-color-to-cos NAME
```

Parameters

`NAME`	Profile name
`default`	Default name

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
(config)#qos profile queue-color-to-cos ac_profile
(config)#no qos profile queue-color-to-cos ac_profile
```


© 2021 IP Infusion Inc. Proprietary

qos profile queue-color-to-dscp

Use this command to create a QoS profile queue-color-to-dscp. This profile will be mapped to nvo vxlan tunnel of local VTEP. The created profile supports remarking of the data packets.

Use the `no` form of this command to delete the profile.

Command Syntax

```
qos profile queue-color-to-dscp (NAME|default)
no qos profile queue-color-to-dscp NAME
```

Parameters

`NAME`	Profile name
`default`	Default name

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
(config)#qos profile queue-color-to-dscp nw_profile
(config-egress-dscp-map)#exit
(config)#no qos profile queue-color-to-dscp nw_profile
```

queue cos

Use this command to configure user defined mapping for queue and cos.

Use the no form of this command to remove the mapping.

Command Syntax

```
queue <0-7> (color(green|yellow|red|all)|) cos <0-7>
no queue <0-7> (color(green|yellow|red|all)|)
```

Parameters

`<0-7>`	Queue and cos range
`color`	Color to map
`all`	Set mapping for all packets
`green`	Set mapping for green packets
`red`	Set mapping for red packets
`yellow`	Set mapping for yellow packets

Default

Default queue and cos value is one-one default mapping if it is not configured.

Command Mode

QoS config mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
(config)#qos profile queue-color-to-cos ac_profile
(config-egress-cos-map)#queue 5 cos 2
(config-egress-cos-map)#no queue 5
```


© 2021 IP Infusion Inc. Proprietary

queue dscp

Use this command to configure user-defined mapping for queue to DSCP. This will be mapped with nvo VXLAN tunnel of local VTEP.

Use the `no` form of this command to remove the queue-to-DSCP mapping.

Command Syntax

```
queue <0-7> (color(green|yellow|red|all)|) dscp <0-63>
no queue <0-7> (color(green|yellow|red|all)|)
```

Parameters

`<0-7>`	Queue number
`<0-63>`	DSCP
`color`	Color to map
`all`	Set mapping for all packets
`green`	Set mapping for green packets
`red`	Set mapping for red packets
`yellow`	Set mapping for yellow packets

Default

Default queue and cos value is one-one default mapping if it is not configured.

Command Mode

QoS config mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
(config)#qos profile queue-color-to-dscp nw_profile
(config-egress-dscp-map)# queue 1 dscp 63
(config-egress-dscp-map)#no queue 1
```

© 2021 IP Infusion Inc. Proprietary

SECTION 14 Guest Virtual Machine

Guest Virtual Machine Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Guest Virtual Machine Command Reference*

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Guest Virtual Machine Command Reference

This chapter contains the guest virtual machine commands.

- debug vm-events
- dhcp-lease-max
- dhcp-lease-time
- dhcp-range
- disk-image
- feature guest-vm
- gateway-ip
- host-core-affinity
- iptables
- iptables restore
- iptables-template
- memory
- nat dnat
- nat snat
- os-type
- os-variant
- reload vm-name
- secondary-disk-image
- service dns-masq
- show vm
- show vm-bridge
- show vm-iptables
- show vm-iptables kernel
- show vm-nat details
- show vm-template
- start vm-name
- static-bind
- stop vm-name
- vcpu count
- virt-type
- virtual-nic
- vm-bridge-create
- vm-image delete
- vm-template

© 2021 IP Infusion Inc. Proprietary

debug vm-events

Use this command to log virtual machine operations.

Use the `no` form of this command to stop logging virtual machine operations.

Command Syntax

```
debug vm-events
no debug vm-events
```

Parameters

None

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug vm-events
```


© 2021 IP Infusion Inc. Proprietary

dhcp-lease-max

Use this command to set the maximum number of DHCP leases for the VM bridge.

Command Syntax

```
dhcp-lease-max <10-1000>
```

Parameters

<10-1000>	Maximum number of DHCP leases

Default

The default maximum number of DHCP leases is 1000.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#dhcp-lease-max 100
```

dhcp-lease-time

Use this command to set the maximum time for leasing an IP address for the VM bridge.

Command Syntax

```
dhcp-lease-time <2-3600>
```

Parameters

<2-3600>	Maximum time for leasing an IP address in minutes

Default

The default maximum time for leasing an IP address is 360 minutes.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#dhcp-lease-time 1400
```


© 2021 IP Infusion Inc. Proprietary

dhcp-range

Use this command to set a DHCP range for the virtual machine bridge.

Use the `no` form of this command to remove the DHCP range.

Command Syntax

```
dhcp-range A.B.C.D A.B.C.D
no dhcp-range
```

Parameters

`A.B.C.D`	Starting and ending IP address of the DHCP range

Default

NA.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#dhcp-range 10.12.65.2 10.12.65.12
```

disk-image

Use this command to configure the disk image location for the VM template.

Command Syntax

```
disk-image DISK-IMAGE-LOCATION
```

Parameters

`DISK-IMAGE-LOCATION`

Location of the disk image to boot up the VM.

Default

NA.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#disk-image \sample_location
```


© 2021 IP Infusion Inc. Proprietary

feature guest-vm

Use this command to enable the guest VM feature.

Use the `no` form of this command to disable the guest VM feature.

Command Syntax

```
feature guest-vm enable
no feature guest-vm enable
```

Parameters

None

Default

NA

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#feature guest-vm enable
```

gateway-ip

Use this command to set the gateway IP address for a virtual machine bridge.

Use the `no` form of this command to remove a gateway IP address.

Command Syntax

```
gateway-ip (A.B.C.D A.B.C.D | A.B.C.D/M)
no gateway-ip
```

Parameters

`A.B.C.D A.B.C.D`	Gateway IP address and subnet mask
`A.B.C.D/M`	Gateway IP address and subnet mask

Default

NA.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#gateway-ip 10.12.65.1/24
```


© 2021 IP Infusion Inc. Proprietary

host-core-affinity

Use this command to set the core affinity value for a virtual machine template.

Use the `no` form of this command to set the core affinity value to its default.

Command Syntax

```
host-core-affinity AFFINITY-VALUE
no host-core-affinity
```

Parameters

`AFFINITY-VALUE` The core affinity values between 0 and 7.

Default

Default value is 0.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#host-core-affinity 6
```

iptables

Use this command to create a rule for the IP tables.

Use the `no` form of this command to remove an IP tables rule.

Command Syntax

```
iptables STRING (position POS_NUM |)
no iptables STRING
```

Parameters

`STRING`	Rule string in double quotes.
`POS_NUM`	Position to insert the rule string <1-65535>.

Default

NA.

Command Mode

IP tables mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#iptables-template sample_template
(config-iptables)#iptables "INPUT DROP" position 65535
```


© 2021 IP Infusion Inc. Proprietary

iptables restore

Use this command to restore the entries in the IP tables template to the IP tables.

Use the `no` form of this command to remove the entries in the IP tables.

Command Syntax

```
iptables restore iptables-template TEMPLATE_NAME (vrf VRF-NAME |)
no iptables restore (iptables-template TEMPLATE_NAME |) (vrf VRF-NAME |)
```

Parameters

`TEMPLATE-NAME`	Name of the IP tables template
`VRF-NAME`	Name of the VRF

Default

NA.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#iptables restore iptables-template sample_template vrf VRF1
```

iptables-template

Use this command to create an IP tables template and enter IP tables mode.

Use the `no` form of this command to remove an IP tables template.

Command Syntax

```
iptables-template TEMPLATE_NAME
no iptables-template TEMPLATE_NAME
```

Parameters

`TEMPLATE_NAME`	Name of the IP tables template.

Default

NA.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#iptables-template sample_template
(config-iptables)
```


© 2021 IP Infusion Inc. Proprietary

memory

Use this command to configure the RAM size for the VM template.

Command Syntax

```
memory <128-8192>
```

Parameters

<128-8192>	Memory for Virtual Machine in MB

Default

Default value is 0.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#memory 1024
```

nat dnat

Use this command to set destination NAT addresses in the IP tables.

Use the `no` form of this command to remove the destination NAT addresses.

Command Syntax

```
nat dnat match-ip A.B.C.D to A.B.C.D (protocol (tcp | udp)|) (sport-num <0-65535>
  |) (dport-num <0-65535> |) (vrf VRF-NAME|)
no nat dnat match-ip A.B.C.D to A.B.C.D (protocol (tcp | udp)|) (sport-num <0-
  65535> |) (dport-num <0-65535> |) (vrf VRF-NAME|)
```

Parameters

`A.B.C.D`	From IP address
`A.B.C.D`	To IP address
`tcp`	Use TCP for NAT
`udp`	Use UDP for NAT
`sport-num`	Source port
`<0-65535>`	Source port number
`dport-num`	Destination port
`<0-65535>`	Destination port number
`VRF-NAME`	VRF Name

Default

NA.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nat dnat match-ip 1.1.1.1 to 1.1.1.2 protocol tcp
```


© 2021 IP Infusion Inc. Proprietary

nat snat

Use this command to set the source NAT addresses in the IP tables.

Use the `no` form of this command to remove the source NAT addresses.

Command Syntax

```
nat snat from A.B.C.D/M to A.B.C.D (vrf VRF-NAME|)
no nat snat from A.B.C.D/M to A.B.C.D (vrf VRF-NAME|)
```

Parameters

`A.B.C.D/M`	From IP address and subnet mask
`A.B.C.D`	To IP address
`VRF-NAME`	VRF Name

Default

NA.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#nat snat from 10.12.65.1 to 10.12.65.102 vrf VRF1
```

os-type

Use this command to configure the Operating System type of Virtual Machine.

Command Syntax

```
os-type (xen|linux|hvm|exe|uml)
```

Parameters

`xen`	Xen
`linux`	Linux
`hvm`	HVM
`exe`	Exe
`uml`	UML

Default

NA

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#os-type linux
```


© 2021 IP Infusion Inc. Proprietary

os-variant

Use this command to set the operating system variant for a virtual machine template.

Use the `no` form of this command to remove the operating system variant.

Command Syntax

```
os-variant (generic|fedora|rhel|ubuntu|debian)
no os-variant (generic|fedora|rhel|ubuntu|debian)
```

Parameters

`generic`	Generic
`fedora`	Fedora
`rhel`	Red Hat Linux
`ubuntu`	Ubuntu
`debian`	Debian

Default

NA.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#os-variant debian
```

reload vm-name

Use this command to reload a running VM with a new template configuration.

Command Syntax

```
reload vm-name VM_NAME vm-template TEMPLATE_NAME
```

Parameters

VM-NAME	Name of the VM.
TEMPLATE-NAME	Name of the VM template.

Default

NA.

Command Mode

Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

#reload vm-name new vm-template sample

© 2021 IP Infusion Inc. Proprietary

secondary-disk-image

Use this command to configure the secondary disk image location for the VM template.

Command Syntax

```
secondary-disk-image SECONDARY-DISK-IMAGE-LOCATION
no secondary-disk-image
```

Parameters

SECONDARY-DISK-IMAGE-LOCATION

Location of the secondary disk image to boot up the VM.

Default

NA.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#secondary-disk-image \sample_location
```

service dns-masq

Use this command to start the DHCP service in the virtual machne.

Use the `no` form of this command to stop the DHCP service.

Command Syntax

```
service dns-masq
no service dns-masq
```

Parameters

None

Default

NA.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#service dns-masq
```


© 2021 IP Infusion Inc. Proprietary

show vm

Use this command to display the status of the virtual machine.

Command Syntax

```
show vm (details |) (VM_NAME |)
```

Parameters

`details`	Details
`VM_NAME`	Name of the virtual machine

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm
```

show vm-bridge

Use this command to display the bridge configuration.

Command Syntax

```
show vm-bridge (vrf VRF-NAME|)
```

Parameters

VRF-NAME	Name of the VRF

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm-bridge
```


© 2021 IP Infusion Inc. Proprietary

show vm-iptables

Use this command to display the IP tables.

Command Syntax

```
show vm-iptables (TEMPLATE_NAME | restored-iptables |)
```

Parameters

`TEMPLATE_NAME` Name of the IP tables template

`restored-iptables`
Restored IP tables

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm-iptables
```

show vm-iptables kernel

Use this command to display the kernel IP tables.

Command Syntax

```
show vm-iptables kernel (vrf VRF-NAME|)
```

Parameters

VRF-NAME	Name of the VRF

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm-iptables kernel
```


© 2021 IP Infusion Inc. Proprietary

show vm-nat details

Use this command to display virtual machine NAT details.

Command Syntax

```
show vm-nat details (vrf VRF-NAME|)
```

Parameters

VRF-NAME	Name of the VRF

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm-nat details
```

show vm-template

Use this command to display the status of the virtual machine template.

Command Syntax

```
show vm-template (VM-TEMP-NAME |)
```

Parameters

VM-TEMP-NAME	Name of the virtual machine template

Default

NA.

Command Mode

Exec and Privileged Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show vm-template
```


© 2021 IP Infusion Inc. Proprietary

start vm-name

Use this command to create a virtual machine (VM) based on the template configuration.

Use the `no` form of this command to end a running VM.

Command Syntax

```
start vm-name VM_NAME vm-template TEMPLATE_NAME
no start vm-name VM_NAME
```

Parameters

`VM-NAME`	Name of the VM
`TEMPLATE-NAME`	Name of the VM template

Default

NA

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)# start vm-name new vm-template sample
(config)# exit

#configure terminal
(config)# no start vm-name new
(config)# exit
```

static-bind

Use this command to bind an IP address to a MAC address for the virtual machine.

Use the `no` form of this command to unbind an IP address from a MAC address.

Command Syntax

```
static-bind vm-mac-address XXXX.XXXX.XXXX ip-address A.B.C.D
no static-bind vm-mac-address XXXX.XXXX.XXXX ip-address A.B.C.D
```

Parameters

`XXXX.XXXX.XXXX`	MAC Address
`A.B.C.D`	IP Address

Default

NA.

Command Mode

Virtual machine bridge mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)#static-bind vm-mac-address ABCD.HHHH.EFGH.HHHH ip-address
10.12.65.102
```


© 2021 IP Infusion Inc. Proprietary

stop vm-name

Use this command to stop arunning VM.

Command Syntax

```
stop vm-name VM_NAME
```

Parameters

VM-NAME	Name of the VM.

Default

NA

Command Mode

Exec Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#stop vm-name new
```

vcpu count

Use this command to configure the virtual CPU count for the VM template.

Command Syntax

```
vcpu count <1-16>
```

Parameters

<1-16>	Virtual CPU count

Default

Default value is 0.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#vcpu count 16
```


© 2021 IP Infusion Inc. Proprietary

virt-type

Use this command to set the virt-type as KVM or QEMU.

Command Syntax

```
virt-type (KVM | QEMU)
```

Parameters

KVM	Give VM
VQEMU	Give QEMU

Default

NA.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.5.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#virt-type kvm
(config-vm-temp)#virt-type qemu
```

virtual-nic

Use this command to set the MAC address of a virtual machine template.

Use the `no` form of this command to remove the MAC address.

Command Syntax

```
virtual-nic (vm-mac-addr XXXX.XXXX.XXXX|)(vrf VRF-NAME|)
no virtual-nic (vrf VRF-NAME|)
```

Parameters

`XXXX.XXXX.XXXX`	MAC address of the VM
`VRF-NAME`	VRF Name

Default

NA.

Command Mode

Virtual machine template mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#virtual-nic vm-mac-address ABCD.HHHH.EFGH.HHHH vrf VRF1
```


© 2021 IP Infusion Inc. Proprietary

vm-bridge-create

Use this command to create a virtual machine bridge and enter virtual machine bridge mode.

Use the `no` form of this command to remove a virtual machine bridge.

Command Syntax

```
vm-bridge-create VM-BRIDGE-NAME
no vm-bridge-create VM-BRIDGE-NAME
```

Parameters

`VM-BRIDGE-NAME` Name of the VM bridge.

Default

NA.

Command Mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf VRF1
(config-vrf)#vm-bridge-create Bridge1
(config-vrf-vm-bridge)
```

vm-image delete

Use this command to delete a virtual machine image.

Command Syntax

```
vm-image delete VM_IMAGE_LOCATION
```

Parameters

VM_IMAGE_LOCATION

Location of the virtual machine image.

Default

NA.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-image delete \sample_location
```


© 2021 IP Infusion Inc. Proprietary

vm-template

Use this command to create a virtual machine template and enter VM template mode.

Use the `no` form of this command to remove a virtual machine template.

Command Syntax

```
vm-template TEMPLATE_NAME
no vm-template TEMPLATE_NAME
```

Parameters

`TEMPLATE_NAME` Name of the VM template.

Default

NA.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vm-template sample
(config-vm-temp)#
```

© 2021 IP Infusion Inc. Proprietary

SECTION 15 Multi-Protocol Label Switching

Multi-Protocol Label Switching Configuration Guide

Contents

This document contains these chapters and appendices:

- Chapter 1, *Understanding Label Space*
- Chapter 2, *Understanding MPLS TTL Processing*
- Chapter 3, *Virtual Private Wire Service Configuration*
- Chapter 4, *LDP Configuration*
- Chapter 5, *LDP Inter-Area Configuration*
- Chapter 6, *MPLS LDP-IGP Synchronization*
- Chapter 7, *MPLS Statistics Configuration*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 Understanding Label Space

This chapter contains configurations for Label Space. It also provides an overview of Label Space concepts.

Overview

The Label space refers to the scope of labels in a given LSR. It determines assignment and distribution of labels to a given peer. During data flow, it decides the key for looking up MPLS table and takes appropriate action based on the entry. Label space is designated either as platform label space or per-interface label space.

Per-platform label space

In this implementation, a label must be unique for the entire platform. A label will be interpreted the same way at all the interfaces. The FIB entry in the router does not contain incoming interface related information. Thus the incoming traffic will be matched only with the label.

Per-interface label space

In this implementation, a label must be unique for a given input interface. A label will be interpreted Uniquely at different interface which allows us to re-use label for different entries. The FIB entry in router must contain incoming interface information along with label. Thus the incoming traffic will be matched with label and incoming interface.

Topology

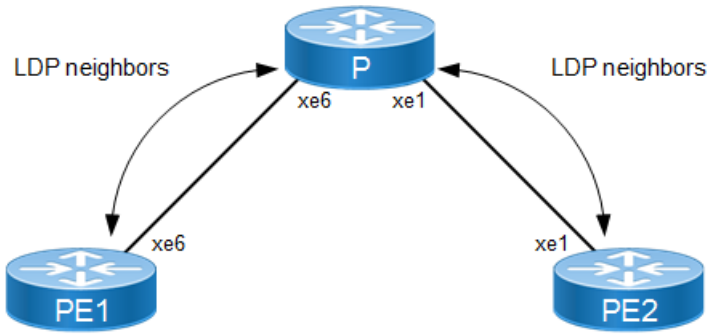


Figure 1-80: LDP Topology

Configuration

Per-Platform Label Space

PE1

`PE1#configure terminal`	Enter configure mode
`PE1(config)#interface lo`	Enter interface mode.

`PE1(config-if)#ip address 1.1.1.1/32`	Configure IP address for the loopback address
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#interface xe6`	Specify the interface `(xe6)` to be configured
`PE1(config-if)#ip address 10.10.10.1/24`	Configure IP address for the interface
`PE1(config-if)#no shutdown`	Administratively bringing up the interface
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)
`PE1(config-router)#network 10.10.10.0/24 area 0` `PE1(config-router)#network 1.1.1.1/32 area 0`	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface
`PE1(config-router)#exit`	Exit configure mode
`PE1(config)#router ldp`	Enter router mode for LDP
`PE1(config-router)#exit`	Exit router mode for LDP
`PE1(config)#interface xe6`	Specify the interface (xe6)to be configured
`PE1(config-if)#label-switching`	Enabling label switching capability on router
`PE1(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#exit`	Exit configure mode

P

`P#configure terminal`	Enter configure mode.
`P(config)#interface lo`	Enter interface mode.
`P(config-if)#ip address 2.2.2.2/32`	Configure IP address for the loopback address
`P(config-if)#exit`	Exit interface mode
`P(config)#interface xe6`	Specify the interface `(xe6)` to be configured
`P(config-if)#ip address 10.10.10.2/24`	Configure IP address for the interface
`P(config-if)#no shutdown`	Administratively bringing up the interface
`P(config)#interface xe1`	Specify the interface `(xe1)` to be configured
`P(config-if)#ip address 20.20.20.1/24`	Configure IP address for the interface
`P(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)

`P(config-router)#network 10.10.10.0/24 area 0`
`P(config-router)#network 20.20.20.0/24 area 0`
`P(config-router)#network 2.2.2.2/32 area 0`
	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface

`P(config-router)#exit`	Exit router mode
`P(config)#router ldp`	Enter router mode for LDP
`P(config-router)#exit`	Exit router mode for LDP
`P(config)#mpls min-label-value 1000 max-label-value 50000 label-space 0`	Configure the minimum label value and maximum label value to be used by Platform label space (Label space 0)
`P(config)#interface xe6`	Specify the interface (xe6)to be configured

© 2021 IP Infusion Inc. Proprietary

P(config-if)#label-switching	Enabling label switching capability on router
P(config-if)#enable-ldp ipv4	Enabling ldp on interface
P(config-if)#exit	Exit interface mode
P(config)#interface xe1	Specify the interface (xe1)to be configured
P(config-if)#label-switching	Enabling label switching capability on router
P(config-if)#enable-ldp ipv4	Enabling ldp on interface
P(config-if)#exit	Exit interface mode
P(config)#exit	Exit configure mode

PE2

PE2#configure terminal	Enter configure mode.
PE2(config)#interface lo	Enter interface mode.
PE2(config-if)#ip address 3.3.3.3/32	Configure IP address for the loopback address
PE2(config-if)#exit	Exit interface mode
PE2(config)#interface xe1	Specify the interface (xe1) to be configured
PE2(config-if)#ip address 20.20.20.2/24	Configure IP address for the interface
PE2(config-if)#no shutdown	Administratively bringing up the interface
PE2(config-if)#exit	Exit interface mode
PE2(config)#router ospf 100	Configure the routing process and specify the Process ID (100)
PE2(config-router)#network 20.20.20.0/24 area 0 PE2(config-router)#network 3.3.3.3/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface
PE2(config-router)#exit	Exit router mode
PE2(config)#router ldp	Enter router mode for LDP
PE2(config-router)#exit	Exit router mode for LDP
PE2(config)#interface xe1	Specify the interface (xe1)to be configured
PE2(config-if)#label-switching	Enabling label switching capability on router
PE2(config-if)#enable-ldp ipv4	Enabling ldp on interface
PE2(config-if)#exit	Exit interface mode

Validation

```
P#sh ldp
Router ID                : 2.2.2.2
LDP Version              : 1
Global Merge Capability  : Merge Capable
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode     : Liberal
Label Control Mode       : Independent
Instance Loop Detection  : Off
Request Retry            : Off
Propagate Release        : Disabled
```

```
Graceful Restart         : Disabled
Hello Interval           : 5
Targeted Hello Interval  : 15
Hold time                : 15
Targeted Hold time       : 45
Keepalive Interval       : 10
Keepalive Timeout        : 30
Request retry Timeout    : 5
Transport Address data   :
  Labelspace 0           : 2.2.2.2 (in use)
Import BGP routes        : No

P#show mpls label-space 0
 Min-label-value : 1000
 Max-label-value : 50000

 module-static   min-label-value  : 1000
                 max-label-value  : 15999
 module-srgb     min-label-value  : 16000
                 max-label-value  : 24319
 module-rsvp     min-label-value  : 0
                 max-label-value  : 0
 module-ldp      min-label-value  : 0
                 max-label-value  : 0
 module-bgp      min-label-value  : 0
                 max-label-value  : 0
 module-ospf     min-label-value  : 0
                 max-label-value  : 0
P#sh mpls ilm-table
Codes: > - selected ILM, p - stale ILM, K - CLI ILM, T - MPLS-TP

Code  FEC                ILM-ID      In-Label    Out-Label   In-Intf   Out-Intf
Nexthop                      LSP-Type
  >   1.1.1.1/32          1           3840         3          N/A      eth1
172.168.25.56                LSP_DEFAULT
  >   3.3.3.3/32          2           3841         3          N/A      eth2
10.10.20.51                  LSP_DEFAULT
```

Per-Interface Label Space

PE1

`PE1#configure terminal`	Enter configure mode
`PE1(config)#interface lo`	Enter interface mode.
`PE1(config-if)#ip address 1.1.1.1/32`	Configure IP address for the loopback address
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#interface xe6`	Specify the interface `(xe6)` to be configured
`PE1(config-if)#ip address 10.10.10.1/24`	Configure IP address for the interface

 © 2021 IP Infusion Inc. Proprietary

PE1(config-if)#no shutdown	Administratively bringing up the interface
PE1(config-if)#exit	Exit interface mode
PE1(config)#router ospf 100	Configure the routing process and specify the Process ID (100)
PE1(config-router)#network 10.10.10.0/24 area 0 PE1(config-router)#network 1.1.1.1/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface
PE1(config-router)#exit	Exit configure mode
PE1(config)#router ldp	Enter router mode for LDP
PE1(config-router)#exit	Exit router mode for LDP
PE1(config)#mpls min-label-value 60000 max-label-value 80000 label-space 1	Configure the minimum label value and maximum label value to be used by interface label space (Label space 1 in this case)
PE1(config)#interface xe6	Specify the interface (xe6)to be configured
PE1(config-if)#label-switching	Enabling label switching capability on router
PE1(config-if)#enable-ldp ipv4	Enabling ldp on interface
PE1(config-if)#exit	Exit interface mode
PE1(config)#exit	Exit configure mode

P

P#configure terminal	Enter configure mode.
P(config)#interface lo	Enter interface mode.
P(config-if)#ip address 2.2.2.2/32	Configure IP address for the loopback address
P(config-if)#exit	Exit interface mode
P(config)#interface xe6	Specify the interface (xe6) to be configured
P(config-if)#ip address 10.10.10.2/24	Configure IP address for the interface
P(config-if)#no shutdown	Administratively bringing up the interface
P(config)#interface xe1	Specify the interface (xe1) to be configured
P(config-if)#ip address 20.20.20.1/24	Configure IP address for the interface
P(config)#router ospf 100	Configure the routing process and specify the Process ID (100)
P(config-router)#network 10.10.10.0/24 area 0 P(config-router)#network 20.20.20.0/24 area 0 P(config-router)#network 2.2.2.2/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface
P(config-router)#exit	Exit router mode
P(config)#router ldp	Enter router mode for LDP
P(config-router)#exit	Exit router mode for LDP
P(config)#mpls min-label-value 60000 max-label-value 80000 label-space 1	Configure the minimum label value and maximum label value to be used by Interface label space (Label space 1)
P(config)#interface xe6	Specify the interface (xe6)to be configured
P(config-if)#label-switching 1	Enabling label switching capability on router

`P(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`P(config)#interface xe1`	Specify the interface (xe1)to be configured
`P(config-if)#label-switching 1`	Enabling label switching capability on router
`P(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`P(config-if)#exit`	Exit interface mode
`P(config)#exit`	Exit configure mode

PE2

`PE2#configure terminal`	Enter configure mode.
`PE2(config)#interface lo`	Enter interface mode.
`PE2(config-if)#ip address 3.3.3.3/32`	Configure IP address for the loopback address
`PE2(config-if)#exit`	Exit interface mode
`PE2(config)#interface xe1`	Specify the interface `(xe1)` to be configured
`PE2(config-if)#ip address 20.20.20.2/24`	Configure IP address for the interface
`PE2(config-if)#no shutdown`	Administratively bringing up the interface
`PE2(config-if)#exit`	Exit interface mode
`PE2(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)
`PE2(config-router)#network 20.20.20.0/24 area 0` `PE2(config-router)#network 3.3.3.3/32 area 0`	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface
`PE2(config-router)#exit`	Exit router mode
`PE2(config)#router ldp`	Enter router mode for LDP
`PE2(config-router)#exit`	Exit router mode for LDP
`PE2(config)#mpls min-label-value 60000 max-label-value 80000 label-space 1`	Configure the minimum label value and maximum label value to be used by interface label space (Label space 1)
`PE2(config)#interface xe1`	Specify the interface (xe1)to be configured
`PE2(config-if)#label-switching`	Enabling label switching capability on router
`PE2(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`PE2(config-if)#exit`	Exit interface mode

Validation

```
P#show ldp

Router ID                : 2.2.2.2
LDP Version              : 1
Global Merge Capability  : Merge Capable
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode     : Liberal
Label Control Mode       : Independent
Instance Loop Detection  : Off
```


© 2021 IP Infusion Inc. Proprietary

```
Request Retry            : Off
Propagate Release        : Disabled
Graceful Restart         : Disabled
Hello Interval           : 5
Targeted Hello Interval  : 15
Hold time                : 15
Targeted Hold time       : 45
Keepalive Interval       : 10
Keepalive Timeout        : 30
Request retry Timeout    : 5
Transport Address data   :
  Labelspace 1           : 2.2.2.2 (in use)
Import BGP routes        : No

P#show mpls label-space 1
 Min-label-value : 60000
 Max-label-value : 80000

 module-static   min-label-value  : 60000
                 max-label-value  : 61000
 module-rsvp     min-label-value  : 0
                 max-label-value  : 0
 module-ldp      min-label-value  : 0
                 max-label-value  : 0
 module-bgp      min-label-value  : 0
                 max-label-value  : 0
 module-ospf     min-label-value  : 0
                 max-label-value  : 0
P#sh mpls ilm
Codes: > - selected ILM, p - stale ILM, K - CLI ILM, T - MPLS-TP

Code  FEC                ILM-ID      In-Label    Out-Label   In-Intf   Out-Intf
Nexthop                      LSP-Type
  >   3.3.3.3/32          3           61441        3          eth1     eth2
10.10.20.51                   LSP_DEFAULT
  >   1.1.1.1/32          4           61440        3          eth2     eth1
172.168.25.56                 LSP_DEFAULT
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Understanding MPLS TTL Processing

This chapter contains configurations for MPLS-TTL-Processing. It also provides an overview of MPLS-TTL-Processing concepts.

Overview

This feature performs 'Time To Live' (TTL) processing for Multi-Protocol Label Switching (MPLS) packets. The TTL processing is decided by the model chosen by you. This feature provides TTL processing of MPLS packets on ingress, egress, and intermediate routers. TTL processing is compliant with RFC 3443.

The details of TTL processing vary with the tunnel model that is configured for TTL processing. The incoming and outgoing TTL of the packet is determined by the configured tunnel model. Two Models are supported, pipe model and uniform model. Pipe model is default model, where MPLS header TTL Value wont get propagated to IP header.

To know more about uniform model and pipe model, refer chapter MPLS DiffServ Configuration.

Topology

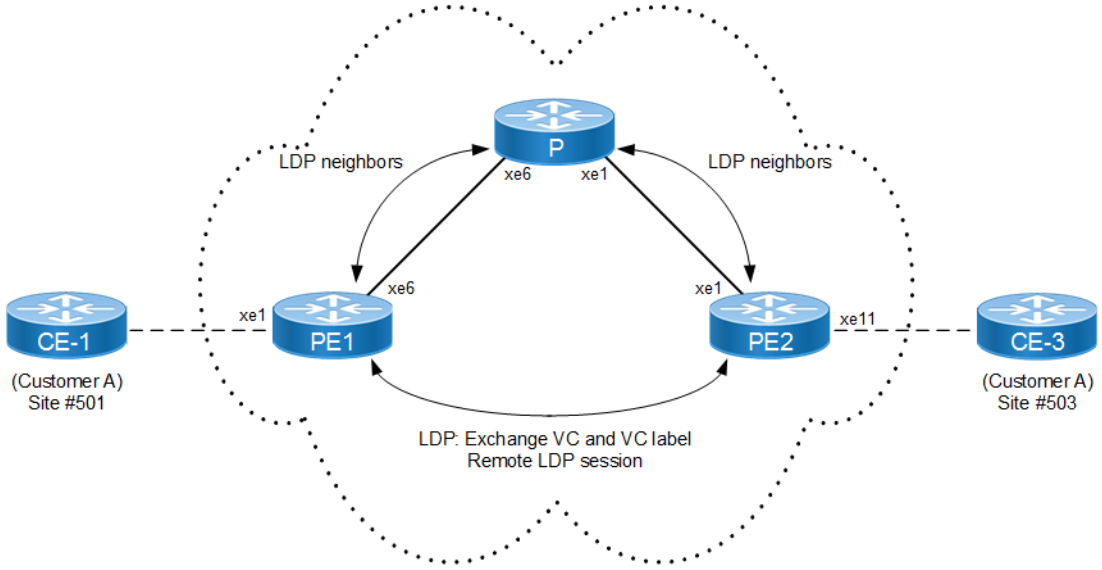


Figure 2-81: TTL Processing Topology

Configuration

PE1

`PE1#configure terminal`	Enter configure mode
`PE1(config)#interface lo`	Enter interface mode.
`PE1(config-if)#ip address 1.1.1.1/32`	Configure IP address for the loopback address
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#mpls lsp-model pipe`	Configure Lsp-Model as Pipe
`PE1(config)#interface xe6`	Specify the interface `(xe6)` to be configured

© 2021 IP Infusion Inc. Proprietary

`PE1(config-if)#ip address 10.10.10.1/24`	Configure IP address for the interface
`PE1(config-if)#no shutdown`	Administratively bringing up the interface
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)
`PE1(config-router)#network 10.10.10.0/24 area 0` `PE1(config-router)#network 1.1.1.1/32 area 0`	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface
`PE1(config-router)#exit`	Exit configure mode
`PE1(config)#router ldp`	Enter router mode for LDP
`PE1(config-router)#exit`	Exit router mode for LDP
`PE1(config)#interface xe6`	Specify the interface (xe6)to be configured
`PE1(config-if)#label-switching`	Enabling label switching capability on router
`PE1(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#exit`	Exit configure mode

P

`P#configure terminal`	Enter configure mode.
`P(config)#interface lo`	Enter interface mode.
`P(config-if)#ip address 2.2.2.2/32`	Configure IP address for the loopback address
`P(config-if)#exit`	Exit interface mode
`P(config)#interface xe6`	Specify the interface `(xe6)` to be configured
`P(config-if)#ip address 10.10.10.2/24`	Configure IP address for the interface
`P(config-if)#no shutdown`	Administratively bringing up the interface
`P(config)#interface xe1`	Specify the interface `(xe1)` to be configured
`P(config-if)#ip address 20.20.20.1/24`	Configure IP address for the interface
`P(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)

`P(config-router)#network 10.10.10.0/24 area 0`
`P(config-router)#network 20.20.20.0/24 area 0`
`P(config-router)#network 2.2.2.2/32 area 0`
	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface

`P(config-router)#exit`	Exit router mode
`P(config)#router ldp`	Enter router mode for LDP
`P(config-router)#exit`	Exit router mode for LDP
`P(config)#interface xe6`	Specify the interface (xe6)to be configured
`P(config-if)#label-switching`	Enabling label switching capability on router
`P(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`P(config)#interface xe1`	Specify the interface (xe1)to be configured
`P(config-if)#label-switching`	Enabling label switching capability on router
`P(config-if)#enable-ldp ipv4`	Enabling ldp on interface

© 2021 IP Infusion Inc. Proprietary

`P(config-if)#exit`	Exit interface mode
`P(config)#exit`	Exit configure mode

PE2

`PE2#configure terminal`	Enter configure mode.
`PE2(config)#interface lo`	Enter interface mode.
`PE2(config-if)#ip address 3.3.3.3/32`	Configure IP address for the loopback address
`PE2(config-if)#exit`	Exit interface mode
`PE2(config)#interface xe1`	Specify the interface `(xe1)` to be configured
`PE2(config-if)#ip address 20.20.20.2/24`	Configure IP address for the interface
`PE2(config-if)#no shutdown`	Administratively bringing up the interface
`PE2(config-if)#exit`	Exit interface mode
`PE2(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)
`PE2(config-router)#network 20.20.20.0/24 area 0` `PE2(config-router)#network 3.3.3.3/32 area 0`	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface
`PE2(config)#router ldp`	Enter router mode for LDP
`PE2(config-router)#exit`	Exit router mode for LDP
`PE2(config)#interface xe1`	Specify the interface (xe1)to be configured
`PE2(config-if)#label-switching`	Enabling label switching capability on router
`PE2(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`PE2(config-if)#exit`	Exit interface mode

© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 LDP Configuration

This chapter contains LDP (Label Distribution Protocol) configuration examples.

Label Distribution Protocol Overview

The Label Distribution Protocol (LDP) is a routing protocol used in MPLS technology. The LDP daemon (`ldpd`) uses NSM services to obtain routing information. Routers send Hello packets to establish Hello Adjacencies with other nearby routers. This opens the way for sessions between routers to be established during which routers exchange labels in preparation for forwarding packets.

LDP generates labels for and exchanges labels between peer routers. It works in with other routing protocols (RIP, OSPF and BGP) to create label-switched paths (LSP) used when forwarding packets. A label-switched path is the path taken by all packets that belong to the Forwarding Equivalence Class (FEC) corresponding to that LSP. This is analogous to establishing a virtual circuit in ATM (Asynchronous Transfer Mechanism). In this way, OcNOS LDP assigns labels to every destination address and destination prefix provided by OcNOS. The LDP interface to the MPLS forwarder adds labels to, and deletes labels from, the forwarding tables.

LDP Adjacencies

LDP defines a mechanism for discovering adjacent, LDP capable Label Switching Routers (LSR) that participate in label switching (adjacencies). Whenever a new router comes up it sends out a hello packet to a specified, multicast address announcing itself to the network. Every router directly connected to the network receives the packet. Receipt of a hello packet from another LSR creates a *Hello Adjacency* with that LSR. To create a Hello Adjacency with an LSR that cannot send/receive multicast packets, LDP allows a router to be manually configured to send unicast Hello packets to non-multicast LSRs . This non-multicast LSR is a *targeted peer*. Adjacencies are maintained by sending out periodic Hello packets to the multicast group and to all targeted peers. Hello packets are sent using UDP.

LDP Session

LDP capable LSRs establish a session before exchanging label information. All the session messages are sent using TCP to ensure reliable delivery. After the LSRs establish a session and negotiate options, a given pair of routers may exchange label information. The labels exchanged over a session are valid only during the lifetime of the session and routers release them when session is closed.

Forwarding Equivalence Class

A Forwarding Equivalence Class (FEC) section defines a set of packets that are forwarded on the same path by the MPLS network. Two common methods to define FEC are by advertising the IPv4 routes using:

- **Host Address** The LSR uses the address of the destination host to create this FEC. This means that all the packets going to this destination will take the same LSP.
- **Prefix** The LSR uses destination prefix to create this FEC. This means that all the packets take the LSP corresponding to the longest matching prefix.

Label Generation

An LDP Label is a 20-bit number the LSR uses to forward a packet to its destination. When an LSR creates a new FEC, the router generates new labels and distributes them to its peers. A router keeps both incoming and outgoing labels in its database.

Label Distribution Modes

The OcNOS LDP implementation supports two label distribution modes:

- **Downstream Unsolicited** In this mode, next hop LSRs distribute labels to peers without waiting for a label request.
- **Downstream on Demand** In this mode, a LSR distributes a label to a peer only if there is a pending label request from the peer.

Label Retention Mode

The OcNOS LDP implementation supports two label retention modes:

- **Liberal Retention Mode** In this mode, the LSR retains all labels received from all sources. This mode helps in fast LSP setup in case of a change in next hop.
- **Conservative Retention Mode** In this mode, the LSR retains only those labels received from peers that are the next hop for a given FEC. This mode is used by LSRs that have a constraint on the number of labels that it can retain at any given time.

LSP Control

LSPs can be set up in the following two ways:

- **Ordered Control** In this mode, an LSR distributes a label for a FEC to its peer only if it has a corresponding label from its next hop or it is the egress node.
- **Independent Control** In this mode, an LSR may distribute a label to its peers without waiting for a corresponding label from its next hop.

Loop Detection

Loop detection can be enabled to detect routing loops in LSPs. There are two methods supported for the loop detection mechanism:

- **Hop Count** During setup of an LSP, the LSP passes hop count with the LSP setup messages. This hop count is incriminated by each node router participating in LSP establishment. If the hop count exceeds the maximum configured value, the LSP setup process is stopped and a notification message is passed back to the message originator.
- **Path Vector** A path vector contains a list of LSR identifiers. This is passed as a part of LSP setup messages. Each LSR participating in the LSP establishment adds its own LSR identifier to the path vector. If an LSR finds its own identifier in the path vector, it drops the message and sends a message back to the originator.

The use of these messages ensures that a loop is detected while establishing a label switched path and before any data is passed over that LSP.

Configure LDP

The `enable-ldp ipv4 and enable-ldp ipv6` command are used to enable LDP for IPv4 or LDP for IPv6, on a specified interface, as follows:

- `enable-ldp ipv4` enables only IPv4 on the interface
- `enable-ldp ipv6` enables only IPv6 on the interface

© 2021 IP Infusion Inc. Proprietary

For the examples covered in this section, the command `enable-ldp ipv4` is used.

Enable Label Switching

Running LDP on a system requires the following tasks:

1. Enabling label-switching on the interface on NSM.
2. Enabling LDP on an interface in the LDP daemon.
3. Running an IGP (Internal Gateway Protocol), for example, OSPF, to distribute reachability information within the MPLS cloud.
4. Configuring the transport address.

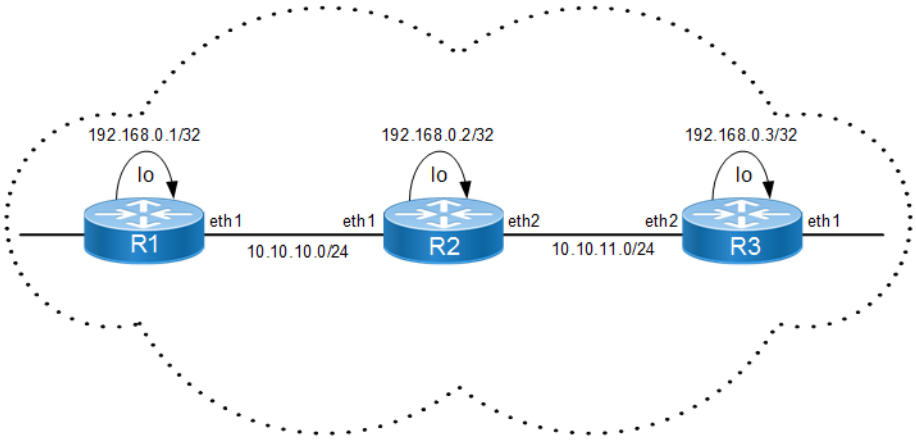


Figure 4-82: Basic LDP Topology

R1

NSM

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (`lo`) interface to be configured.
`(config-if)#ip address 192.168.0.1/32`	Set the IP address of the loopback interface to `192.168.0.1/32`.

LDP

`(config)#router ldp`	Enter `Router` mode for LDP.
`(config-router)#router-id 192.168.0.1`	Set the router ID to IP address `192.168.0.1`.
`(config-router)#transport-address ipv4 192.168.0.1`	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. **Note**: It is preferable to use the loopback address as transport address. In addition, use the parameter “ipv6” if you are configuring an IPv6 interface.

(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on eth1.
(config-if)#exit	Exit interface mode.

OSPF

(config)#router ospf 100	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 10.10.10.0/24 area 0 (config-router)#network 192.168.0.1/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.

R2

NSM

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the loopback (lo) interface to be configured.
(config-if)#ip address 192.168.0.2/32	Set the IP address of the loopback interface to 192.168.0.2/32.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#exit	Exit interface mode.

LDP

(config)#router ldp	Enter Router mode.
(config-router)#router-id 192.168.0.2	Set the router ID to IP address 192.168.0.2.
(config-router)#transport-address ipv4 192.168.0.2	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. **Note**: It is preferable to use the loopback address as transport address. In addition, use the parameter “ipv6” if you are configuring an IPv6 interface.
(config-router)#exit	Exit Router mode and return to Configure mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#enable-ldp ipv4	Enable LDP on a specified interface (eth1).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.

© 2021 IP Infusion Inc. Proprietary

(config-if)#enable-ldp ipv4	Enable LDP on a specified interface (eth2).
(config-if)#exit	Exit interface mode.

OSPF

(config)#router ospf 100	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 10.10.10.0/24 area 0 (config-router)#network 10.10.11.0/24 area 0 (config-router)#network 192.168.0.2/32 area 0	Define the interfaces on which OSPF runs and associate the area ID (0) with them.

R3

NSM

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the loopback (lo) interface to be configured.
(config-if)#ip address 192.168.0.3/32	Set the IP address of the loopback interface to 192.168.0.3/32.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#exit	Exit interface mode.

LDP

(config)#router ldp	Enter Router mode.
(config-router)#router-id 192.168.0.3	Set the router ID for IP address 192.168.0.3.
(config-router)#transport-address ipv4 192.168.0.3	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. **Note**: It is preferable to use the loopback address as transport address. In addition, use the parameter “ipv6” if you are configuring an IPv6 interface.
(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface eth2	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on eth2.
(config-if)#exit	Exit interface mode.

OSPF

`(config)#router ospf 100`	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.11.0/24 area 0` `(config-router)#network 192.168.0.3/32 area 0`	Define the interfaces on which OSPF runs and associate the area ID `(0)` with them.

LDP MD5 Authentication

LDP MD5 configuration enables LDP MD5 password authentication on a per-peer basis.

Direct LDP Session

In this example, MD5 authentication is configured for a direct LDP session.

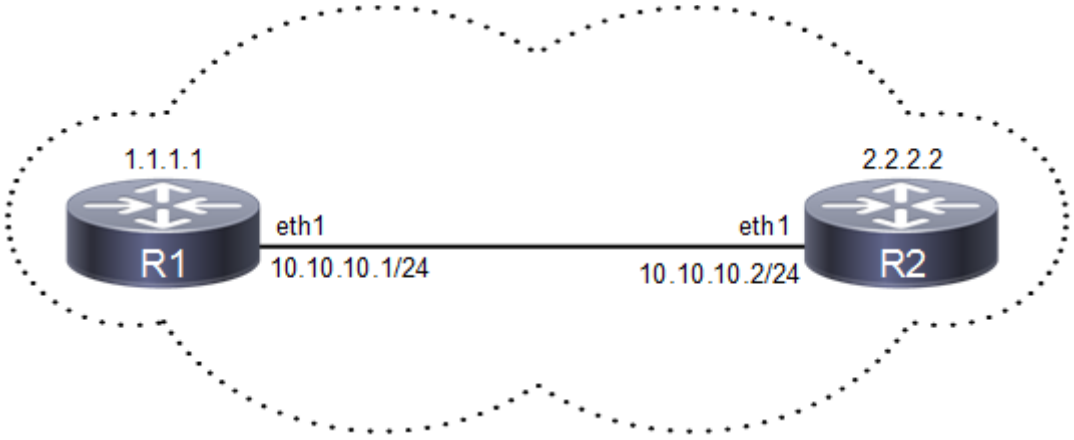


Figure 4-83: Topology for Direct Session MD5

R1

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter `Router` mode.
`(config-router)#neighbor 10.10.10.2 auth md5 password 0 pwd1`	Configure the MD5 authentication and password, `pwd1`, for the neighbor, `10.10.10.2`.
`(config-router)#exit`	Exit the `Router` mode and return to the `Configure` mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#enable-ldp ipv4`	Enable LDP on interface `eth1`.
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

R2

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter `Router` mode.
`(config-router)#neighbor 10.10.10.1 auth md5 password 0 pwd1`	Configure the MD5 authentication and password, `pwd1`, for the neighbor, `10.10.10.1`.
`(config-router)#exit`	Exit the `Router` mode and return to the `Configure` mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#enable-ldp ipv4`	Enable LDP on interface `eth1`.
`(config-if)#exit`	Exit interface mode.

Configure LDP MD5 for Targeted LDP Session

In this example, MD5 authentication is configured for the targeted LDP session established between R1 and R3.

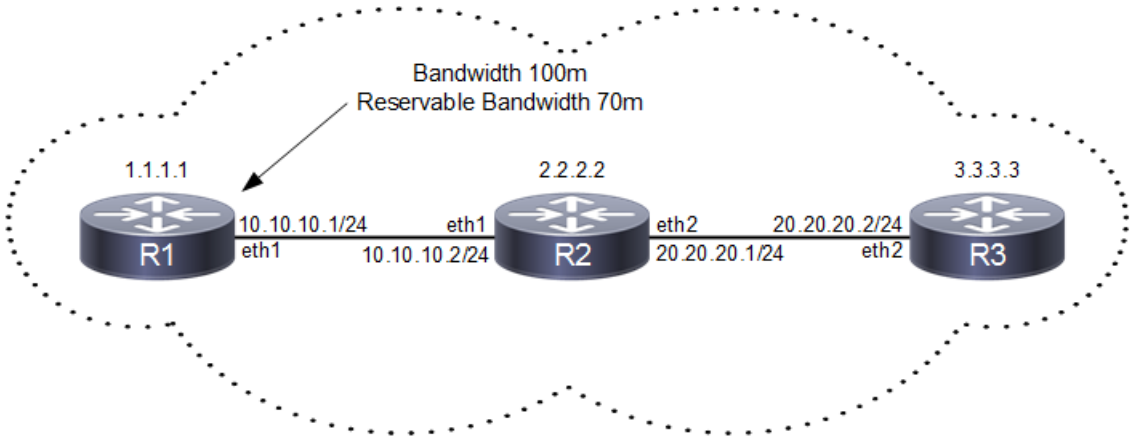


Figure 4-84: Topology for Targeted Session MD5

R1

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter `Router` mode.
`(config-router)#neighbor 10.10.10.2 auth md5 password 0 pwd1`	Configure the MD5 authentication and password, `pwd1`, for the neighbor, `10.10.10.2`.
`(config-router)#targeted-peer ipv4 3.3.3.3`	Configure the targeted peer IP address (R3 loopback address).
(config-router-targeted-peer)#exit	Exit targeted peer mode.
`(config-router)#neighbor 3.3.3.3 auth md5 password 0 pwd2`	Configure the MD5 authentication and password, `pwd2`, for the targeted peer, `3.3.3.3`.
`(config-router)#exit`	Exit the `Router` mode and return to the `Configure` mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.

(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#enable-ldp ipv4	Enable LDP on interface eth1.
(config-if)#exit	Exit interface mode.

R2

#configure terminal	Enter configure mode.
(config)#router ldp	Enter Router mode to enable LDP.
(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#enable-ldp ipv4	Enable LDP on interface eth1.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#enable-ldp ipv4	Enable LDP on interface eth2.
(config-if)#exit	Exit interface mode.

R3

#configure terminal	Enter configure mode.
(config)#router ldp	Enter Router mode.
(config-router)#targeted-peer ipv4 1.1.1.1	Configure the targeted peer IP address (R1 loopback address).
(config-router-targeted-peer)#exit	Exit targeted peer mode.
(config-router)#neighbor 1.1.1.1 auth md5 password 0 pwd2	Configure the MD5 authentication and password, pwd2, for the targeted peer, 1.1.1.1.
(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#enable-ldp ipv4	Enable LDP on interface eth1.
(config-if)#exit	Exit interface mode.

Removing MD5 Authentication for LDP Session

This example shows removing the MD5 authentication configuration from an LDP session.

© 2021 IP Infusion Inc. Proprietary

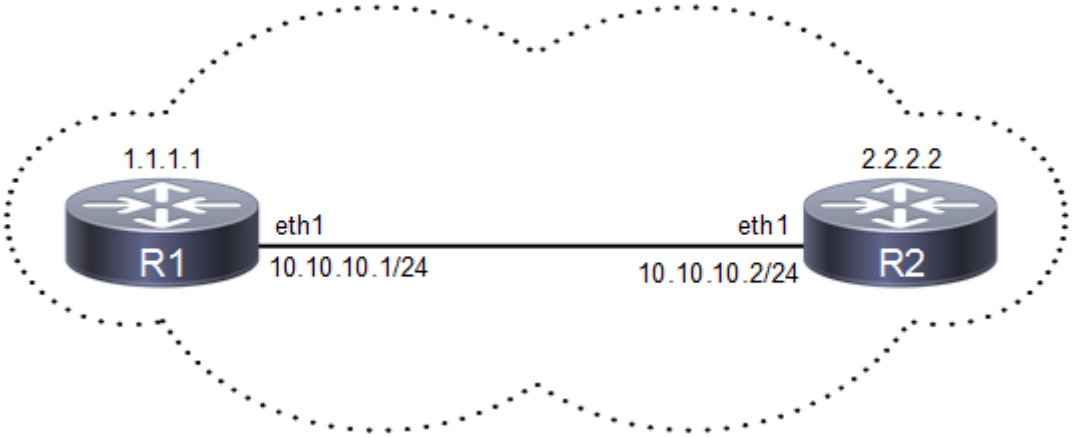


Figure 4-85: LDP Session Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter `Router` mode.
`(config-router)#no neighbor 10.10.10.2 auth md5 password 0`	Remove MD5 authentication for the neighbor, `10.10.10.2`.
`(config-router)#exit`	Exit the `Router` mode and return to the `Configure` mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter `Router` mode.
`(config-router)#no neighbor 10.10.10.1 auth md5 password 0`	Remove MD5 authentication for the neighbor, `10.10.10.1`.
`(config-router)#exit`	Exit the `Router` mode and return to the `Configure` mode.

Validation for LDP Session Count

This example shows the number of configured LDP basic neighbors and targeted neighbors count.

```
 #show ldp session count
 ------------------------------------------
 Multicast Peers      : 1          [UP: 1]
 Targeted Peers       : 1          [UP: 1]
 Total Sessions       : 2          [UP: 2]
------------------------------------------

 #show ldp targeted-peer count
 ------------------------------------------------
 Num Targeted Peers: 500          [UP: 500]
 ------------------------------------------------
```

Validation for FTN, SWAP, and POP Entries

This example shows forwarding table entries, SWAP entries and POP entries for IPV4 and IPV6 prefixes.

```
#show mpls forwarding-table count
-------------------------------------------
Num FTNs            : 3          [UP: 3, INSTALLED: 3]
Primary FTNs        : 3          [UP: 3, INSTALLED: 3]
Secondary FTNs      : 0          [UP: 0, INSTALLED: 0]
-------------------------------------------
-------------------------------------------
Num IPV6 FTNs       : 0          [UP: 0, INSTALLED: 0]
Primary IPV6 FTNs   : 0          [UP: 0, INSTALLED: 0]
Secondary IPV6 FTNs : 0          [UP: 0, INSTALLED: 0]
-------------------------------------------

#show mpls ilm-table count
-------------------------------------------
Num ILMs         : 0          [UP: 0, INSTALL: 0]
  Swap Entries   : 0          [UP: 0, INSTALL: 0]
  Pop Entries    : 0          [UP: 0, INSTALL: 0]
  VC Pop Entries : 0          [UP: 0]
-------------------------------------------
```

MPLS LDP PING and TRACEROUTE

This example shows MPLS ping and trace route for LDP

```
#show ip ospf neighbor
Total number of full neighbors: 1
OSPF process 0 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address
Interface           Instance ID
43.43.43.43       1   Full/DR         00:00:33    21.21.21.43
xe21                  0
RTR-29#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive
43.43.43.43               xe21       Passive   OPERATIONAL   30

#show mpls  forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type
Out-Label    Out-Intf    ELC   Nexthop
   L>   13.1.1.1/32         1         1         -           -     LSP_DEFAULT
3            xe13        No    20.20.20.12
   L>   20.1.1.1/32         2         2         -           -     LSP_DEFAULT
24320        xe13        No    20.20.20.12
   L>   20.20.20.10/31      3         1         -           -     LSP_DEFAULT
3            xe13        No    20.20.20.12
```


© 2021 IP Infusion Inc. Proprietary

```
#ping mpls ldp 43.43.43.43/32 detail
Sending 5 MPLS Echos to 43.43.43.43, timeout is 5 seconds

Codes:
'!' - Success, 'Q' - request not sent, '.' - timeout,
'x' - Retcode 0, 'M' - Malformed Request, 'm' - Errored TLV,
'N' - LBL Mapping Err, 'D' - DS Mismatch,
'U' - Unknown Interface, 'R' - Transit (LBL Switched),
'B' - IP Forwarded, 'F' No FEC Found, 'f' - FEC Mismatch,
'P' - Protocol Error, 'X' - Unknown code,
'Z' - Reverse FEC Validation Failed

Type 'Ctrl+C' to abort
! seq_num = 1 43.43.43.43 1.73 ms
! seq_num = 2 43.43.43.43 1.46 ms
! seq_num = 3 43.43.43.43 0.64 ms
! seq_num = 4 43.43.43.43 0.65 ms
! seq_num = 5 43.43.43.43 0.62 ms

Success Rate is 100.00 percent (5/5)
round-trip min/avg/max = 0.62/1.18/1.73

#trace mpls ldp 43.43.43.43/32 detail
Tracing MPLS Label Switched Path to 43.43.43.43, timeout is 5 seconds
Codes:
'!' - Success, 'Q' - request not sent, '.' - timeout,
'x' - Retcode 0, 'M' - Malformed Request, 'm' - Errored TLV,
'N' - LBL Mapping Err, 'D' - DS Mismatch,
'U' - Unknown Interface, 'R' - Transit (LBL Switched),
'B' - IP Forwarded, 'F' No FEC Found, 'f' - FEC Mismatch,
'P' - Protocol Error, 'X' - Unknown code,
'Z' - Reverse FEC Validation Failed
Type 'Ctrl+C' to abort
  0 21.21.21.29 [Labels:  0]
! 1 43.43.43.43 0.69 ms

#ping mpls ldp 43.43.43.43/32 detail interval 5000 rep
reply-mode  repeat
#ping mpls ldp 43.43.43.43/32 detail interval 5000 repeat 50
Sending 50 MPLS Echos to 43.43.43.43, timeout is 5 seconds

Codes:
'!' - Success, 'Q' - request not sent, '.' - timeout,
'x' - Retcode 0, 'M' - Malformed Request, 'm' - Errored TLV,
'N' - LBL Mapping Err, 'D' - DS Mismatch,
'U' - Unknown Interface, 'R' - Transit (LBL Switched),
'B' - IP Forwarded, 'F' No FEC Found, 'f' - FEC Mismatch,
'P' - Protocol Error, 'X' - Unknown code,
'Z' - Reverse FEC Validation Failed

Type 'Ctrl+C' to abort

! seq_num = 1 43.43.43.43 0.70 ms
! seq_num = 2 43.43.43.43 0.73 ms
! seq_num = 3 43.43.43.43 0.71 ms
Success Rate is 100.00 percent (3/3)
round-trip min/avg/max = 0.70/0.71/0.73
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 LDP Inter-Area Configuration

This chapter contains LDP inter-area configuration examples.

Overview

Provider-based MPLS (Multiprotocol Label Switching) networks are expanding with the success of Layer 3 Virtual Private Networks and the new deployments of Layer 2 VPNs. Service providers MPLS backbones are significantly growing both in terms of density with the addition of Provider Edge (PE) routers to connect new customers and in terms of footprint as traditional Layer 2 aggregation networks may be replaced by IP/MPLS networks. As a consequence, many providers need to introduce IGP areas. Inter-area LSPs (that is, LSPs that traverse at least two IGP areas) are required to ensure MPLS connectivity between PEs located in distinct IGP areas.

On a large MPLS networks, multiple IGP areas need to be configured for flexible network deployment and fast route convergence. When advertising routes between IGP areas, to prevent a large number of routes from consuming too many resources, an Area Border Router (ABR) needs to aggregate the routes in the area and advertises the aggregated route to the neighboring IGP areas. By default, when establishing LSPs, LDP searches the routing table for the route that exactly matches the FEC in the received Label Mapping message.

The LDP inter-area feature provides a longest-match label mapping procedure where a label is used if the Forwarding Equivalence Class (FEC) matches an entry in the Routing Information Base (RIB). Matching is defined by an IP longest-match search and does not mandate an exact match.

Configure LDP Inter-Area

The LDP Inter-Area configuration process can be divided into the following tasks:

1. Enable label-switching on the interface in NSM.
2. Enable LDP on an interface in LDP.
3. Run an IGP (Internal Gateway Protocol) such as OSPF or ISIS to distribute reachability information within the MPLS cloud.
4. Give the `inter-area-lsp` command in LDP router mode to enable creation of inter-area LSPs.

To configure a summary route on an ABR, configure two networks such R4 and R5 in Figure 5-86, so that two prefixes are summarized. For example, 4.4.4.0/24 is a summary route for the networks 4.4.4.1/32 and 4.4.4.2/32.

Give the `area-range` command on the routers to summarize the networks. For example: area 2 range 4.4.4.0/24.

Note: LDP Downstream-On-Demand not supported with inter-area configuration. LDP Inter-Area Graceful Restart (GR) is not supported in this release.

Topology

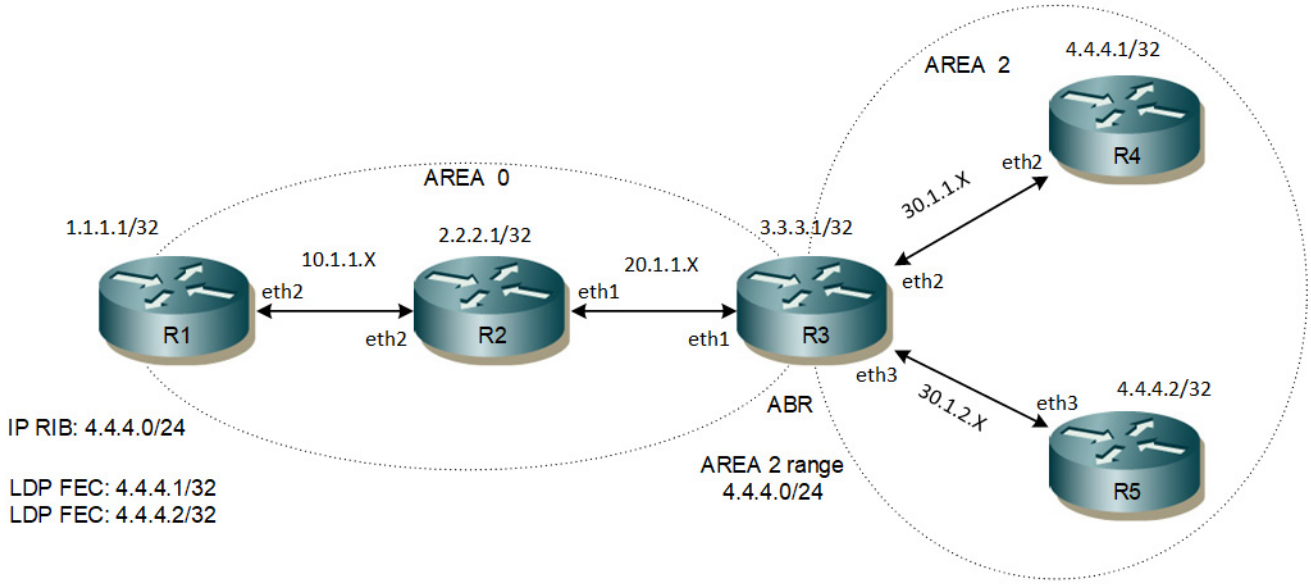


Figure 5-86: LDP inter-area topology

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#label-switching`	Enable label switching on interface `eth2`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 1.1.1.1/32 secondary`	Set the IP address of the loopback interface to 1.1.1.1/32.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 10.1.1.1/24`	Set the IP address of the interface to 10.1.1.1/24
`(config)#router ospf 1`	Configure the routing process and specify the Process ID (1).
`(config-router)#network 1.1.1.1/32 area 0` `(config-router)#network 10.1.1.0/24 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
`(config)#router ldp`	Enter LDP router mode.
`(config-router)#router-id 1.1.1.1`	Set the router ID to IP address 1.1.1.1
`(config-router)#exit`	Exit router mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP on `eth2`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ldp`	Enter LDP router mode.

© 2021 IP Infusion Inc. Proprietary

(config-router)#inter-area-lsp	Enable the inter-area-LSP command.
(config-router)#exit	Exit router mode.

R2

#configure terminal	Enter configure mode.
(config)#interface eth2	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter loopback interface mode.
(config-if)#ip address 2.2.2.1/32	Set the IP address of the loopback interface to 2.2.2.1/32.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Set the IP address of the interface to 10.1.1.2/24
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#ip address 20.1.1.1/24	Set the IP address of the interface to 20.1.1.1/24
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process and specify the Process ID (1).
(config-router)#network 2.2.2.1/32 area 0 (config-router)#network 10.1.1.0/24 area 0 (config-router)#network 20.1.1.0/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config)#router ldp	Enter LDP router mode.
(config-router)#router-id 2.2.2.1	Set the router ID to IP address to 2.2.2.1
(config-router)#exit	Exit router mode.
(config)#interface eth2	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on eth2.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on eth1.
(config-if)#exit	Exit interface mode.
(config)#router ldp	Enter LDP router mode.
(config-router)#inter-area-lsp	Enable the inter-area-LSP command.
(config-router)#exit	Exit router mode.

R3

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface eth1.

(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter loopback interface mode.
(config-if)#ip address 3.3.3.1/32 secondary	Set the IP address of the loopback interface to 3.3.3.1/32.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Set the IP address of the interface to 20.1.1.2/24
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#ip address 30.1.1.1/24	Set the IP address of the interface to 30.1.1.1/24
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Specify the interface (eth3) to be configured.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#ip address 30.1.2.1/24	Set the IP address of the interface to 30.1.2.1/24
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process and specify the Process ID (1).
(config-router)#network 3.3.3.1/32 area 0 (config-router)#network 20.1.1.0/24 area 0 (config-router)#network 30.1.1.0/24 area 2 (config-router)#network 30.1.2.0/24 area 2	Define the interface on which OSPF runs and associate the area ID (0 and 2) respectively with the interface.
(config)#router ldp	Enter LDP router mode.
(config-router)#router-id 3.3.3.1	Set the router ID to IP address 3.3.3.1
(config-router)#exit	Exit router mode.
(config)#interface eth1	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on eth1.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on eth2.
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on eth3.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Configure the routing process and specify the Process ID (1).
(config-router)#area 2 range 4.4.4.0/24	Configure the summary route with range command.
(config-router)#exit	Exit router mode.

R4

#configure terminal	Enter configure mode.
(config)#interface eth2	Enter interface mode.

© 2021 IP Infusion Inc. Proprietary

(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter loopback interface mode.
(config-if)#ip address 4.4.4.1/32 secondary	Set the IP address of the loopback interface to 4.4.4.1/32.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 30.1.1.2/24	Set the IP address of the interface to 30.1.1.2/24
(config)#router ospf 1	Configure the routing process and specify the Process ID (1).
(config-router)#network 4.4.4.1/32 area 2 (config-router)#network 30.1.1.0/24 area 2	Define the interface on which OSPF runs and associate the area ID (2) with the interface.
(config)#router ldp	Enter LDP router mode.
(config-router)#router-id 4.4.4.1	Set the router ID to IP address to 4.4.4.1
(config-router)#exit	Exit router mode.
(config)#interface eth2	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on eth2.
(config-if)#exit	Exit interface mode.

R5

#configure terminal	Enter configure mode.
(config)#interface eth3	Specify the interface (eth3) to be configured.
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter loopback interface mode.
(config-if)#ip address 4.4.4.2/32 secondary	Set the IP address of the loopback interface to 4.4.4.2/32.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 30.1.2.2/24	Set the IP address of the interface to 30.1.2.2/24
(config)#router ospf 1	Configure the routing process and specify the Process ID (1).
(config-router)#network 4.4.4.2/32 area 2 (config-router)#network 30.1.2.0/24 area 2	Define the interface on which OSPF runs and associate the area ID (2) with the interface.
(config)#router ldp	Enter LDP router mode.
(config-router)#router-id 4.4.4.2	Set the router ID to IP address to 4.4.4.2
(config-router)#exi	Exit router mode.
(config)#interface eth3	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on eth3.
(config-if)#exit	Exit interface mode.

Validation

```
R2#sh ip route
```

```
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
O            1.1.1.1/32 [110/2] via 10.1.1.1, xe5, 00:43:19
C            2.2.2.1/32 is directly connected, lo, 00:44:05
O            3.3.3.1/32 [110/2] via 20.1.1.2, xe2, 00:43:13
O IA         4.4.4.0/24 [110/3] via 20.1.1.2, xe2, 00:43:13 ---> Summary Route
C            10.1.1.0/24 is directly connected, xe5, 00:44:04
C            20.1.1.0/24 is directly connected, xe2, 00:44:04
O IA         30.1.1.0/24 [110/2] via 20.1.1.2, xe2, 00:43:13
O IA         30.1.2.0/24 [110/2] via 20.1.1.2, xe2, 00:42:44
C            127.0.0.0/8 is directly connected, lo, 00:44:38

Gateway of last resort is not set

R2#sh ldp inter-area-fecs
LSR codes    : E/N - LSR is egress/non-egress for this FEC,
               L - LSR received a label for this FEC,
               > - LSR will use this route for the FEC
FEC                      Code    Session         Out Label       ELC     Nexthop Addr
Matching RIB prefix - 4.4.4.0/24
4.4.4.1/32               NL>     3.3.3.1         24323           No      20.1.1.2
4.4.4.2/32               NL>     3.3.3.1         24324           No      20.1.1.2


R2#sh mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC               FTN-ID    Tunnel-id   Pri   LSP-Type       Out-Label    Out-Intf   ELC       Nexthop
   L>    1.1.1.1/32         1        0           Yes   LSP_DEFAULT    3            xe5        No        10.1.1.1
   L>    3.3.3.1/32         2        0           Yes   LSP_DEFAULT    3            xe2        No        20.1.1.2
   L>    4.4.4.0/24         3        0           Yes   LSP_DEFAULT    3            xe2        No        20.1.1.2
   L>    4.4.4.1/32         4        0           Yes   LSP_DEFAULT    24323        xe2        No        20.1.1.2
   L>    4.4.4.2/32         7        0           Yes   LSP_DEFAULT    24324        xe2        No        20.1.1.2
   L>    30.1.1.0/24        5        0           Yes   LSP_DEFAULT    3            xe2        No        20.1.1.2
   L>    30.1.2.0/24        6        0           Yes   LSP_DEFAULT    3            xe2        No        20.1.1.2
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 6 MPLS LDP-IGP Synchronization

This chapter contains configurations for MPLS LDP-IGP Synchronization.

Overview

Multi-Protocol Label Switching (MPLS) Label Distribution Protocol (LDP) Interior Gateway Protocol (IGP) Synchronization ensures that LDP is fully established before the IGP path is used for switching. In certain networks, there is dependency on the edge-to-edge Label Switched Paths (LSPs) setup by the Label Distribution Protocol (LDP), e.g., networks that are used for Multi-Protocol Label Switching (MPLS) Virtual Private Network (VPN) applications. For such applications, it is not possible to rely on Internet Protocol (IP) forwarding if the MPLS LSP is not operating appropriately. Labelled traffic can be dropped due to presence of black holes in situations where the Interior Gateway Protocol (IGP) is operational on a link but LDP sessions are not up as the label distribution is not completed. While the link could still be used for IP forwarding, it is not useful for MPLS forwarding, for example, MPLS VPN applications or Border Gateway Protocol (BGP) route-free cores.

The MPLS LDP-IGP Synchronization feature ensures that the Label Distribution Protocol (LDP) is fully established before the Interior Gateway Protocol (IGP) path is used for packet forwarding. It is useful for cases in which the router is the ingress and the decision of whether to take the MPLS LSP or IGP path is decided there.

LDP-IGP synchronization is an interface level feature. It can be selectively enabled in the required interfaces. For each interface there are two commands available for synchronization, one each for IS-IS. Once configured the IGP saves the required information, and also notifies LDP. In between the IGP increases the link cost to maximum and sends advertisements to its peer. This discourages its peers from taking routes that pass via it.

When all LDP sessions hosted on the interface become operational, it sends a notification to the IGP. This is termed as LDP convergence. The IGP then advertises normal cost, so that all traffic now coming to the interface takes the MPLS LSP path established by LDP and not be IP routed.

Prerequisites

Only interfaces that are running Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS) processes are capable of LDP-IGP synchronization. The router must also be running LDP.

Topology

The sample topology diagram is applicable to all configurations in this chapter.

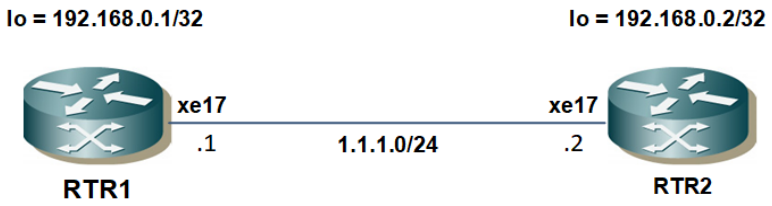


Figure 6-87: Sample Topology for LDP-IGP Synchronization

LDP-IGP Synchronization with OSPF

When IGP synchronization is enabled on OSPF-enabled interfaces, OSPF sends Maximum/Normal cost based on LDP session Down or Up state messages to interfaces until the hold-down-timer expires or synchronization is achieved.

Before configuring LDP-IGP synchronization, the NSM, OSPF and LDP configurations must be completed. The tables below contain examples of how this is done.

RTR1-NSM

`#configure terminal`	Enter configuration mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip address 10.10.10.1/24`	Configure IPv4 address for xe11.
`(config-if)#label-switching`	Enable label switching on interface xe11.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (lo) interface to be configured.
`(config-if)#ip address 1.1.1.1/32 secondary`	Set the IP address of the loopback interface to 1.1.1.1/32.

RTR1-OSPF

`(config)#router ospf 100`	Configure the routing process and specify the Process ID 100. The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 1.1.1.1/32 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface.

RTR1-LDP

`(config)#router ldp`	Enter router mode for LDP.
`(config-router)#router-id 1.1.1.1`	Set the router ID to IP address 1.1.1.1.
`(config-router)#transport-address ipv4 1.1.1.1`	Configure the transport address for IPV4 (for IPV6 use ipv6) to be used for a TCP session over which LDP will run. Note: It is preferable to use the loopback address as the transport address.
`(config-router)#exit`	Exit router mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP for IPv4 on xe11.
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

RTR2-NSM

`#configure terminal`	Enter configuration mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip address 10.10.10.2/24`	Configure IPv4 address for xe11.
`(config-if)#label-switching`	Enable label switching on interface xe11.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (lo) interface to be configured.
`(config-if)#ip address 2.2.2.2/32 secondary`	Set the IP address of the loopback interface to 2.2.2.2/32.

RTR2-OSPF

`(config)#router ospf 100`	Configure the routing process and specify the Process ID 100. The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 2.2.2.2/32 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface.

RTR2-LDP

`(config)#router ldp`	Enter Router mode for LDP.
`(config-router)#router-id 2.2.2.2`	Set the router ID to IP address 2.2.2.2.
`(config-router)#transport-address ipv4 2.2.2.2`	Configure the transport address for IPV4 (for IPV6 use ipv6) to be used for a TCP session over which LDP will run. Note: It is preferable to use the loopback address as transport address.
`(config-router)#exit`	Exit the Router mode and return to the Configure mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP for IPv4 on xe11.
`(config-if)#exit`	Exit interface mode.

Validation

```
R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
2.2.2.2           1   Full/DR         00:00:33    10.10.10.2      xe11
0

R2#show ip ospf neighbor

Total number of full neighbors: 1
```

```
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/Backup     00:00:31    10.10.10.1      xe11
0
R2#

R1#show ldp session
Peer IP Address           IF Name    My Role    State       KeepAlive  UpTime
2.2.2.2                   xe11       Passive    OPERATIONAL    30     00:06:03

R2#show ldp session
Peer IP Address           IF Name    My Role    State       KeepAlive  UpTime
1.1.1.1                   xe11       Active     OPERATIONAL    30     00:06:31

R1#show ldp adjacency
IP Address      Mode          Intf Name    Holdtime   LDP-Identifier
10.10.10.2      Interface     xe11         15         2.2.2.2:0


R2#show ldp adjacency
IP Address      Mode          Intf Name    Holdtime   LDP-Identifier
10.10.10.1      Interface     xe11         15         1.1.1.1:0

R1#show ip ospf interface
lo is up, line protocol is up
  Internet Address 1.1.1.1/32, Area 0.0.0.0, MTU 16436
  Process ID 100, VRF (default), Router ID 1.1.1.1, Network Type LOOPBACK,
Cost: 1
  Transmit Delay is 1 sec,  State Loopback, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
xe11 is up, line protocol is up
  Internet Address 10.10.10.1/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 1.1.1.1, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 2.2.2.2, Interface Address 10.10.10.2
  Backup Designated Router (ID) 1.1.1.1, Interface Address 10.10.10.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 61 sent 62, DD received 3 sent 6
  LS-Req received 1 sent 1, LS-Upd received 4 sent 5
  LS-Ack received 4 sent 3, Discarded 0
  No authentication

R2#sh ip ospf interface
lo is up, line protocol is up
  Internet Address 2.2.2.2/32, Area 0.0.0.0, MTU 16436
  Process ID 100, VRF (default), Router ID 2.2.2.2, Network Type LOOPBACK,
Cost: 1
  Transmit Delay is 1 sec,  State Loopback, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
xe11 is up, line protocol is up
  Internet Address 10.10.10.2/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 2.2.2.2, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
```


© 2021 IP Infusion Inc. Proprietary

```
    Designated Router (ID) 2.2.2.2, Interface Address 10.10.10.2
    Backup Designated Router (ID) 1.1.1.1, Interface Address 10.10.10.1
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:01
    Neighbor Count is 1, Adjacent neighbor count is 1
    Hello received 62 sent 63, DD received 6 sent 3
    LS-Req received 1 sent 1, LS-Upd received 5 sent 4
    LS-Ack received 3 sent 4, Discarded 0
    No authentication

R1#show mpls ldp igp sync
R1#

R2#show mpls ldp igp sync
R2#
```

LDP-IGP Synchronization

Now that NSM, OSPF and LDP are all enabled, the LDP-IGP synchronization can be configured.

RTR1

`(config)#interface xe11`	Enter interface mode.
`(config-if)#mpls ldp-igp sync ospf holddown-timer 500`	Enable LDP-IGP Synchronization for xe11 belonging to an OSPF process and 500 seconds is holddown-timer value for IGP to wait until LDP converges. **OSPF:** This command is part of OSPF Process. Note: Holddown-timer range is 1 to 2147483 seconds. If holddown timer is not configured, IGP waits indefinitely for LDP to converge. Use the command mpls ldp-igp sync ospf to configure without a holddown-timer.
`(config-if)#mpls ldp-igp sync-delay 60`	Configure time delay in seconds for notification of LDP convergence to IGP. This is not applicable for notification of non-convergence. Range is 5 to 60 seconds. This command is optional. **LDP:** This command is part of LDP Process. **Default:** If not configured the delay is 0 seconds.
`(config-if)#exit`	Exit interface mode.

RTR2

`(config)#interface xe11`	Enter interface mode.
`(config-if)#mpls ldp-igp sync ospf holddown-timer 500`	Enable LDP-IGP Synchronization for interfaces (xe11) belonging to an OSPF process.and 500 secs is Holddown-timer value for IGP to wait until LDP Converge. **OSPF:** This command is part of the OSPF Process.vNote: Holddown-timer range is <1-2147483> seconds. If holddown timer is not configured, IGP waits indefinitely for LDP to converge. Use command mpls ldp-igp sync ospf to configure without a holddown-timer.

`(config-if)#mpls ldp-igp sync-delay 60`	Configure the time delay in seconds for the notification of LDP convergence to IGP. (This is not applicable for notification of non-convergence.) Range is 5 to 60 seconds. This command is optional. **LDP:** This command is part of LDP Process. **Default:** If not configured the delay is 0 seconds.
`(config-if)#exit`	Exit interface mode.

RTR1 Validation

When LDP IGP SYNC is Configured with hold-down and sync-delay timer

```
R1#show ip ospf interface
lo is up, line protocol is up
  Internet Address 1.1.1.1/32, Area 0.0.0.0, MTU 16436
  Process ID 100, VRF (default), Router ID 1.1.1.1, Network Type LOOPBACK,
Cost:
 1
  Transmit Delay is 1 sec,  State Loopback, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
xe11 is up, line protocol is up
  Internet Address 10.10.10.1/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 1.1.1.1, Network Type BROADCAST,
Cost
: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  LDP-OSPF Sync configured
    Holddown timer : 500 seconds, Remaining time = 0 seconds
  Designated Router (ID) 2.2.2.2, Interface Address 10.10.10.2
  Backup Designated Router (ID) 1.1.1.1, Interface Address 10.10.10.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 178 sent 179, DD received 3 sent 6
  LS-Req received 1 sent 1, LS-Upd received 5 sent 6
  LS-Ack received 5 sent 4, Discarded 0
  No authentication
R1#

R1#show mpls ldp igp sync
xe11 is up, line protocol is up
  LDP configured; LDP-IGP Synchronization enabled.
  Session IP Address : 2.2.2.2
    Sync status: Achieved
    Delay timer: Configured, 60 seconds, Not Running
```

RTR2 Validation

```
R2#show ip ospf interface
lo is up, line protocol is up
  Internet Address 2.2.2.2/32, Area 0.0.0.0, MTU 16436
  Process ID 100, VRF (default), Router ID 2.2.2.2, Network Type LOOPBACK,
Cost:
 1
  Transmit Delay is 1 sec,  State Loopback, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```


© 2021 IP Infusion Inc. Proprietary

```
xe11 is up, line protocol is up
  Internet Address 10.10.10.2/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 2.2.2.2, Network Type BROADCAST,
Cost
: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  LDP-OSPF Sync configured
    Holddown timer : 500 seconds, Remaining time = 0 seconds
  Designated Router (ID) 2.2.2.2, Interface Address 10.10.10.2
  Backup Designated Router (ID) 1.1.1.1, Interface Address 10.10.10.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 211 sent 211, DD received 6 sent 3
  LS-Req received 1 sent 1, LS-Upd received 8 sent 7
  LS-Ack received 6 sent 7, Discarded 0
  No authentication
R2#

R2#show mpls ldp igp sync
xe11 is up, line protocol is up
  LDP configured; LDP-IGP Synchronization enabled.
  Session IP Address : 1.1.1.1
    Sync status: Achieved
    Delay timer: Configured, 60 seconds, Not Running
```

LDP-IGP Synchronization with IS-IS

When IGP synchronization is enabled on an IS-IS enabled interfaces, IS-IS sends Maximum/Normal cost based on LDP session or Up state on interfaces until hold-down-timer expires or synchronization is achieved.

Before configuring LDP-IGP synchronization, the NSM, IS-IS and LDP configurations must be completed. The tables below contain examples of how this is done.

RTR1-NSM

`#configure terminal`	Enter configuration mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip address 10.10.10.1/24`	Set the IP address of the xe11 to 10.10.10.1/24.
`(config-if)#label-switching`	Enable label switching on xe11.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (lo) interface to be configured.
`(config-if)#ip address 1.1.1.1/32 secondary`	Set the IP address of the loopback interface to 1.1.1.1/32.
`(config-if)#exit`	Exit interface mode.

RTR1-IS-IS

`(config)#router isis 1`	Configure the IS-IS routing instance and specify the TAG (1). The TAG should be a WORD - ISO routing area tag.
`(config-router)#is-type level-1`	Define the IS to the specified level of routing for router.

`(config-router)#net 49.0001.0000.0000.0001.00`	Configure the Network Entity Title (NET) for the instance.
`(config-router)#exit`	Exit the Router mode and return to the Configure mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip router isis 1`	Configure IS-IS IPv4 routing on the interface with IS-IS tag instance 1.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Enter interface mode for the loopback interface (lo).
`(config-if)#ip router isis 1`	Configure IS-IS IPv4 routing on the interface with IS-IS tag instance 1.
`(config-if)#exit`	Exit interface mode.

RTR1-LDP

`(config)#router ldp`	Enter Router mode for LDP.
`(config-router)#router-id 1.1.1.1`	Set the router ID to IP address 1.1.1.1.
`(config-router)#transport-address ipv4 1.1.1.1`	Configure the transport address for IPV4 (for IPv6 use an IPv6 address) to use for a TCP session over which LDP will run. Note: It is preferable to use the loopback address as transport address.
`(config-router)#exit`	Exit the Router mode and return to the Configure mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP for IPv4 on xe11.
`(config-if)#exit`	Exit interface mode.

RTR2-NSM

`#configure terminal`	Enter configuration mode
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip address 10.10.10.2/24`	Set the IP address of xe11 to 10.10.10.2/24
`(config-if)#label-switching`	Enable label switching on interface xe11.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (lo) interface to be configured.
`(config-if)#ip address 2.2.2.2/32 secondary`	Set the IP address of the loopback interface to 2.2.2.2/32.
`(config-if)#exit`	Exit interface mode.

RTR2-IS-IS

`(config)#router isis 1`	Configure the IS-IS routing instance and specify the TAG as 1. The TAG should be a WORD - ISO routing area tag.
`(config-router)#is-type level-1`	Define the IS to the specified level of routing for router.
`(config-router)#net 49.0001.0000.0000.0002.00`	Configure the Network Entity Title (NET) for the instance.
`(config-router)#exit`	Exit the Router mode and return to the Configure mode.
`(config)#interface xe11`	Enter interface mode.

© 2021 IP Infusion Inc. Proprietary

(config-if)#ip router isis 1	Configure IS-IS IPv4 routing on the interface with is-is tag instance 1.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode for the loopback (lo) interface.
(config-if)#ip router isis 1	Configure IS-IS IPv4 routing on the interface with IS-IS tag instance 1.
(config-if)#exit	Exit interface mode.

RTR2-LDP

(config)#router ldp	Enter Router mode for LDP.
(config-router)#router-id 2.2.2.2	Set the router ID to IP address 2.2.2.2.
(config-router)#transport-address ipv4 2.2.2.2	Configure the transport address for IPv4 (for IPv6 use an IPv6 address) to use for a TCP session over which LDP will run. Note: It is preferable to use the loopback address as transport address.
(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface xe11	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP for IPv4 on xe11.
(config-if)#exit	Exit interface mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 xe11        6cb9.c5cf.da69      Up     24        L1   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 xe11        b86a.97d1.24d1      Up     9         L1   IS-IS

R1#show clns is-neighbors

Tag 1:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0002 xe11        Up     L1   64        0000.0000.0001.01

R2#show clns is-neighbors

Tag 1:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
```

```
0000.0000.0001 xe11        Up     L1   64        0000.0000.0001.01

R1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
2.2.2.2                   xe11       Passive   OPERATIONAL   30    00:08:08

R1#show ldp adjacency
IP Address      Mode          Intf Name    Holdtime   LDP-Identifier
10.10.10.2      Interface     xe11        15         2.2.2.2:0

R2#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
1.1.1.1                   xe11       Active    OPERATIONAL   30    00:08:24

R2#show ldp adjacency
IP Address      Mode          Intf Name    Holdtime   LDP-Identifier
10.10.10.1      Interface     xe11        15         1.1.1.1:0

R1#show isis interface xe11
xe11 is up, line protocol is up
  Routing Protocol: IS-IS (1)
    Network Type: Broadcast
    Circuit Type: level-1
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x0000271C
    Local SNPA: b86a.97d1.24d1
    IP interface address:
      10.10.10.1/24
    IPv6 interface address:
      fe80::ba6a:97ff:fed1:24d1/64
    Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-1 adjacencies: 1
    Level-1 LSP MTU: 1492
    Next IS-IS LAN Level-1 Hello in 792 milliseconds

R2#show isis interface xe11
xe11 is up, line protocol is up
  Routing Protocol: IS-IS (1)
    Network Type: Broadcast
    Circuit Type: level-1
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x0000271B
    Local SNPA: 6cb9.c5cf.da69
    IP interface address:
      10.10.10.2/24
    IPv6 interface address:
      fe80::6eb9:c5ff:fecf:da69/64
    Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-1 adjacencies: 1
    Level-1 LSP MTU: 1492
    Next IS-IS LAN Level-1 Hello in 1 seconds


R1#show isis database detail
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
```


© 2021 IP Infusion Inc. Proprietary

```
0000.0000.0001.00-00* 0x00000002   0xB193        516               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   10.10.10.1
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 10.10.10.0 255.255.255.0
  Metric:   10         IP 1.1.1.1 255.255.255.255
0000.0000.0001.01-00* 0x00000001   0x1FBD        516               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00  0x00000002   0x84BA        519               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   10.10.10.2
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 10.10.10.0 255.255.255.0
  Metric:   10         IP 2.2.2.2 255.255.255.255

R2#show isis database detail
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000002   0xB193        521               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   10.10.10.1
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 10.10.10.0 255.255.255.0
  Metric:   10         IP 1.1.1.1 255.255.255.255
0000.0000.0001.01-00  0x00000001   0x1FBD        521               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000002   0x84BA        526               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   10.10.10.2
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 10.10.10.0 255.255.255.0
  Metric:   10         IP 2.2.2.2 255.255.255.255



R1#show mpls ldp igp sync
R1#

R2#show mpls ldp igp sync
R2#
```

LDP-IGP SYNC Configuration

Now that NSM, IS-IS and LDP are all enabled, the LDP-IGP synchronization can be configured.

RTR1

`(config)#interface xe11`	Enter interface mode.
`(config-if)#mpls ldp-igp sync isis level-1 holddown-timer 700`	Configure LDP-IGP Synchronization for interface xe11 belonging to an IS-IS process with corresponding IS-IS level.700 seconds is the holddown-timer value for IGP to wait until LDP converges. The values level-1|level-2-only|level-1-2 identify the IS-IS level instance. The interface can be acting on any level, but the sync is applicable only when it matches with the level given in IGP sync command. **IS-IS:** This command is part of ISIS Process. **Default:** Mandatory configuration. No default option. Note: The holddown-timer Range is 1 to 2147483 seconds. If no holddown timer is configured, IGP waits indefinitely for LDP to Converge. Use the command mpls ldp-igp sync is-is <level-type> to configure without a holddown-timer.
`(config-if)#mpls ldp-igp sync-delay 55`	Set the time delay in seconds for the notification of LDP convergence to IGP. This is not applicable for notification of non-convergence. Range is 5 to 60 seconds. This command is optional. **LDP:** This command is part of LDP Process. **Default:** If not configured, the delay is 0 seconds.
`(config-if)#exit`	Exit interface mode.

LDP-IGP SYNC Configuration

Now that NSM, IS-IS and LDP are all enabled, the LDP-IGP synchronization can be configured.

RTR2

`(config)#interface xe11`	Enter interface mode.
`(config-if)#mpls ldp-igp sync isis level-1 holddown-timer 700`	Configure LDP-IGP Synchronization for interface xe11 belonging to an IS-IS process with corresponding IS-IS level.700 secs is the holddown-timer value for IGP to wait until LDP converges. The parameters level-1|level-2-only|level-1-2 identify the IS-IS instance level. The interface can be acting on any level, but sync is applicable only when it matches with the level given in IGP sync command. **IS-IS:** This command is part of IS-IS Process. **Default:** Mandatory configuration. No default option. Note: The holddown-timer Range is 1 to 2147483 seconds. If no holddown timer is configured, IGP waits indefinitely for LDP to Converge. Use command mpls ldp-igp sync is-is <level-type> to configure without a holddown-timer.

© 2021 IP Infusion Inc. Proprietary

(config-if)#mpls ldp-igp sync-delay 55	Set the time delay in seconds for notification of LDP convergence to IGP. This is not applicable for notification of non-convergence. Range is 5 to 60 seconds. This command is optional. **LDP:** This command is part of LDP Process. **Default:** If not configured, the delay is 0 seconds.
(config-if)#exit	Exit interface mode.

RTR1 Validation

When LDP IGP SYNC is Configured with hold-down and sync-delay timer

```
R1#show isis interface xe11
xe11 is up, line protocol is up
  Routing Protocol: IS-IS (1)
    Network Type: Broadcast
    Circuit Type: level-1
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x0000271C
    Local SNPA: b86a.97d1.24d1
    IP interface address:
      10.10.10.1/24
    IPv6 interface address:
      fe80::ba6a:97ff:fed1:24d1/64
    LDP-ISIS Sync Configured
      Holddown timer = 700 seconds, Remaining time = 0 seconds
    Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-1 adjacencies: 1
    Level-1 LSP MTU: 1492
    Next IS-IS LAN Level-1 Hello in 420 milliseconds
R1#

R1#show mpls ldp igp sync
xe11 is up, line protocol is up
  LDP configured; LDP-IGP Synchronization enabled.
  Session IP Address : 2.2.2.2
    Sync status: Achieved
    Delay timer: Configured, 55 seconds, Not Running
R1#
```

RTR2 Validation

```
R2#show  isis interface xe11
xe11 is up, line protocol is up
  Routing Protocol: IS-IS (1)
    Network Type: Broadcast
    Circuit Type: level-1
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x0000271B
    Local SNPA: 6cb9.c5cf.da69
    IP interface address:
      10.10.10.2/24
    IPv6 interface address:
      fe80::6eb9:c5ff:fecf:da69/64
```

```
    LDP-ISIS Sync Configured
      Holddown timer = 700 seconds, Remaining time = 0 seconds
    Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-1 adjacencies: 1
    Level-1 LSP MTU: 1492
    Next IS-IS LAN Level-1 Hello in 4 seconds
R2#
R2#show mpls ldp igp sync
xe11 is up, line protocol is up
  LDP configured; LDP-IGP Synchronization enabled.
  Session IP Address : 1.1.1.1
    Sync status: Achieved
    Delay timer: Configured, 55 seconds, Not Running
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 7 MPLS Statistics Configuration

This chapter provides the configuration required for configuring MPLS LSPs and verifying the statistics of packets captured at the supported interfaces, in terms of both packet count and bytes, when traffic is sent.

Configure LDP-LSP

Topology

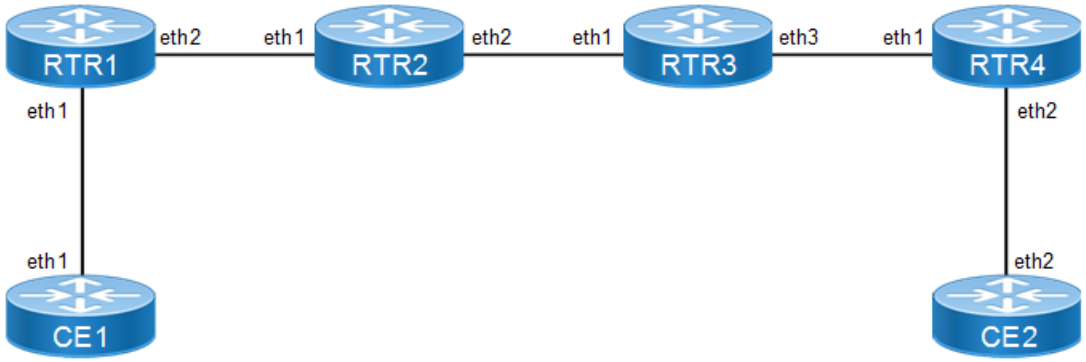


Figure 7-88: MPLS Statistics Topology

RTR1

Loopback Interface configuration

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface `(lo)` to be configured.
`(config-if)#ip address 11.11.11.11/32 secondary`	Configure IP address on loopback interface
`(config-if)#exit`	Exit interface mode.

Global LDP configuration

`(config)#router ldp`	Enter `Router` mode for LDP.
`(config-router)#transport-address ipv4 11.11.11.11`	Configure the loopback address as transport-address
`(config-router)#targeted-peer ipv4 44.44.44.44`	Configure the loopback address of RTR4 as targeted peer.
`(config-router-targeted-peer)#exit`	Exit router-targeted-peer mode and enter config-router mode
`(config-router)#end`	Exit router and configure mode

© 2021 IP Infusion Inc. Proprietary

Enabling LDP and label switching on interface

`#configure terminal`	Enter configure mode.
`(config)#interface eth2`	Enter interface mode for eth2.
`(config-if)#enable-ldp ipv4`	Enable LDP on the interface.
`(config-if)#label-switching`	Enable Label switching on the interface.
`(config-if)#ip address 10.10.10.1/24`	Configure IP address on the interface.
`(config-if)#exit`	Exit interface mode.

Global OSPF configuration

`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 11.11.11.11/32 area 0`	Advertise loopback address in OSPF.
`(config-router)#network 10.10.10.0/24 area 0`	Advertise network address (eth2) in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.

RTR2

Loopback Interface configuration

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface `(lo)` to be configured.
`(config-if)#ip address 22.22.22.22/32 secondary`	Configure IP address on loopback interface
`(config-if)#exit`	Exit interface mode.

Global LDP configuration

`(config)#router ldp`	Enter `Router` mode for LDP.
`(config-router)#transport-address ipv4 22.22.22.22`	Configure the loopback address as transport-address
`(config-router)#end`	Exit router and configure mode

Enabling LDP and label switching on interface

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode for eth1.
`(config-if)#enable-ldp ipv4`	Enable LDP on the interface.
`(config-if)#label-switching`	Enable Label switching on the interface.
`(config-if)#ip address 10.10.10.2/24`	Configure IP address on the interface.
`(config-if)#exit`	Exit interface mode.

© 2021 IP Infusion Inc. Proprietary

(config)#interface eth2	Enter interface mode for eth2.
(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#ip address 20.20.20.1/24	Configure IP address on the interface.
(config-if)#exit	Exit interface mode.

OSPF Configuration

(config)#router ospf 100	Enter the Router OSPF mode
(config-router)#network 22.22.22.22/32 area 0.0.0.0	Advertise loopback address in OSPF
(config-router)#network 10.10.10.2/24 area 0.0.0.0	Advertise network address (eth1) in OSPF.
(config-router)#network 20.20.20.1/24 area 0.0.0.0	Advertise network address (eth2) in OSPF.
(config-router)#exit	Exit OSPF router configuration mode.

RTR3

Loopback Interface configuration

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the interface (lo) to be configured.
(config-if)#ip address 33.33.33.33/32 secondary	Configure IP address on loopback interface
(config-if)#exit	Exit interface mode.

Global LDP configuration

(config)#router ldp	Enter Router mode for LDP.
(config-router)#transport-address ipv4 33.33.33.33	Configure the loopback address as transport-address
(config-router)#end	Exit router and configure mode

Enabling LDP and label switching on interface

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode for eth1.
(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#ip address 20.20.20.2/24	Configure IP address on the interface.
(config-if)#exit	Exit interface mode.

(config)#interface eth2	Enter interface mode for eth2.
(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#ip address 30.30.30.1/24	Configure IP address on the interface.
(config-if)#exit	Exit interface mode.

OSPF Configuration

(config)#router ospf 100	Enter the Router OSPF mode
(config-router)#network 33.33.33.33/32 area 0.0.0.0	Advertise loopback address in OSPF
(config-router)#network 20.20.20.2/24 area 0.0.0.0	Advertise network address (eth1) in OSPF.
(config-router)#network 30.30.30.1/24 area 0.0.0.0	Advertise network address (eth2) in OSPF.
(config-router)#exit	Exit OSPF router configuration mode.

RTR4

Loopback Interface configuration

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the interface (lo) to be configured.
(config-if)#ip address 44.44.44.44/32 secondary	Configure IP address on loopback interface
(config-if)#exit	Exit interface mode.

Global LDP configuration

(config)#router ldp	Enter Router mode for LDP.
(config-router)#transport-address ipv4 44.44.44.44	Configure the loopback address as transport-address
(config-router)#targeted-peer ipv4 11.11.11.11	Configure the loopback address of RTR1 as targeted peer.
(config-router-targeted-peer)#exit	Exit router-targeted-peer mode and enter config-router mode
(config-router)#end	Exit router and configure mode

Enabling LDP and label switching on interface

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode for eth1.

© 2021 IP Infusion Inc. Proprietary

(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#ip address 30.30.30.2/24	Configure IP address on the interface.
(config-if)#exit	Exit interface mode.

Global OSPF Configuration

(config)#router ospf 100	Enter the Router OSPF mode
(config-router)#network 44.44.44.44/32 area 0.0.0.0	Advertise loopback address in OSPF
(config-router)#network 30.30.30.2/24 area 0.0.0.0	Advertise network address (eth1) in OSPF.
(config-router)#exit	Exit OSPF router configuration mode.

Virtual Circuit Configuration

RTR1

Global VC Configuration

(config)#mpls l2-circuit t1 100 44.44.44.44	Enter the VC configuration command in router mode.
(config)#bridge 1 protocol ieee vlan-bridge	Creating a VLAN-bridge in router mode.

Interface Configuration

(config)#service-template st1	Template configuration
(config-svc)#exit	Exit service template configuration
(config)#interface eth1	Enter interface mode for eth1.
(config-if)#switchport	Enable switchport on the interface.
(config-if)#mpls-l2-circuit t1 service-template st1	Bind the interface to VC created in ethernet mode.
(config-if)#exit	Exit interface mode.

RTR4

Global VC Configuration

(config)#mpls l2-circuit t1 100 11.11.11.11	Enter the VC configuration command in router mode.
(config)#bridge 1 protocol ieee vlan-bridge	Creating a VLAN-bridge in router mode.

Interface Configuration

(config)#service-template st1	Template configuration
(config-svc)#exit	Exit service template mode
(config)#interface eth2	Enter interface mode for eth2.

`(config-if)#switchport`	Enable switchport on the interface.
`(config-if)#mpls-l2-circuit t1 service-template st1`	Bind the interface to VC created in ethernet mode.
`(config-if)#exit`	Exit interface mode.

Configure Static-LSP

RTR1

Global Static configuration

`(config)#mpls ftn-entry 44.44.44.44/32 100 10.10.10.2 eth2`	Configure FTN entry for rtr4 loopback.
`(config)#mpls ilm-entry 900  pop`	Pop the incoming label

Enabling label switching on interface

`(config)#interface eth2`	Enter interface mode for eth2.
`(config-if)#label-switching`	Enable Label switching on the interface.
`(config-if)#exit`	Exit interface mode.

RTR2

Global Static configuration

`mpls ilm-entry 100 swap 200 eth2 20.20.20.2 44.44.44.44/32`	Swap the incoming label
`mpls ilm-entry 800 swap 900 eth1 10.10.10.1 11.11.11.11/32`	Swap the incoming label

Enabling label switching on interface

`(config)#interface eth1`	Enter interface mode for eth1.
`(config-if)#label-switching`	Enable Label switching on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for eth2.
`(config-if)#label-switching`	Enable Label switching on the interface.
`(config-if)#exit`	Exit interface mode.

RTR3

Global Static configuration

© 2021 IP Infusion Inc. Proprietary

(config)#mpls ilm-entry 200 swap 300 eth2 30.30.30.2 44.44.44.44/32	Swap the incoming label
(config)#mpls ilm-entry 700 swap 800 eth1 20.20.20.1 11.11.11.11/32	Swap the incoming label

Enabling label switching on interface

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode for eth2.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#exit	Exit interface mode.

RTR4

Global Static configuration

(config)#mpls ftn-entry 11.11.11.11/32 700 30.30.30.1 eth1	Configure FTN entry for RTR1 loopback.
(config)mpls ilm-entry 300 pop	Pop the incoming label.

Enabling label switching on interface

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#exit	Exit interface mode.

Validation

Here, 1000 packets are transmitted between the PE nodes and the output of counters at each node is mentioned below.

For Static-LSP

```
RTR1#show mpls counters static
[FTN statistics]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+
 44.44.44.44/32     100         49939                807798
[ILM statistics]
+------------------+-----------+-----------+--------------------+-------------
-------+--------------------+--------------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx
bytes      |     Tx packets     |      Tx bytes      |
```

```
+------------------+-----------+-----------+--------------------+------------
-------+--------------------+--------------------+
 0.0.0.0/0         900         n/a         40546               3486956
n/a                  n/a
RTR1#


RTR2#show mpls counters static
[FTN statistics]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+

[ILM statistics]
+------------------+-----------+-----------+--------------------+------------
--
-----+--------------------+--------------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx
bytes
     |     Tx packets     |      Tx bytes      |
+------------------+-----------+-----------+--------------------+------------
--
-----+--------------------+--------------------+
 44.44.44.44/32     100         200         9393                 807798
      9393                 807798
 11.11.11.11/32     800         900         40546                3486956
      40546                3486956
RTR2#


RTR3#show mpls counters static
[FTN statistics]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+

[ILM statistics]
+------------------+-----------+-----------+--------------------+------------
-------+--------------------+--------------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx
bytes      |     Tx packets     |      Tx bytes      |
+------------------+-----------+-----------+--------------------+------------
-------+--------------------+--------------------+
 44.44.44.44/32     200         300         9393                 807798
9393                 807798
 11.11.11.11/32     700         800         40546                3486956
40546                3486956
RTR3#


RTR4#show mpls counters static
[FTN statistics]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+
 11.11.11.11/32     700         49939                3486956

[ILM statistics]
```


© 2021 IP Infusion Inc. Proprietary

```
+------------------+----------+----------+--------------------+------------
--
-----+--------------------+--------------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx
bytes
     |     Tx packets     |      Tx bytes      |
+------------------+----------+----------+--------------------+------------
--
-----+--------------------+--------------------+
 0.0.0.0/0          300         n/a         9393                 807798
      n/a                  n/a
RTR4#
```

For LDP-LSP

```
RTR1#show mpls counters ldp
[FTN statistics]
+------------------+----------+--------------------+--------------------+
|       FEC          | out-label |   Tx packets    |      Tx bytes      |
+------------------+-------------+------------------+--------------------+
 44.44.44.44/32     52483          1000                1004000
[ILM statistics]
+-----+---------+-----------+------------+---------+-----------+---------+
| FEC |in-label | out-label | Rx packets | Rx bytes| Tx packets| Tx bytes|
+-----+---------+-----------+------------+---------+-----------+---------+

RTR2#show mpls counters ldp
[FTN statistics]
+------------------+----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+----------+--------------------+--------------------+
[ILM statistics]
+-----+----------+-----------+------------+----------+------------+----------+
| FEC | in-label | out-label | Rx packets | Rx bytes | Tx packets | Tx bytes |
+-----+----------+-----------+------------+----------+------------+----------+
44.44.44.44/32     52483   52483  1000        1004000   1000         1004000
```

For LDP-VC

```
R1#show mpls l2-circuit t1 statistics
MPLS Layer-2 Virtual Circuit: t1, id 100
 Access port statistics:
   RX:  Input packets  : 0
        Input bytes    : 0
   TX:  Output packets : 4642811
        Output bytes   : 297139904

 Network port statistics:
   RX:  Input packets  : 4642804
        Input bytes    : 399281144
   TX:  Output packets : 0
        Output bytes   : 0


R4#show mpls l2-circuit t1 statistics
MPLS Layer-2 Virtual Circuit: t1, id 100
```

```
Access port statistics:
  RX:  Input packets  : 4633957
       Input bytes    : 296573248
  TX:  Output packets : 0
       Output bytes   : 0

Network port statistics:
  RX:  Input packets  : 0
       Input bytes    : 0
  TX:  Output packets : 4633960
       Output bytes   : 398520560
```


© 2021 IP Infusion Inc. Proprietary

Multi-Protocol Label Switching Command Reference

Contents

This document contains these chapters:

- Chapter 1, *MPLS Commands*
- Chapter 2, *Differentiated Services Commands*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 MPLS Commands

This chapter is a reference for the MPLS commands:

- bandwidth
- clear mpls counters ldp
- clear mpls counters rsvp
- clear mpls counters static
- clear mpls l2-circuit statistics
- clear mpls l2-circuit statistics
- control-word
- label-switching
- match vlan
- mpls ac-group
- mpls admin-groups
- mpls bandwidth-class
- mpls disable-all-interfaces
- mpls enable-all-interfaces
- mpls ftn-entry tunnel-id
- mpls ftn-entry
- mpls ilm-entry pop
- mpls ilm-entry swap
- mpls ilm-entry vpnpop
- mpls ingress-ttl
- mpls l2-circuit
- mpls-l2-circuit NAME
- mpls l2-circuit-fib-entry
- mpls label mode
- mpls local-packet-handling
- mpls lsp-model
- mpls lsp-stitching
- mpls map-route
- mpls min-label-value
- mpls propagate-ttl
- mpls traffic-eng
- mpls traffic-eng srlg
- ping mpls

© 2021 IP Infusion Inc. Proprietary

- secondary srlg-disjoint
- secondary-priority srlg-disjoint
- rewrite ingress
- service-template
- service-tpid
- show mpls
- show mpls admin-groups
- show mpls bandwidth-class
- show mpls counters ldp
- show mpls counters rsvp
- show mpls counters static
- show mpls cross-connect-table
- show mpls forwarding-table
- show mpls ftn-table
- show mpls ilm-table
- show mpls in-segment-table
- show mpls l2-circuit
- show mpls l2-circuit statistics
- show mpls mapped-routes
- show mpls out-segment-table
- show mpls qos-resource
- show mpls vc-table
- show mpls vrf
- show mpls vrf-forwarding-table vrf
- show running-config interface mpls
- show running-config mpls
- show running-config service-template
- show running-config vc
- show running-config vpls
- show service-template
- show vccv statistics
- srlg-disjoint
- trace mpls
- tunnel-id
- tunnel-name
- tunnel-select-policy
- vccv cc-type
- vccv cv-type

© 2021 IP Infusion Inc. Proprietary

bandwidth

Use this command to specify the maximum bandwidth to be used for a band-class. The bandwidth value is in bits.

Note: Run this command in the Bandwidth-class mode (refer to mpls bandwidth-class).

Command Syntax

```
bandwidth BANDWIDTH setup-priority <0-7> hold-priority <0-7>
```

Parameter

BANDWIDTH	<1-999>k for 1 to 999 kilo bits/s
	<1-999>m for 1 to 999 mega bits/s
	<1-100>g for 1 to 100 giga bits/s
setup-priority	Indicate the setup-priority parameter
<0-7>	The actual setup priority value
hold-priority	Indicate the hold-priority parameter
<0-7>	The actual hold priority value

Default

By default, bandwidth priority is 0

Command Mode

Bandwidth-class mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls bandwidth-class new-BC
(config-mpls-bw)#bandwidth 100m setup-priority 1 hold-priority 1
```

clear mpls counters ldp

Use this command to clear traffic statistics for FTNs and ILMs configured by LDP.

Command Syntax

```
clear mpls counters ldp ((ftn (|A.B.C.D/M)) | (ilm (|A.B.C.D/M)) |)
```

Parameter

`ftn`	FEC-to-NHLFE map counters
`A.B.C.D/M`	FEC prefix
`ilm`	Incoming label map counters
`A.B.C.D/M`	FEC prefix

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear mpls counters ldp
```


© 2021 IP Infusion Inc. Proprietary

clear mpls counters rsvp

Use this command to clear traffic statistics for LSPs configured by RSVP.

Command Syntax

```
clear mpls counters rsvp ((tunnel-name NAME) | (tunnel-id TUNNEL_ID) | (node-role
  (ingress | transit | egress)) |)
```

Parameter

NAME	RSVP tunnel name
TUNNEL_ID	RSVP tunnel identifier
ingress	LSP role is ingress
transit	LSP role is transit
egress	LSP role is egress

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear mpls counters rsvp
```

clear mpls counters static

Use this command to clear traffic statistics for statically configured FTNs and ILMs.

Command Syntax

```
clear mpls counters static ((ftn (|A.B.C.D/M)) | (ilm (|A.B.C.D/M)) |)
```

Parameter

`ftn`	FEC-to-NHLFE map counters
`A.B.C.D/M`	FEC prefix
`ilm`	Incoming label map counters
`A.B.C.D/M`	FEC prefix

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear mpls counters static
```


© 2021 IP Infusion Inc. Proprietary

clear mpls l2-circuit statistics

Use this command to clear MPLS traffic statistics for l2 circuit.

Command Syntax

```
clear mpls l2-circuit NAME statistics(access-port|network-port|)
```

Parameters

`name`	Name of L2 circuit
`access-port`	Displays the access port statistics
`network-port`	Displays the network port statistics

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear mpls l2-circuit vcl statistics
```

group-id

Use this command to configure a specific group identifier to existing group with a group name in the MPLS layer-2 virtual circuit.

Use the no parameter with this command to remove group identifier from the MPLS layer-2 virtual circuit

Command Syntax

```
group-id <1-4294967295>
no group-id
```

Parameters

`<1-4294967295>` Value for group identifier

Default

By default, group-id is disabled. If group-name is configured, default group-id is the first available identifier.

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#group-name group-1
(config-pseudowire)#group-id 11
```


© 2021 IP Infusion Inc. Proprietary

group-name

Use this command to map the MPLS layer-2 virtual circuit with a specific group.

Use the no parameter with this command to remove group from the MPLS layer-2 virtual circuit

Command Syntax

```
group-name NAME
no group-name
```

Parameters

NAME	String identifying group NAME

Default

By default, group-name is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#group-name group-1
```

control-word

Use this command to enable control word for the MPLS layer-2 virtual circuit.

Use the no parameter with this command to disable control word from the MPLS layer-2 virtual circuit.

Command Syntax:

```
control-word
no control-word
```

Parameters

NA

Default

By default, control-word is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#control-word
```


© 2021 IP Infusion Inc. Proprietary

label-switching

Use this command to either enable label-switching on an interface or to modify the label-space to which this interface is bound.

Use the `no` parameter and the interface is bound to the platform-wide (zero) label-space.

Command Syntax

```
label-switching
label-switching <0-60000>
no label-switching
```

Parameter

`<0-60000>`	Label space value in this range

Default

By default, label switching is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows the enabling of label switching on the `eth0` interface.

```
#configure terminal
(config)#interface eth0
(config-if)#label-switching 654
```

match vlan

Use this command to configure a match VLAN action for a service template.

Use the `no` parameter to remove a match VLAN action for a service template.

Command Syntax

```
match (all | double-tag outer-vlan <2-4094> inner-vlan VLAN_RANGE | outer-vlan
  VLAN_RANGE | untagged)
no match (double-tag outer-vlan <2-4094> inner-vlan VLAN_RANGE | outer-vlan
  VLAN_RANGE | untagged)
```

Parameter

`all`	Accept all matches
`double-tag`	Double tag match
`outer-vlan`	Double tag outer VLAN
`<2-4094>`	Outer VLAN identifier
`inner-vlan`	Double tag inner VLAN
`VLAN_RANGE`	VLAN identifier <2-4094> range: 2-5,10 or 2-5,7-19
`outer-vlan`	Single tag outer-VLAN
`VLAN_RANGE`	VLAN identifier <2-4094> range: 2-5,10 or 2-5,7-19
`untagged`	Match untagged. This parameter depends on the `switchport dot1q ethertype` configuration. Packets received with a TPID other than 0x8100 (default value) and the TPID value configured by `switchport dot1q ethertype` are treated as untagged. For example, if you give the command: `switchport dot1q ethertype 0x8888` then packets received with TPID 0x8100 or 0x88a8 are treated as tagged. Packets received with other TPIDs are treated as untagged.

Command Mode

MPLS SVC mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS-SP version 1.0.

The inner vlan range option added in OcNOS-SP version 4.1.

Example

```
#configure terminal
(config)#service-template C2
(config-svc)#match double-tag outer-vlan 10 inner-vlan 20
(config-svc)#exit
(config)#service-template C2
(config-svc)#no match double-tag outer-vlan 10 inner-vlan 20
(config-svc)#exit
#configure terminal
```


© 2021 IP Infusion Inc. Proprietary

```
(config)#service-template C3
(config-svc)#match double-tag outer-vlan 10 inner-vlan 200-300
(config-svc)#exit
(config)#service-template C4
(config-svc)#no match double-tag outer-vlan 10 inner-vlan 200-300
(config-svc)#exit
#configure terminal
(config)#service-template t1
(config-svc)#match untagged
(config-svc)#rewrite ingress push 100
```

mpls ac-group

Use this command to create a new access circuit group for MPLS.

Use the `no` parameter with this command to remove an access circuit group.

Command Syntax

```
mpls ac-group NAME <1-4294967295>
no mpls ac-group NAME
```

Parameter

`NAME`	The name of the access circuit group
`<1-4294967295>`	The identifier for the group; used in LDP

Default

By default, mpls ac group is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls ac-group new-ac 123

(config)#no mpls ac-group new-ac
```


© 2021 IP Infusion Inc. Proprietary

mpls admin-groups

Use this command to create a name-to-value binding for an administrative group.

Note: Only 32 administrative groups can be configured at one time.

Use the `no` parameter with this command to remove a named administrative group.

Command Syntax

```
mpls admin-group NAME <0-31>
no mpls admin-group NAME <0-31>
```

Parameters

`NAME`	Name of administrative group
`<0-31>`	The value of the administrative group

Default

By default, mpls admin group is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls admin-group mygroup 3
```

mpls bandwidth-class

Use this command to create a new bandwidth class name. Using this command changes the command mode to Bandwidth-class mode.

Use the `no` parameter with this command to remove a bandwidth class name.

Command Syntax

```
mpls bandwidth-class NAME
no mpls bandwidth-class NAME
```

Parameter

`NAME`	Name of the bandwidth class

Default

By default, mpls bandwidth-class is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls bandwidth-class new-BC
(config-mpls-bw)#

(config)#no mpls bandwidth-class new-BC
```


© 2021 IP Infusion Inc. Proprietary

mpls disable-all-interfaces

Use this command to disable all interfaces for MPLS. This command completely stops all signaling on the router. When issued, all signaling protocols are made aware of this change, which stops all MPLS-specific processing.

Command Syntax

```
mpls disable-all-interfaces
```

Parameters

None

Default

By default, mpls disable-all-interfaces is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls disable-all-interfaces
```

mpls enable-all-interfaces

Use this command to enable all interfaces for MPLS. This command enables all interfaces on a router for label-switching, and is helpful when using a router with many interfaces.

Note: Executing this command does not enable any signaling protocol interaction via all the interfaces. Each protocol needs to be explicitly enabled per interface.

Command Syntax

```
mpls enable-all-interfaces
```

Parameters

None

Default

By default, all interfaces are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls enable-all-interfaces
```


© 2021 IP Infusion Inc. Proprietary

mpls ftn-entry tunnel-id

This command will be used to create a static tunnel.

In hardware, it creates a logical interface to which services can be mapped.

Command Syntax

```
mpls ftn-entry tunnel-id <1-5000> A.B.C.D/M LABEL A.B.C.D IFNAME
  (primary|secondary|)
mpls ftn-entry tunnel-id <1-5000> A.B.C.D A.B.C.D LABEL A.B.C.D IFNAME
  (primary|secondary|)
mpls ftn-entry tunnel-id <1-5000> (A.B.C.D/M|A.B.C.D A.B.C.D) <16-1048575> A.B.C.D
  IFNAME ((secondary|primary)|)


no mpls ftn-entry tunnel-id <1-5000> A.B.C.D/M WORD A.B.C.D IFNAME
  (primary|secondary|)
no mpls ftn-entry tunnel-id <1-5000> A.B.C.D A.B.C.D WORD A.B.C.D IFNAME
  (primary|secondary|)
```

Command Syntax

```
mpls ftn-entry tunnel-id <1-5000> X:X::X:X/M <16-1048575> X:X::X:X IFNAME
  ((secondary|primary)|)
mpls ilm-entry <16-52443> swap <16-52443> IFNAME X:X::X:X X:X::X:X/M
mpls ilm-entry <16-52443> IFNAME swap <16-52443> IFNAME X:X::X:X X:X::X:X/M


no mpls ftn-entry tunnel-id <1-5000> X:X::X:X/M <16-1048575> X:X::X:X IFNAME
  ((secondary|primary)|)
no mpls ilm-entry <16-52443> swap <16-52443> IFNAME X:X::X:X X:X::X:X/M
no mpls ilm-entry <16-52443> IFNAME swap <16-52443> IFNAME X:X::X:X X:X::X:X/M
```

Parameters

`<1-5000>`	The tunnel ID value
`A.B.C.D/M`	Forwarding equivalence class with mask
`A.B.C.D`	Mask for forwarding equivalency class
`LABEL`	Outgoing label
`A.B.C.D`	Nexthop IPv4 address
`IFNAME`	Outgoing interface name
`INDEX`	FTN index for update

Note: When the INDEX parameter is passed, the FTN entry is updated. When INDEX is not used, a new FTN entry is created.

`primary`	The primary LSP; default is primary
`secondary`	The secondary LSP Command Mode

Default

By default, mpls ftn-entry tunnel-id are disabled

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls ftn-entry tunnel-id 2 10.10.0.0/24 16 1.2.3.4 eth1 secondary
(config)#no mpls ftn-entry tunnel-id 2 10.10.0.0/24 16 1.2.3.4 eth1 secondary
```


© 2021 IP Infusion Inc. Proprietary

mpls ftn-entry

Use this command to create a static LSP. In the hardware, this command creates an IP route with outgoing MPLS parameters.

Command Syntax

```
mpls ftn-entry (A.B.C.D/M|A.B.C.D A.B.C.D) <16-52443> A.B.C.D IFNAME
no mpls ftn-entry A.B.C.D/M LABEL A.B.C.D IFNAME
```

Parameters

A.D.C.D/M	Forwarding Equivalence Class with Mask
LABEL	Outgoing label <16-1048575>
A.B.C.D	Nexthop IPv4 address
IFNAME	Outgoing interface name
INDEX	FTN index for update

Default

By default, mpls ftn-entry are disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)# mpls ftn-entry 2.2.2.2/32 111 20.0.0.2 eth1
(config)# no mpls ftn-entry 2.2.2.2/32 111 20.0.0.2 eth1
```

© 2021 IP Infusion Inc. Proprietary

mpls ilm-entry pop

Use this command to create an ILM entry in the ILM table to which a POP incoming interface is bound. Upon receipt of a labeled packet on an MPLS-enabled router, a lookup is done based on the incoming label in the ILM table. If a match is found, the packet may either be label-switched downstream, or popped and passed over IP. In a pop operation, an outgoing label is not needed as is either accepted or forwarded over IP. The nexthop option is also not mandatory because the FEC IP address could be a local IP address.

Use the `no` option with the command to delete an ILM entry. If there is no match, an error message displays.

Command Syntax

```
mpls ilm-entry LABEL IFNAME (pop)
no mpls ilm-entry LABEL IFNAME (pop)
```

Parameters

`LABEL`	Incoming label value
`IFNAME`	Incoming interface name
`pop`	Pop the incoming label

Default

By default, mpls ilm-entry are disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls ilm-entry 100 eth0 pop
```


© 2021 IP Infusion Inc. Proprietary

mpls ilm-entry swap

Use this command to create an ILM entry in the ILM table to which a swap incoming interface is bound. Upon receipt of a labeled packet on an MPLS-enabled router, a lookup is done based on the incoming label in the ILM table. If a match is found, the packet may either be label-switched downstream, or popped and passed over IP.

Use the `no` option with the command to delete an ILM entry. If there is no match, an error message displays.

Command Syntax

```
mpls ilm-entry <16-52443> swap <16-52443> IFNAME A.B.C.D (A.B.C.D/M|A.B.C.D
  A.B.C.D)
mpls ilm-entry <16-52443> IFNAME swap <16-52443> IFNAME A.B.C.D (A.B.C.D/M|A.B.C.D
  A.B.C.D)


no mpls ilm-entry <16-52443> swap <16-52443> IFNAME A.B.C.D (A.B.C.D/M|A.B.C.D
  A.B.C.D)
no mpls ilm-entry <16-52443> IFNAME swap <16-52443> IFNAME A.B.C.D (A.B.C.D/
  M|A.B.C.D A.B.C.D)
```

Parameters

`LABEL`	Incoming label value range <16-1048575>
`IFNAME`	Incoming interface name
`swap`	Specify swap for the incoming label
`LABEL`	Configure an outgoing label with a value from <16-1048575>

Note: A value of 2 indicates explicit NULL and a value of 3 indicates implicit NULL.

`IFNAME`	Outgoing interface name
`A.B.C.D`	Nexthop IPv4 address
`A.B.C.D`	The FEC for which this ILM entry is created
`A.B.C.D/M`	The FEC for which this ILM entry is created, plus mask
`A.B.C.D`	A mask for forwarding equivalence class mask
`<1-429496725>`	ILM index update

Note: When an ILM index value is passed, the ILM entry is updated. If the ILM index is not used, then a new ILM entry is created.

Default

By default, mpls ilm-entry are disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls ilm-entry 16 eth1 swap 17 eth2 1.1.1.1 1.1.1.1/3 1
```


© 2021 IP Infusion Inc. Proprietary

mpls ilm-entry vpnpop

Use this command to create an ILM entry in the ILM table to which a VPN POP incoming interface is bound. Upon receipt of a labeled packet on an MPLS-enabled router, a lookup is done based on the incoming label in the ILM table. If a match is found, the packet may either be label-switched downstream, or popped and passed over IP.

Use the `no` option with the command to delete an ILM entry. If there is no match, an error message displays.

Note: This command is not supported for ZebIC releases.

Command Syntax

```
mpls ilm-entry LABEL IFNAME (vpnpop) LABEL IFNAME A.B.C.D (A.B.C.D/M|A.B.C.D
  A.B.C.D) (<1-4294967295>|)
no mpls ilm-entry LABEL IFNAME (vpnpop) LABEL IFNAME A.B.C.D (A.B.C.D/M|A.B.C.D
  A.B.C.D|) (<1-4294967295>|)
```

Parameters

`LABEL`	Incoming label value
`IFNAME`	Incoming interface name
`vpnpop`	Specify pop for the incoming label
`LABEL`	Configure an outgoing label with a value from <16-1048575>

Note: A value of 0 indicates explicit NULL and a value of 3 indicates implicit NULL.

`IFNAME`	Outgoing interface name
`A.B.C.D`	Nexthop IPv4 address
`A.B.C.D`	The FEC for which this ILM entry is created
`A.B.C.D/M`	The FEC for which this ILM entry is created, plus mask
`A.B.C.D`	A mask for forwarding equivalence class mask
`<1-429496725>`	ILM index update

Note: When an ILM index value is passed, the ILM entry is updated. If the ILM index is not used, then a new ILM entry is created.

Default

By default, mpls ilm-entry are disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls ilm-entry 100 eth0 vpnpop 200 eth1 1.2.3.4 10.10.0.0/24
```

mpls ingress-ttl

Use this command to set a Time to Live (TTL) value for LSPs for which this LSR is the ingress.

Use the `no` parameter with this command to unset the custom TTL value being used for LSPs for which this LSR is the ingress.

Command Syntax

```
mpls ingress-ttl <0-255>
no mpls ingress-ttl
```

Parameter

`<0-255>`	Set the TTL value to use

Default

By default, mpls ingress-ttl value is 64

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls ingress-ttl 3
```


© 2021 IP Infusion Inc. Proprietary

mpls l2-circuit

Use this command to create an instance of an MPLS layer 2 virtual circuit, without specifying a group to which the VC belongs. Refer to group-name for information on how to create an MPLS “with” a specific group. A Layer-2 MPLS Virtual Circuit instance may be bound to any interface on the router; however, only one interface may be bound to a Layer-2 circuit at a time.

Use the `no` parameter with this command to delete an instance of an MPLS Layer-2 Virtual Circuit.

Command Syntax

```
mpls l2-circuit NAME <1-4294967295> A.B.C.D
mpls l2-circuit NAME <1-4294967295> A.B.C.D mode raw
mpls l2-circuit NAME <1-4294967295> A.B.C.D mode tagged
no mpls l2-circuit NAME <1-4294967295> A.B.C.D
```

Parameters

`NAME`	String identifying the MPLS Layer-2 virtual circuit
`<1-4294967295>`	A 32-bit identifier to which the L2 circuit name should be mapped
`A.B.C.D`	IPv4 address for the MPLS L2 virtual circuit end-point

Default

By default, mpls l2-circuit is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
```

mpls-l2-circuit NAME

Use this command in the Interface mode to bind an interface to a MPLS Layer-2 Virtual Circuit created in the configure mode. The qos profiles cos-to-queue and queue-color-to-cos are optional parameters and are configurable dynamically on the virtual circuit by repeating mpls-l2-circuit command along with one or both profile options. In order to dynamically unbind the profile, same command pattern should be repeated by removing the profile which needs to be unbound from the command. Refer ‘qos profile’ commands from configuration guide for more details about qos profiles.

Use the `no` parameter with this command to delete this instance.

Note: QoS profiles are supported only on vlan based virtual circuits. For port based virtual circuits (service template with match-all option), qos profiles can be bound to interface which will take effect, otherwise default qos profile will take effect. Refer ‘qos map-profile’ command for binding qos profiles on interface.

Note: For untagged traffic forwarded via port based virtual circuits (service template with match-all option), queue will be 0 by default. In order to assign a non-zero queue for untagged traffic, use ‘qos untagged-priority <0-7>’ command on the interface.

Note: QoS profile queue-color-to-cos will take effect when MPLS model is uniform. For virtual circuit without rewrite option, ‘qos remark-cos’ need to be additionally configured to update cos. For virtual circuits with rewrite action pop, cos will always be updated based on qos profile irrespective of the MPLS model.

Command Syntax

```
mpls-l2-circuit NAME service-template NAME ({cos-to-queue NAME | queue-color-to-cos
  NAME}|) ((primary|secondary)|)
no  mpls-l2-circuit NAME
```

Parameters

`NAME`	A string identifying the MPLS Layer-2 Virtual Circuit
`primary`	Identify L2 circuit as the primary link
`secondary`	Identify L2 circuit as the secondary link; the secondary link is not activated unless the primary link fails
`service-template`	Customer service template
`NAME`	Name of Customer service template
`cos-to-queue`	Profile for cos to queue map
`NAME`	Profile name for cos to queue map
`queue-color-to-cos`	Profile for queue color to cos map
`NAME`	Profile name for queue color to cos map

Default

By default, mpls l2-circuit is disabled

Command Mode

Interface mode

© 2021 IP Infusion Inc. Proprietary

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal

(config)#interface eth1
(config-if)#switchport
(config-if)#mpls-l2-circuit vc1 service-template C1

(config-if)#no mpls-l2-circuit vc1

(config)#interface eth2
(config-if)#switchport
(config-if)#mpls-l2-circuit vc2 service-template C2

(config-if)#no mpls-l2-circuit vc2

(config-if)#mpls-l2-circuit vc2 service-template C2
(config-if)#no mpls-l2-circuit vc2

(config)#interface eth2
(config-if)#switchport
(config-if)#mpls-l2-circuit vc2 service-template C2

(config-if)#no mpls-l2-circuit vc2

(config-if)#mpls-l2-circuit vc2 service-template C2
(config-if)#no mpls-l2-circuit vc2
```

© 2021 IP Infusion Inc. Proprietary

mpls l2-circuit-fib-entry

Use this command to add a static Layer-2 MPLS Virtual Circuit FIB entry.

Use the `no` parameter with this command to delete a Layer-2 MPLS Virtual Circuit FIB entry.

Command Syntax

```
mpls l2-circuit-fib-entry VC-ID
mpls l2-circuit-fib-entry VC-ID LABEL LABEL A.B.C.D IFNAME NAME
no mpls l2-circuit-fib-entry VC-ID
```

Parameters

`VC-ID`	Virtual Circuit ID
`LABEL`	Incoming label in the range of <16-1048575>
`LABEL`	Outgoing label in the range of <16-1048585>
`A.B.C.D`	Nexthop IPv4 address
`IFNAME`	Provider-facing interface name
`NAME`	Access interface name or VC to be stitched to.

Default

By default, mpls l2-circuit is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls l2-circuit-fib-entry 10 100 200 10.10.10.10 eth1 eth2
```


© 2021 IP Infusion Inc. Proprietary

mpls label mode

Use this command to configure label allocation mode for VPNv4 and/or VPNv6 routes. Label allocation mode as per-vrf is the default mode in which single mpls-label is allocated for all VPN Routes in a VRF. Label allocation mode as per-prefix will allocate unique mpls-labels per VPN route in a VRF. If allocation model is disabled using no mpls label mode configuration, the configuration reverts back to default-mode .

Label allocation mode is the local property i.e. the VRF routes are distributed to BGP-peer as per the mode configured on local node. When per-vrf mode is configured, single label for all routes in the VRF will be distributed to peer node.

Label allocation mode can be set for all VRFs or selective VRFs by these commands:

```
mpls label mode vpnv4 all-vrfs per-vrf
```

- If the admin selects the per-vrf mode for the entire system, then all VRFs switches to per-vrf allocation mode except for the VRFs that has been explicitly configured using command mpls label mode vpnv4 vrf WORD per-prefix. Label allocation mode set using specific VRF takes precedence over all-vrf command.

```
mpls label mode vpnv6 vrf WORD per-vrf
```

- If the admin selects per-vrf mode for a particular vrf say vrf1, then only vrf1 switches to per-vrf mode and rest of the vrfs will remain in default allocation mode.

Command Syntax

```
mpls label mode (vpnv4|vpnv6|all-afs) (all-vrfs|vrf WORD) (per-prefix|per-vrf)
no mpls label mode (vpnv4|vpnv6|all-afs) (all-vrfs|vrf WORD) (per-prefix)


mpls label mode 6pe per-prefix
no mpls label mode 6pe per-prefix
```

Parameters

`vrf WORD`	Enter a string to identify the VRF
`all-vrfs`	All the VRFs
`per-prefix`	Unique MPLS labels are allocated per VPN route in a VRF
`per-vrf`	Single MPLS labels are allocated for all VPN routes in a VRF
`all-afs`	All the address families

Default

By default, per-vrf is enabled.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#mpls label mode all-afs all-vrfs per-vrf
```

```
(config)#no mpls label mode all-afs all-vrfs

(config)#mpls label mode 6pe per-prefix

(config)#no mpls label mode 6pe per-prefix
```


© 2021 IP Infusion Inc. Proprietary

mpls local-packet-handling

Use this command to enable the labeling of locally generated TCP packets. All other locally generated packets are not looked at by the MPLS Forwarder

Use the `no` parameter with this command to disable labeling of locally generated TCP packets.

Command Syntax

```
mpls local-packet-handling
```

```
no mpls local-packet-handling
```

Default

By default, mpls local packet handling is disabled

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls local-packet-handling
```

mpls lsp-model

Use this command to configure the MPLS LSP model as Uniform.

Use the `no` parameter with this command to configure the MPLS LSP model as Pipe or short-pipe.

Command Syntax

```
mpls lsp-model uniform
no mpls lsp-model uniform
```

Parameter

None

Default

By default, model configuration is pipe for XGS devices.

Qumran device has following default behavior:

For L3VPN services, model is short-pipe by default and pipe model can be achieved by configuring policy-maps with match exp and set queue.

For L2VPN services, short-pipe model is not supported and default model is pipe.

For L2VPN services with rewrite action pop, cos value will always be updated from qos profile irrespective of model.

For L2VPN services without rewrite, uniform model command doesn't take effect until 'qos remark-cos' is configured on egress interface.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls lsp-model uniform
(config)#exit

#configure terminal
(config)#no mpls lsp-model uniform
(config)#exit
```


© 2021 IP Infusion Inc. Proprietary

mpls lsp-stitching

Use this command to stitch the LSP segment for an FEC created via a different label signaling protocol.

Use the `no` form of this command to disable this configuration.

Command Syntax

```
mpls lsp-stitching
no mpls lsp-stitching
```

Parameters

None

Default

By default, MPLS LSP stitching is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Command Example

```
#configure terminal
(config)#mpls lsp-stitching
```

mpls map-route

Use this command to map a prefix to an FEC.

Use the `no` parameter with this command to disable this configuration.

Command Syntax

```
mpls map-route (A.B.C.D/M|A.B.C.D A.B.C.D) (A.B.C.D/M|A.B.C.D A.B.C.D)
no mpls map-route (A.B.C.D/M|A.B.C.D A.B.C.D)
```

Parameters

`A.B.C.D`	IPv4 prefix to map
`A.B.C.D/M`	IPv4 prefix to map, plus mask
`A.B.C.D`	Mask for IPv4 prefix to map
`A.B.C.D/M`	Mask for IPv4 prefix to map, plus mask.
`A.B.C.D`	IPv4 forwarding equivalence class for route to map
`A.B.C.D`	Mask for IPv4 forwarding equivalence class

Default

By default, mpls map-route is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following examples 5.6.7.8/32 is the FEC for an LSP, and 1.2.3.4 is the prefix to be mapped.

```
#configure terminal
(config)#mpls map-route 1.2.3.4/32 5.6.7.8/32

#configure terminal
(config)#mpls map-route 1.2.3.4 255.255.255.255 5.6.7.8 255.255.255.255
```


© 2021 IP Infusion Inc. Proprietary

mpls min-label-value

Use this command to configure minimum and maximum label value for a label space. Use module names (rsvp | ldp | bgp) to configure minimum and maximum label value for module in a label space, minimum and maximum label space value for a module should be within the range of label space being used. After setting minimum and maximum label value for a label space, make sure to bind the label space to an interface.

Use the `no` parameter with this command to use the default minimum and maximum label value for all the label pools.

Note: The system allows label-space range (maximum and minimum label values) changes for interface-specific label spaces only. The platform-wide label-space range cannot be modified.

Note: Only label-space 0 (global) is supported. Any label-space other than 0, is not supported.

Command Syntax

```
mpls (rsvp|ldp|bgp|) min-label-value <16-1048575> max-label-value <16-1048575>
  (label-space <0-60000>|)
no mpls min-label-value max-label-value (label-space <0-60000>|)
no mpls (rsvp|ldp|bgp) (label-space <0-60000>|))
```

Parameters

`rsvp`	Label range value for RSVP
`ldp`	Label range value for LDP
`bgp`	Label range value for BGP
`min-label-value`	Specify the minimum label value
`<16-1048575>`	Minimum size to be used for label pools or protocol range
`max-label-value`	Specify the maximum label value
`<16-1048575>`	Maximum size for all label pools
`label-space`	Label space for which the minimum value needs to be modified
`<0-60000>`	Range for label space

Default

By default, mpls min-label value is 16

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls min-label-value 50000 max-label-value 80000 label-space 0
```

mpls propagate-ttl

Use this command to enable TTL propagation. Enabling TTL propagation causes the TTL value in the IP header to be copied onto the TTL field in the shim header, at the LSP ingress.

Use the `no` parameter with this command to disable TTL propagation.

Command Syntax

```
mpls propagate-ttl
no mpls propagate-ttl
```

Parameters

None

Default

By default, TTL propagation is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls propagate-ttl

#configure terminal
(config)#no mpls propagate-ttl
```


© 2021 IP Infusion Inc. Proprietary

mpls traffic-eng

Use this command to configure a routing command level for MPLS Traffic Engineering (MPLS-TP).

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
mpls traffic-eng (level-1|level-2|router-id)
no mpls traffic-eng (level-1|level-2|router-id)
```

Parameters

`level-1`	Run MPLS-TE only at IS-IS level 1
`level-2`	Run MPLS-TE only at IS-IS level 2
`router-id`	Traffic Engineering stable IP address for system

Command Mode

IS-IS Router mode

Examples

```
#configure terminal
(config)#mpls traffic-eng level-1

(config-router)#no mpls traffic-eng level-1
```

mpls traffic-eng srlg

Use this command to create a Shared Risk Link Group (SRLG). An SRLG uses secondary backup LSPs or Fast Reroute bypass/detour LSPs that minimize the probability of "fate sharing" with the path of the primary LSP.

Use the `no` form of this command to remove an SRLG.

Note: An interface can be part of multiple SRLG groups upto a maximum of 255 SRLG groups.

Any addition or deletion of SRLG value on an interface will not recalculate Primary/Backup. It is advised to configure SRLG values before bringing UP rsvp sessions or clear rsvp sessions after updating SRLG values.

Command Syntax:

```
mpls traffic-eng srlg <0-4294967295>
no mpls traffic-eng srlg <0-4294967295>
```

Parameters

```
<0-4294967295> Risk group number
```

Command Mode

Interface mode

Example

```
#configure terminal
(config)#int eth1
(config-if)#mpls traffic-eng srlg 1
```


© 2021 IP Infusion Inc. Proprietary

ping mpls

Use this command to start sending MPLS request packets using various parameters as defined below. Ping packets can be configured for LDP, RSVP, L2 circuit, VPLS, L3 VPN, or generic FEC types.

Command Syntax

```
ping mpls (ldp A.B.C.D/M|rsvp (tunnel-name NAME|egress A.B.C.D)|l2-circuit (vccv|)
  <1-4294967295> |vpls <1-10000> peer A.B.C.D/M|l3vpn VRFNAME A.B.C.D/M |ipv4
  A.B.C.D/M) ({reply-mode (1|2)|flags|destination A.B.C.D|source A.B.C.D|ttl <1-
  255>|timeout <1-500>|repeat <5-5000>|interval <2-20000>|force-explicit-
  null|detail}|)
ping mpls (ldp A.B.C.D/M|rsvp (tunnel-name NAME|egress A.B.C.D)|l2-circuit (vccv|)
  <1-4294967295> |vpls <1-10000> peer A.B.C.D/M|l3vpn VRFNAME A.B.C.D/M |ipv4
  A.B.C.D/M) ({reply-mode (1|2)|flags|destination A.B.C.D|source A.B.C.D|ttl <1-
  255>|timeout <1-500>|repeat <5-5000>|interval <2-20000>|force-explicit-
  null|detail}|)
ping mpls (l3vpn (VRFNAME A.B.C.D/M X:X::X:X/M source A.B.C.D destination A.B.C.D))
  ({timeout <1-500>|ttl <1-255>|repeat <5-5000>|interval <2-20000>|detail}|)
ping mpls (6pe default X:X::X:X/M source A.B.C.D destination A.B.C.D)) ({timeout
  <1-500>|ttl <1-255>|repeat <5-5000>|interval <2-20000>|detail}|)
```

Parameters

`ldp`	FEC type is LDP
`A.B.C.D/M`	LDP prefix address
`rsvp`	FEC type is RSVP
`tunnel-name`	RSVP tunnel name
`NAME`	Tunnel name string
`egress`	RSVP tunnel egress
`A.B.C.D`	RSVP tunnel egress address
`l2-circuit`	FEC type is L2 circuit
`vccv`	Virtual Circuit Connectivity Verification
`<1-4294967295>`	L2 circuit ID
`vpls`	FEC type is MPLS VPLS (L2-VPN)
`<1-10000>`	VPLS instance ID
`peer`	VPLS peer
`A.B.C.D/M`	VPLS peer address
`l3vpn`	FEC type is MPLS VPN (L3-VPN)
`VRFNAME`	VPN instance name
`A.B.C.D./M`	VPN prefix
`X:X::X:X/M`	VPNv6 prefix
`6pe`	FEC type (6PE)

default	VPN Instance Name (default)
X:X::X:X/M	6PE Prefix
ipv4	FEC type is generic; use for static/SNMP label switched paths
A.B.C.D/M	IPv4 prefix address
reply-mode	Reply mode, one of
1	Do not reply
2	Reply via UDP/IP packet (default)
flags	Validate FEC stack
destination	Destination address
A.B.C.D	IPv4 address of the destination
source	Source address
A.B.C.D	IPv4 address of the source
ttl	Trace packet Time-to-live
<1-255>	Trace packet TTL value
repeat	Repeat sending of ping packets
<5-5000>	Number of pings to send
interval	Interval between ping packets, in milliseconds
<2-20000>	Interval value
timeout	Time to wait before rejecting the probe as a failure, in seconds
<1-500>	Timeout value
force-explicit-null	Force Explicit NULL label
detail	Print detailed output of the ping

Defaults

Default TTL value is 255.

Default timeout value is 60 seconds.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#ping mpls ipv4 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

#ping mpls l2-circuit 3 reply-mode 2 flags destination 127.1.3.4 source 10.10.0.1
ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

#ping mpls l3vpn vrfa 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null
```


© 2021 IP Infusion Inc. Proprietary

```
#ping mpls ldp 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

#ping mpls rsvp egress 1.2.3.5 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

#ping mpls rsvp tunnel-name tun1 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

#ping mpls vpls 2 peer 10.10.0.0 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

Codes:
'!' - Success, 'Q' - request not sent, '.' - timeout,
'x' - Retcode 0, 'M' - Malformed Request, 'm' - Errored TLV,
'N' - LBL Mapping Err, 'D' - DS Mismatch,
'U' - Unknown Interface, 'R' - Transit (LBL Switched),
'B' - IP Forwarded, 'F' No FEC Found, 'f' - FEC Mismatch,
'P' - Protocol Error, 'X' - Unknown code,
'Z' - Reverse FEC Validation Failed

 Type 'Ctrl+C' to abort

! seq_num = 1 200.0.0.1 2.02 ms
! seq_num = 2 200.0.0.1 2.00 ms
! seq_num = 3 200.0.0.1 1.93 ms
! seq_num = 4 200.0.0.1 2.14 ms
! seq_num = 5 200.0.0.1 1.78 ms

Success Rate is 100.00 percent (5/5)
round-trip min/avg/max = 1.78/1.96/2.14
```

rewrite ingress

Use this command to configure a match VLAN action for a service template.

Use the `no` parameter with this command to remove a match VLAN action for a service template.

Command Syntax

```
rewrite ingress (((pop |translate <2-4094>)(|outgoing-tpid (dot1.ad |dot1.q)))|
  (push <2-4094>))
no rewrite ingress (pop |push |translate)
```

Parameters

`pop`	Pop the outer VLAN identifier
`translate`	Translate the outer VLAN identifier
`<2-4094>`	Outer VLAN identifier
`outgoing-tpid`	Outgoing TPID
`dot1.ad`	Set TPID value as 0x88a8
`dot1.q`	Set TPID value as 0x8100
`push`	Push the outer VLAN identifier
`<2-4094>`	Outer VLAN identifier

Command Mode

MPLS SVC mode

Applicability

This command was introduced in OcNOS version 1.3.3, and changed in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#service-template C2
(config-svc)#match double-tag outer-vlan 9 inner-vlan 8
(config-svc)#rewrite ingress translate 7 outgoing-tpid dot1.ad
(config-svc)#exit

(config)#service-template C2
(config-svc)#no rewrite ingress translate
(config-svc)#exit
```


© 2021 IP Infusion Inc. Proprietary

secondary srlg-disjoint

Use this command to set how to avoid the SRLGs (Shared Risk Link Groups) of a protected primary.

A fast-reroute/secondary path for an LSP that is disjoint from the primary ensures that a single point of failure on a particular link does not bring down both the primary and secondary paths in the LSP.

Note: The SRLG option configured in RSVP-TRUNK mode (this command) takes higher preference than the option configured in RSVP router mode (see 'srlg-disjoint').

Use the `no` form of this command to not avoid the SRLGs of a protected interface.

Command Syntax

```
secondary srlg-disjoint (forced|preferred)
no secondary srlg-disjoint
```

Parameters

`forced`	The router does not create the secondary/backup tunnel unless it avoids SRLGs of the primary-path/protected-interface.
`preferred`	With two explicit paths, the first explicit path tries to avoid the SRLGs of the primary-path/ protected interface. If that does not work, the secondary/backup tunne uses the second path (which ignores SRLGs).

Command Mode

RSVP -TRUNK mode

Example

```
#configure terminal
(config)#rsvp-trunk t1
(config-rsvp)# secondary srlg-disjoint forced
```

secondary-priority srlg-disjoint

Use this command to set how to avoid the SRLGs (Shared Risk Link Groups) of a protected primary.

A fast-reroute/secondary path for an LSP that is disjoint from the primary ensures that a single point of failure on a particular link does not bring down both the primary and secondary paths in the LSP.

Note: The SRLG option configured in RSVP-TRUNK mode (this command) takes higher preference than the option configured in RSVP router mode (see the srlg-disjoint command).

Use the `no` form of this command to not avoid the SRLGs of a protected interface.

Command Syntax

```
secondary-priority <1-5> srlg-disjoint (forced|preferred)
no secondary-priority <1-5> srlg-disjoint
```

Parameters

`forced`	The router does not create the secondary/backup tunnel unless it avoids SRLGs of the primary-path/protected-interface.
`preferred`	With two explicit paths, the first explicit path tries to avoid the SRLGs of the primary-path/ protected interface. If that does not work, the secondary/backup tunnel uses the second path (which ignores SRLGs).

Command Mode

RSVP -TRUNK mode

Example

```
#configure terminal
(config)#rsvp-trunk t1
(config-rsvp)# secondary-piority 1 srlg-disjoint forced
```


© 2021 IP Infusion Inc. Proprietary

service-template

Use this command to configure a service template.

Use no form of this command to remove a service template.

Command Syntax

```
service-template NAME
no service-template NAME
```

Parameters

NAME	Name of the customer service template

Defaults

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.3.

Examples

```
#configure terminal
(config)#service-template C1
(config-svc)#
```

service-tpid

Use this command to configure service tpid for the MPLS layer-2 virtual circuit.

Use the no parameter with this command to delete service tpid from the MPLS layer-2 virtual circuit.

Command Syntax

```
service-tpid (dot1.q|dot1.ad|0x9100)
no service-tpid
```

Parameters

`0x9100`	Set tpid value as 0x9100
`dot1.ad`	Set tpid value as 0x88a8
`dot1.q`	Set tpid value as 0x8100

Default

By default, service-tpid is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#service-tpid dot1.ad
```


© 2021 IP Infusion Inc. Proprietary

show mpls

Use this command to display MPLS data.

Command Syntax

```
show mpls
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following subsection displays a variety of `show mpls` commands.

```
#show mpls
Minimum label configured: 16
 Maximum label configured: 1048575
 Per label-space information:
   Label-space 0 is using minimum label: 16 and maximum label: 1048575
   Label-space 2342 is using minimum label: 556 and maximum label: 1048575
 Custom ingress TTL configured: none
 Custom egress TTL configured: none
 Log message detail: none
 Admin group detail: none
 Packets dropped IP:115167, dropped MPLS:0 sent to IP:490943, labeled:0,
switch
d:0

MPLS Differentiated Services Supported Classes data:
CLASS       DSCP_value
  be           000000

MPLS Differentiated Services CLASS to EXP mapping data:
CLASS    DSCP_value     EXP_value
  be      000000           0
#
```

Table 1-250 explains the show command output fields.

Table 1-250: show mpls output field

Field	Description
Packets dropped IP	Displays the number of packets dropped over the internet protocol.
Dropped MPLS	Displays the number of packets dropped over the MPLS.

Table 1-250: show mpls output field

Field	Description
Sent to IP	Displays the number of packets transmitted to the internet protocol.
Labeled	Number of labeled packets in the interface. The MPLS-labeled packets are switched after a label lookup/switch instead of a lookup into the IP table. Labels of pop-and-forward mpls tunnel: P—Pop labels. D—Delegation labels.
Switch	Type of switching on the links needed for the MPLS.
Class	Creates a class map to be used for matching traffic to a specified class, and enters class-map configuration mode.
DSCP Value	The value of the DSCP and DSCP classifier is used for routing Layer 3 packets.
EXP value	Sets the value of the MPLS EXP field on all imposed label entries.

© 2021 IP Infusion Inc. Proprietary

show mpls admin-groups

Use this command to display all configured administrative groups.

Command Syntax

```
show mpls admin-groups
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following sample shows the output of the `show mpls admin-group` command.

```
#show mpls admin-groups
 Admin group detail:
  Value of 0 associated with admin group 'a'
  Value of 1 associated with admin group 'b'
  Value of 2 associated with admin group 'c'
  Value of 4 associated with admin group 'd'
#
```

Table 1-251 explains the show command output fields.

Table 1-251: show mpls admin-groups output field

Field	Description
Admin group detail	Display information about configured Multi Protocol Label Switching (MPLS) administrative groups.

show mpls bandwidth-class

Use this command to view bandwidth class parameters: bandwidth class name; allocated bandwidth; setup hold priority

Command Syntax

```
show mpls bandwidth-class
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
> show mpls bandwidth-class
Bandwidth-class: BW_1
Bandwidth:  6k        Setup-priority: 1  Class-type: 1
```

Table 1-252 explains the show command output fields.

Table 1-252: show mpls bandwidth-class output field

Field	Description
Bandwidth-class	Bandwidth for each class type.
Bandwidth	Bandwidth configured for the active MPLS.
Setup-Priority	The setup priority is compared with other setup priorities for established sessions on the link to determine whether some of them should be preempted to accommodate the new session. Sessions with lower hold priorities are preempted.
Class-type	Bandwidth allocated for the specified class type.

© 2021 IP Infusion Inc. Proprietary

show mpls counters ldp

Use this command to display traffic statistics for FTNs and ILMs configured by LDP.

Command Syntax

```
show mpls counters ldp ((ftn (|A.B.C.D/M)) | (ilm (|A.B.C.D/M)) |)
```

Parameter

`ftn`	FEC-to-NHLFE map counters
`A.B.C.D/M`	FEC prefix
`ilm`	Incoming label map counters
`A.B.C.D/M`	FEC prefix

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.2.

Note: For Qumran, counters are not available for transit nodes.

Examples

```
#show mpls counters ldp
[ FTN statistics ]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+
 1.1.61.0/24        52480       0                    0
 1.1.62.0/24        52481       0                    0
 1.1.63.0/24        52482       0                    0
 1.1.64.0/24        52483       0                    0
 9.9.9.3/32         52485       0                    0

[ ILM statistics ]
+------------------+-----------+-----------+--------------------+--------------------+--------------------+----------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx bytes      |     Tx packets     |      Tx bytes  |
+------------------+-----------+-----------+--------------------+--------------------+--------------------+----------------+
#
```

Table 1-253 explains the show command output fields.

Table 1-253: show mpls counters ldp output field

Field	Description
FTN statistics	Displays the statistics details of FTN.
ILM statistics	Displays the statistics details of ILM.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
In-label	Displays the ingress (incoming interface) label for this segment.

Table 1-253: show mpls counters ldp output field

Field	Description
Out-label	Displays the egress (outgoing interface) label for this segment.
Rx packets	Number of hello packets received from the neighbor.
Rx bytes	Size of hello packets received from the neighbor.
Tx packets	Number of hello packets sent to the neighbor.
Tx bytes	Size of hello packets sent to the neighbor.

© 2021 IP Infusion Inc. Proprietary

show mpls counters rsvp

Use this command to display traffic statistics for LSPs configured by RSVP.

Command Syntax

```
show mpls counters rsvp ((tunnel-name NAME) | (tunnel-id TUNNEL_ID) | (node-role
  (ingress | transit | egress)) |)
```

Parameter

NAME	RSVP tunnel name
TUNNEL_ID	RSVP tunnel identifier
ingress	LSP role is ingress
transit	LSP role is transit
egress	LSP role is egress

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.2.

Note: For Qumran, counters are not available for transit nodes.

Examples

```
#show mpls counters rsvp
Tunnel-id 5001 Extended Tunnel-ID 9.9.9.1 Egress 9.9.9.2
 lsp-name : t1-Primary                                  [Ingress]
 lsp-ingress : 9.9.9.1          lsp-id : 101
 Rx pkts : 0                    Rx bytes : 0
 Tx pkts : 0                    Tx bytes : 0

 lsp-name : t1-Secondary                                [Ingress]
 lsp-ingress : 9.9.9.1          lsp-id : 102
 Rx pkts : 0                    Rx bytes : 0
 Tx pkts : 0                    Tx bytes : 0

Tunnel-id 5002 Extended Tunnel-ID 9.9.9.1 Egress 9.9.9.3
 lsp-name : t2-Primary                                  [Ingress]
 lsp-ingress : 9.9.9.1          lsp-id : 104
 Rx pkts : 0                    Rx bytes : 0
 Tx pkts : 0                    Tx bytes : 0

 lsp-name : t2-Detour                                   [Ingress]
 lsp-ingress : 1.1.49.1         lsp-id : 104
 Rx pkts : 0                    Rx bytes : 0
 Tx pkts : 0                    Tx bytes : 0
```

Table 1-254 explains the show command output fields.

Table 1-254: show mpls counters rsvp output field

Field	Description
Tunnel-id	Tunnel identifier (destination port) for the RSVP session.
Extended Tunnel-ID	Extended Tunnel identifier (destination port) for the RSVP session.
Egress	Egress router is the final MPLS device that removes the last label before packets leave the MPLS network.
lsp-name	Name of the SPRING-TE LSP.
Ingress	The router at the beginning of an LSP. This router encapsulates IP packets with an MPLS Layer 2 frame and forwards it to the next router in the path.
lsp-ingress	The router at the beginning of an LSP.
lsp-id	Specify the generic LSP identifier.
Rx packets	Number of hello packets received from the neighbor.
Rx bytes	Size of hello packets received from the neighbor.
Tx packets	Number of hello packets sent to the neighbor.
Tx bytes	Size of hello packets sent to the neighbor.

© 2021 IP Infusion Inc. Proprietary

show mpls counters static

Use this command to display traffic statistics for statically configured FTNs and ILMs.

Command Syntax

```
show mpls counters static ((ftn (A.B.C.D/M|)) | (ilm (A.B.C.D/M|)) |)
```

Parameter

`ftn`	FEC-to-NHLFE map counters
`A.B.C.D/M`	FEC prefix
`ilm`	Incoming label map counters
`A.B.C.D/M`	FEC prefix

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.2.

Note: For Qumran, counters are not available for transit nodes.

Examples

```
#show mpls counters static
[ FTN statistics ]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+
 192.168.1.0/24     100         0                    0
 192.168.2.0/24     200         0                    0

[ ILM statistics ]
+------------------+-----------+-----------+--------------------+--------------------+--------------------+----------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx bytes      |     Tx packets     |      Tx bytes  |
+------------------+-----------+-----------+--------------------+--------------------+--------------------+----------------+
 0.0.0.0/0          201         n/a         0                    0                    n/a                  n/a
 0.0.0.0/0          101         n/a         0                    0                    n/a                  n/a
 192.168.3.0/24     301         302         0                    0                    0                    0
 192.168.4.0/24     401         402         0                    0                    0                    0
#
```

Table 1-255 explains the show command output fields.

Table 1-255: show mpls counters static output field

Field	Description
FTN statistics	Displays the statistics details of FTN.
ILM statistics	Displays the statistics details of ILM.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
In-label	Displays the ingress (incoming interface) label for this segment.

Table 1-255: show mpls counters static output field

Field	Description
Out-label	Displays the egress (outgoing interface) label for this segment.
Rx packets	Number of hello packets received from the neighbor.
Rx bytes	Size of hello packets received from the neighbor.
Tx packets	Number of hello packets sent to the neighbor.
Tx bytes	Size of hello packets sent to the neighbor.

© 2021 IP Infusion Inc. Proprietary

show mpls cross-connect-table

Use this command to display detailed information for all entries created in the MPLS cross-connect table.

Command Syntax

```
show mpls cross-connect-table
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the show mpls cross-connect-table

```
#show mpls cross-connect-table
  Cross connect ix: 3, in intf: -, in label: 0, out-segment ix: 3
    Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 3, owner: RSVP, out intf: eth1, out label: 16
    Nexthop addr: 10.10.20.80, cross connect ix: 3, op code: Push

  Cross connect ix: 6, in intf: -, in label: 0, out-segment ix: 6
    Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 6, owner: RSVP, out intf: eth1, out label: 17
    Nexthop addr: 10.10.20.80, cross connect ix: 6, op code: Push
#
```

Table 1-256 explains the show command output fields.

Table 1-256: show mpls cross-connect-table output field

Field	Description
Cross connect ix	Displays the table index for the cross-connect.
In intf	Installed as a result of configuring an interface.
In label	Displays the ingress (incoming interface) label for this segment.
Out-segment ix	Displays the outbound segment index.
Owner	Displays the creator of this segment, typically a protocol such as BGP.
Persistent	Displays whether the tunnel is persistent – Yes or No.
Admin Status	Indicates whether the user can administratively disable a peer while still preserving its configuration. Up = Yes, Down = No.

Table 1-256: show mpls cross-connect-table output field

Field	Description
Oper Status	Displays the current status of the cross-connect segment – Up or Down
Nexthop addr	Displays the IP address of the next hop.
Op code	PUSH = Replace the top label with another and then push one or more additional labels onto the label stack SET = Set the next hop label.

© 2021 IP Infusion Inc. Proprietary

show mpls forwarding-table

Use this command to view forwarding table entries.

Command Syntax

```
show mpls forwarding-table (count|)
```

Parameters

count	Count of IPv4 FTNs.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, B - BGP FTN, K - CLI FTN, t -
tunnel
L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code   FEC    FTN-ID   Tunnel-id  Pri  LSP-Type   Out- Label   ELC  Out-Intf  Nexthop
R(t)> 29.29.29.29/32 1  5001 Yes  LSP_DEFAULT 24322  yes
eth2  41.41.41.31
R(t)> 29.29.29.29/32 2   5001 No   LSP_DEFAULT 24322  yes
eth1  69.69.69.42

#show mpls forwarding-table count

-------------------------------------------
Num FTNs         : 3          [UP: 3, INSTALLED: 3]
  Primary FTNs   : 3          [UP: 3, INSTALLED: 3]
  Secondary FTNs : 0          [UP: 0, INSTALLED: 0]
-------------------------------------------
-------------------------------------------
Num  FTNs         : 0          [UP: 0]
  Primary  FTNs   : 0          [UP: 0]
  Secondary  FTNs : 0          [UP: 0]
-------------------------------------------
```

Table 1-257 shows the status codes displayed at the start of a route entry.

Table 1-257: status code output field

Status Code	Field	Description
P	Stale FTN	Stale marked FTN due to on-going Graceful Restart of MPLS module.
B	BGP FTN	FTN entry installed by BGP.
K	CLI FTN	Admin configured Static FTN entry.
L	LDP FTN	FTN entry installed by LDP.
R	RSVP-TE FTN	FTN entry installed by RSVP.
S	SNMP FTN	FTN entry installed via SNMP.
I	IGP-Shortcut	FTN entry installed by IGP shortcut.
U	Unknown FTN	FTN entry installed by unknown module.
O	SR-OSPF FTN	FTN entry installed by OSPF segment-Routing.
I	SR-ISIS FTN	FTN entry installed by ISIS segment-routing.
K	SR-CLI FTN	FTN entry installed by Static Segment Routing.

Table 1-258 explains the show command output fields.

Table 1-258: show mpls forwarding-table output field

Field	Description
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
FTN-ID	FEC-to-NHLFE map counters identification.
Tunnel-ID	Tunnel identification to which packets with this label are going.
Pri	Primary.
LSP-Type	LSP type associated with each interface being protected.
Out-Label	Label received from downstream neighbor for route.
ELC	Whether the RSVP router has Entropy Label Capability.
Out-Intf	Short name of the physical interface through which traffic goes to the protected link.
Nexthop	Displays the IP address of the next hop.
Num FTNs	Number of FEC-to-NHLFE map counters in the interface.
Primary FTNs	Primary FEC-to-NHLFE in the interface.
Secondary FTNs	Secondary FEC-to-NHLFE in the interface.
Num FTNs	Number of FEC-to-NHLFE map counters in protocol.

© 2021 IP Infusion Inc. Proprietary

Table 1-258: show mpls forwarding-table output field

Field	Description
Primary FTNs	Primary FEC-to-NHLFE map counters in protocol.
Secondary FTNs	Secondary FEC-to-NHLFE map counters in protocol.

© 2021 IP Infusion Inc. Proprietary

show mpls ftn-table

Use this command to display FTN (FEC-To-NHLF) table information.

Command Syntax

```
show mpls ftn-table
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls ftn-table
Primary FTN entry with FEC: 5.5.5.5/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0,   Protected LSP id: 0, QoS Resource id: 0, Description: N/A
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: LDP, out intf: p9p1, out label: 3
    Nexthop addr: 40.0.0.2        cross connect ix: 1, op code: Push
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: p8p1, out label: 3
    Nexthop addr: 30.0.0.2        cross connect ix: 3, op code: Push

 Primary FTN entry with FEC: 50.0.0.0/24, id: 6, row status: Active
  Owner: LDP, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0,   Protected LSP id: 0, QoS Resource id: 0, Description: N/A
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: p8p1, out label: 3
    Nexthop addr: 30.0.0.2        cross connect ix: 3, op code: Push
```

Table 1-259 explains the show command output fields.

Table 1-259: show mpls ftn-table output field

Field	Description
Action-type	Packets flow direction in the tunnel.
Exp-bits	Experimental bits (EXP) field is a 3-bit field in the MPLS header.

© 2021 IP Infusion Inc. Proprietary

Table 1-259: show mpls ftn-table output field

Field	Description
Incoming DSCP	Number of incoming packets in the DSCP.
Tunnel ID	Tunnel identifier (destination port) for the session.
Protected LSP ID	Identifier to protect the LSP in the interface.
QoS Resource ID	Resource identifier of the Quality of Service.
Description	Terms and concepts used to describe MPLS.
Matched bytes	Size of the matched packets.
Pkts	Number packets in the interface.
TX bytes	Size of the packets that transmitted to the neighbor.
Cross connect ix	Displays the table index for the cross-connect.
Pushed pkts	Number of hello packets pushed to the neighbor.
in intf	Installed as a result of configuring an interface.
in label	Displays the ingress (incoming interface) label for this segment.
out-segment ix	Displays the outbound segment index.
Persistent	Displays whether the tunnel is persistent – Yes or No.
Admin Status	Indicates whether the user can administratively disable a peer while still preserving its configuration. Up = Yes, Down = No.
Oper Status	Displays the current status of the cross-connect segment – Up or Down.
Out-Label	Label received from downstream neighbor for route.
Out-Intf	Short name of the physical interface through which traffic goes to the protected link.
Nexthop addr	Displays the IP address of the next hop.
OP code	PUSH = Replace the top label with another and then push one or more additional labels onto the label stack. SET = Set the next hop label.
Primary FTN entry with FEC	Primary FTN entry configured for the FEC.
ID	Displays the Opcode that identifies the specific PDU for this entry.
ROW status	Displays the current status of the row.

show mpls ilm-table

Use this command to view Incoming label mapping (ILM) table entries.

Command Syntax

```
show mpls ilm-table (count|)
```

Parameters

`count`	Count of entries in ILM table.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM,T - MPLS-TP

Code  FEC                ILM-ID      In-Label    Out-Label   In-Intf   Out-
Intf     Nexthop                      LSP-Type
  >   63.63.63.63/32     151187      53121       3          N/A      xe6
6.6.6.63                     LSP_DEFAULT
  >   16.16.16.0/24      151186      53120       3          N/A      xe6
6.6.6.63                     LSP_DEFAULT
 K>   N/A               151189      500         N/A        N/A      N/A
127.0.0.1                    LSP_DEFAULT
  >   65.65.65.65/32     151188      53122       3          N/A      xe1
1.1.1.65                     LSP_DEFAULT

#show mpls ilm-table count
-------------------------------------------
Num ILMs          : 4          [UP: 4, INSTALL: 4]
  Swap Entries    : 3          [UP: 3, INSTALL: 3]
  Pop Entries     : 1          [UP: 1, INSTALL: 1]
-------------------------------------------
```

Table 1-257 shows the status codes displayed at the start of a route entry.

Table 1-260: status code output field

Status Code	Field	Description
	Installed ILM	Number of ILM entry installed.
*	Selected ILM	ILM entry selected in the interface.
P	Stale ILM	Stale marked ILM due to on-going graceful restart of MPLS module.

© 2021 IP Infusion Inc. Proprietary

Table 1-260: status code output field

Status Code	Field	Description
K	CLI ILM	Admin configured static ILM entry.
T	MPLS-TP	ILM entry installed by MPLS-TP.

Table 1-250 explains the show command output fields.

Table 1-261: show mpls ilm-table output field

Field	Description
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
ILM-ID	ILM identifier for the session.
LSP-Type	LSP type associated with each interface being protected.
Out-Label	Label received from downstream neighbor for route.
Out-Intf	Short name of the physical interface through which traffic goes to the protected link.
In label	Displays the ingress (incoming interface) label for this segment.
In intf	Installed as a result of configuring an interface.
Nexthop	Displays the IP address of the next hop.
Num ILMs	Number of ILMs in the session.
Swap Entries	Number of packets in the entry.
Pop Entries	Number of POP entries.

© 2021 IP Infusion Inc. Proprietary

show mpls in-segment-table

Use this command to display detailed information about all entries in the Incoming Label Map (also known as in-segment) table.

Command Syntax

```
show mpls in-segment-table
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls in-segment-table
  Owner: RSVP,#of pops: 1, fec: 192.168.0.5/32
    RX bytes:0, pkts:0, TX bytes:0, Swapped pkts:0, Popped pkts:0
LSP Type: ELSP_CONFIG
Class_Exp mapping:
CLASS    DSCP_value     EXP_value
  be      000000           0
     Cross connect ix: 1, in intf: eth0 in label: 52480 out-segment ix: 1
      Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: RSVP, out intf: eth1, out label: 52480
        Nexthop addr: 20.30.0.3        cross connect ix: 1, op code: Swap
     Cross connect ix: 1, in intf: eth0 in label: 52480 out-segment ix: 2
      Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: RSVP, out intf: eth2, out label: 52481
        Nexthop addr: 30.30.0.3        cross connect ix: 1, op code: Swap
#
```

Table 1-262 explains the show command output fields.

Table 1-262: show mpls in-segment-table output field

Field	Description
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
RX bytes	Size of hello packets received from the neighbor.
Pkts	Number packet in the interface.
TX bytes	Size of the packets that transmitted to the neighbor.
Swapped pkts	Number of swapped packets in session.

© 2021 IP Infusion Inc. Proprietary

Table 1-262: show mpls in-segment-table output field

Field	Description
Popped pkts	Number of popped packets in the interface.
LSP-Type	LSP type associated with each interface being protected.
CLASS	Creates a class map to be used for matching traffic to a specified class, and enters class-map configuration mode.
DSCP value	The value of the DSCP and DSCP classifier is used for routing Layer 3 packets.
EXP value	Sets the value of the MPLS EXP field on all imposed label entries.
Cross-connect ix	Displays the table index for the cross-connect.
Out-Label	Label received from downstream neighbor for route.
Out-Intf	Short name of the physical interface through which traffic goes to the protected link.
In label	Displays the ingress (incoming interface) label for this segment.
In intf	Installed as a result of configuring an interface.
Nexthop	Displays the IP address of the next hop.
Out-segment ix	Displays the outbound segment index.
Persistent	Displays whether the tunnel is persistent – Yes or No.
Admin Status	Indicates whether the user can administratively disable a peer while still preserving its configuration. Up = Yes, Down = No.
Oper Status	Displays the current status of the cross-connect segment – Up or Down.
Op code	PUSH = Replace the top label with another and then push one or more additional labels onto the label stack. SET = Set the next hop label.

show mpls l2-circuit

Use this command to view MPLS-TP L2 circuit parameters.

Command Syntax

```
show mpls l2-circuit (detail|)
show mpls l2-circuit NAME (detail|)
```

Parameters

`detail`	Show detailed information
`NAME`	The name of the virtual circuit

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls l2-circuit detail
MPLS Layer-2 Virtual Circuit: vc1, id: 1 PW-INDEX: 1 service-tpid: 8100

Endpoint: 1.1.1.1
Control Word: 0
MPLS Layer-2 Virtual Circuit Group: none
Bound to interface: xe41
Virtual Circuit Type: Ethernet VLAN
Virtual Circuit is configured as Primary
Virtual Circuit is configured as Active
Virtual Circuit is active
Service-template : C1
Match criteria : 10-14, 16-20
```

Table 1-263 explains the show command output fields.

Table 1-263: show mpls l2-circuit output field

Field	Description
MPLS Layer-2 Virtual Circuit	The MPLS virtual circuit on the egress PE router or switch and the specified neighbor, testing the integrity of the Layer 2 circuit between the ingress and egress PE routers or switches.
Endpoint	Endpoint address.
Control Word	Number of control words.
MPLS Layer-2 Virtual Circuit Group	The MPLS virtual circuit group on the egress PE router or switch and the specified neighbor, testing the integrity of the Layer 2 circuit between the ingress and egress PE routers or switches.

© 2021 IP Infusion Inc. Proprietary

Table 1-263: show mpls l2-circuit output field

Field	Description
Bound to interface	A bound service is the server in a client-server interface.
Virtual Circuit Type	Type of virtual circuit in the interface.
Service-template	Service Templates provides a powerful mechanism to configure advanced service-related options.
Match criteria	The match criteria under which redistribution is allowed for the current route-map.

show mpls l2-circuit statistics

Use this command to display MPLS traffic statistics for l2 circuit.

Command Syntax

```
show mpls l2-circuit NAME statistics (access-port|network-port|)
```

Parameters

NAME	Name of L2 circuit
access-port	Displays the access port statistics
network-port	Displays the network port statistics

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls l2-circuit t1 statistics
MPLS Layer-2 Virtual Circuit: t1, id 100        # Virtual circuit name and ID
Access port statistics:
   RX: Input packets : 1000
       Input bytes : 120000
   TX: Output packets : 0
       Output bytes : 0
Network port statistics:
   RX: Input packets : 0
       Input bytes : 0
   TX: Output packets : 1000
       Output bytes : 120000
```

Table 1-264 explains the show command output fields.

Table 1-264: show mpls l2-circuit statistics output field

Field	Description
MPLS Layer-2 Virtual Circuit	The MPLS virtual circuit on the egress PE router or switch and the specified neighbor, testing the integrity of the Layer 2 circuit between the ingress and egress PE routers or switches.
Virtual circuit name and ID	The MPLS virtual circuit identifier on the egress PE router or switch and the specified neighbor, testing the integrity of the Layer 2 circuit between the ingress and egress PE routers or switches.
Access port statistics	Traffic statistics on Access port of VC/VPLS.
Network port statistics	Traffic statistics on Provider port of VC/VPLS.
RX	Number of received packets.

© 2021 IP Infusion Inc. Proprietary

Table 1-264: show mpls l2-circuit statistics output field

Field	Description
Input packets	Number of hello packets received from the neighbor.
Input bytes	Size of hello packets received from the neighbor.
TX	Number of packets transmitted.
Output packets	Number of hello packets sent to the neighbor.
Output bytes	Size of hello packets sent to the neighbor.

show mpls mapped-routes

Use this command to view MPLS mapped routes.

Use the `no` parameter with this command to reset this configuration.

Command Syntax

```
show mpls mapped-routes
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls mapped-routes

Mapped-route        IPv4 FEC            MPLS-TP Tunnel
14.1.2.3/32         N/A                 NH4
```

Table 1-265 explains the show command output fields.

Table 1-265: show mpls mapped-routes output field

Field	Description
Mapped-route	Map the route of the interface.
IPv4	IPv4 address of the neighbor interface.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
MPLS-TP Tunnel	MPLS-TP tunnel can be provisioned between two arbitrary nodes in an MPLS-TP enabled network.

© 2021 IP Infusion Inc. Proprietary

show mpls out-segment-table

Use this command to display detailed information of out-segment entries (also known as NHLFE) table.

Command Syntax

```
show mpls out-segment-table
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls out-segment-table
       Out-segment with ix: 1, owner: RSVP, out intf: eth1, out label: 52480
        Nexthop addr: 20.30.0.3        cross connect ix: 1, op code: Swap
        TX bytes:0, pkts:0, error pkts:0, discard pkts:0

       Out-segment with ix: 2, owner: RSVP, out intf: eth2, out label: 52481
        Nexthop addr: 30.30.0.3        cross connect ix: 1, op code: Swap
        TX bytes:0, pkts:0, error pkts:0, discard pkts:0Zx
```

Table 1-266 explains the show command output fields.

Table 1-266: show mpls out-segment-table output field

Field	Description
Out-segment ix	Displays the outbound segment index.
Out-Label	Label received from downstream neighbor for route.
Out-Intf	Short name of the physical interface through which traffic goes to the protected link.
Nexthop addr	Displays the IP address of the next hop.
Cross-connect ix	Displays the table index for the cross-connect.
Op code	PUSH = Replace the top label with another and then push one or more additional labels onto the label stack. SET = Set the next hop label.
Pkts	Number packet in the interface.
TX bytes	Size of the packets that transmitted to the neighbor.

Table 1-266: show mpls out-segment-table output field

Field	Description
Error pkts	Number of error packets.
Discard pkts	Number of packets discarded in the interface.

© 2021 IP Infusion Inc. Proprietary

show mpls qos-resource

Use this command to display detailed QoS resource information.

Command Syntax

```
show mpls qos-resource IFNAME
```

Parameters

IFNAME	Display the interface name for a QoS resource

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls qos-resource eth1
<*******************************************>
              QOS RESERVED TABLE
<*******************************************>
HOLD PRIORITY : 0

HOLD PRIORITY : 1

HOLD PRIORITY : 2

HOLD PRIORITY : 3

HOLD PRIORITY : 4

HOLD PRIORITY : 5

HOLD PRIORITY : 6

HOLD PRIORITY : 7
<*******************************************>
   QOS AWAITING TABLE (static resources)
<*******************************************>
HOLD PRIORITY : 0

HOLD PRIORITY : 1

HOLD PRIORITY : 2

HOLD PRIORITY : 3

HOLD PRIORITY : 4

HOLD PRIORITY : 5

HOLD PRIORITY : 6
```

```
    HOLD PRIORITY : 7
    TSUP-173>
```

Table 1-267 explains the show command output fields.

Table 1-267: show mpls qos-resource output fields

Field	Description
QOS RESERVED TABLE	FTM/ILM entries for which QOS is reserved.
HOLD PRIORITY	Determines the degree to which an LSP holds onto its session reservation after the LSP has been set up successfully
QOS AWAITING TABLE (static resources)	FTN/ILM entries for which QOS reservation is pending.

© 2021 IP Infusion Inc. Proprietary

show mpls vc-table

Use this command view configured virtual circuit (VC) components

Command Syntax

```
show mpls vc-table
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show mpls vc-table

VC-ID Vlan-ID Inner-Vlan-ID Access-Intf Network-Intf Out Label  Tunnel-Label
Nexthop Status
500     N/A         N/A           eth2          eth1         544        57
N/A    Active
#
```

Table 1-268 explains the show command output fields.

Table 1-268: show mpls vc-table output fields

Field	Description
VC-ID	The virtual circuit ID for the Provider Edge (PE) MPLS.
Vlan-ID	Virtual LAN (VLAN) ID number.
Inner-Vlan-ID	Inner Virtual LAN (VLAN) ID number.
Access-Intf	The Interface Access page provides a method with which to control access to specific areas of the interface.
Network-Intf	A networking interface allows a computer or mobile device to connect to a local area network (LAN) using Ethernet as the transmission mechanism.
Out Label	Label received from downstream neighbor for route.
Tunnel-Label	Used to provide reachability between PE devices.
Nexthop Status	Displays the network status of the next hop.

© 2021 IP Infusion Inc. Proprietary

show mpls vrf

Use this command to display detailed information of all the configured VRF entries. Specify the name of the VRF to display information about a specific VRF entry.

Command Syntax

```
show mpls vrf-table
show mpls vrf-table VRFNAME (count|)
```

Parameters

VRFNAME	Display the MPLS VRF table by its configured name
count	Display the MPLS VRF FTN's count

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show mpls vrf new_vrf count
-----------------------------------------------
Num VRF-FTNs          : 1           [UP: 1, INSTALLED: 1]
-----------------------------------------------
-----------------------------------------------
Num  VRF-FTNs          : 0           [UP: 0]
-----------------------------------------------
```

Table 1-269 explains the show command output fields.

Table 1-269: show vrf-table output fields

Field	Description
Num VRF-FTNs	Number of FEC-to-NHLFE map counters in VRF protocol.
Num VRF-FTNs	Number of VRF FEC-to-NHLFE map counters in protocol.

© 2021 IP Infusion Inc. Proprietary

show mpls vrf-forwarding-table vrf

This CLI can be used to display a tabular output of the VRF forwarding entries received from the remote PE via MPBGP.

Command Syntax

```
show mpls vrf-forwarding-table vrf <VRFNAME>
```

Parameters

VRFNAME	Display the MPLS VRF table by its configured name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.1.

Examples

```
OcNos#show mpls vrf-forwarding-table vrf BEVrf
Owner     FEC                        FTN-ID    Oper-Status    Out-Label    Tunnel-id    NHLFE-id    Out-Intf    Nexthop
BGP       10.143.73.1/32              1          Up            24320        0            19          xe25       10.143.73.1
BGP       10.143.73.10/32             6          Up            25600        0            30          xe4        10.143.73.10
BGP       10.143.169.26/31            2          Up            24320        0            19          xe25       10.143.73.1
BGP       10.143.170.26/31            3          Up            24324        0            28          xe4        10.143.73.6
```

Table 1-270 explains the show command output fields.

Table 1-270: show mpls vrf-forwarding-table vrf output fileds

Field	Description
Owner	Displays the creator of this entry, typically a protocol such as BGP.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
FTN-ID	FEC-to-NHLFE identification.
Oper-Status	Displays the current status of the entry – Up or Down. It will be “UP” if the vrf entry is installed in the forwarder and it will be in “DOWN“ state if the vrf entry is not installed in the forwarder.
Out-Label	Displays the egress label for this FTN.
Tunnel-id	Tunnel identification to which packets of this FTN are going.
NHLFE-id	Next Hop Label Forwarding Entry identification (also known as out-segment entry identification).
Out-Intf	Name of the physical interface through which traffic goes.
Nexthop	Displays the IP address of the next hop.

show running-config interface mpls

Use this command to show the running system status and configuration for an MPLS interface.

Command Syntax

```
show running-config interface IFNAME mpls
```

Parameters

IFNAME	Display information for this interface name

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 mpls

#
```


© 2021 IP Infusion Inc. Proprietary

show running-config mpls

Use this command to show any Multi-Protocol Label Switching (MPLS) related running configuration.

Command Syntax

```
show running-config mpls
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config mpls
!
mpls propagate-ttl
!
!
!
#
```

show running-config service-template

Use this command to show service-template related running configuration.

Command Syntax

```
show running-config service-template
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.2.

Examples

```
OcNOS#sho running-config service-template
!
service-template s2
 match outer-vlan 200
!
service-template s1
 match outer-vlan 100
!
service-template s3
 match outer-vlan 300
!
service-template s4
 match outer-vlan 400
!
```


© 2021 IP Infusion Inc. Proprietary

show running-config vc

Use this command to show any Virtual Private Wire Service (VPWS) related running configuration.

Command Syntax

```
show running-config vc
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.2.

Examples

```
OcNOS#show running-config vc
!
mpls l2-circuit vc1 1 2.2.2.2
!
mpls l2-circuit vc2 3 2.2.2.2
 tunnel-select-policy p1
!
!
interface xe2
 mpls-l2-circuit vc1 service-template s1 primary
 mpls-l2-circuit vc2 service-template s3 primary
!
```

show running-config vpls

Use this command to show any Virtual Private LAN Service (VPLS) related running configuration.

Command Syntax

```
show running-config vpls
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.2.

Examples

```
#show running-config vpls
!
mpls vpls vpls1 2
 signaling ldp
  vpls-type vlan
  vpls-peer 2.2.2.2
  exit-signaling
 exit-vpls
!
mpls vpls vpls2 4
 signaling ldp
  vpls-type vlan
  vpls-peer 2.2.2.2 tunnel-select-policy p1
  exit-signaling
 exit-vpls
!
!
interface xe2
 mpls-vpls vpls1 service-template s2
 mpls-vpls vpls2 service-template s4
!
```


© 2021 IP Infusion Inc. Proprietary

show service-template

Use this command to display information of all or particular service templates.

Command Syntax

```
show service-template (detail|)
show service-template NAME
```

Parameters

detail	Show detailed information
NAME	Name of customer service template

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.3.

Examples

```
#show service-template detail
 Service-template : C2
  Services mapped : -
  Match criteria : 9/8

 Service-template : C1
  Services mapped : -
  Match criteria : 100

 Service-template : C3
  Services mapped : -
  Match criteria : 2-5

#show service-template C1
 Service-template : C1
  Services mapped : -
  Match criteria : 100
```

Table 1-271 explains the show command output fields.

Table 1-271: show service template output fields

Field	Description
Service-template	Creates a service template and enters service template configuration mode.
Services mapped	Used to match the type of services.
Match criteria	Used to approve the identification result or dismiss it.

show vccv statistics

Use this command to display VCCV messages received prior to advertising capability.

Command Syntax

```
show vccv statistics
```

Parameters

None

Command Mode

Privileged mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is the sample output for `show vccv statistics` command.

```
#show vccv statistics
  CC Mismatch Discards - 10
```

Table 1-272 explains the show command output fields.

Table 1-272: show vccv statistics output fields

Field	Description
CC Mismatch Discards	Number of CC mismatch packets received from neighbor discarded.

© 2021 IP Infusion Inc. Proprietary

srlg-disjoint

Use this command to set how to avoid the SRLGs (Shared Risk Link Groups) of a protected primary.

A fast-reroute/secondary path for an LSP that is disjoint from the primary ensures that a single point of failure on a particular link does not bring down both the primary and secondary paths in the LSP.

Note: The SRLG option configured in RSVP-TRUNK mode (see the secondary-priority srlg-disjoint command) takes higher preference than the option configured in RSVP router mode (this command).

Use the `no` form of this command to not avoid the SRLGs of a protected interface.

Command Syntax

```
srlg-disjoint (forced|preferred)
no srlg-disjoint
```

Parameters

`forced`	The router does not create the secondary/backup tunnel unless it avoids SRLGs of the primary-path/protected-interface.
`preferred`	With two explicit paths, the first explicit path tries to avoid the SRLGs of the primary-path/protected interface. If that does not work, the secondary/backup tunnel uses the second path (which ignores SRLGs).

Command Mode

Router RSVP mode

Example

```
#configure terminal
(config)#router rsvp
(config-rsvp)# srlg-disjoint forced
```

trace mpls

Use this command to trace the route traversed by a specified echo request packet in an MPLS protocol. Trace requests can be configured for LDP, RSVP, L2 VC, VPLS, and L3 VPN label switched paths.

```
trace mpls (6pe default X:X::X:X/M|ldp A.B.C.D/M|rsvp (tunnel-name NAME|egress
  A.B.C.D)|l3vpn VRFNAME A.B.C.D/M|ipv4 A.B.C.D/M) ({reply-mode
  (2)|flags|destination A.B.C.D|source A.B.C.D|timeout <1-500>|force-explicit-
  null|detail}|)
```

Parameters

`6pe`	FEC type is 6pe
`default`	VPN Instance Name (default)
`X:X::X:X/M`	6pe prefix address
`ldp`	FEC type is LDP
`A.B.C.D/M`	LDP prefix address
`rsvp`	FEC type is RSVP
`tunnel-name`	RSVP tunnel name
`NAME`	Tunnel name string
`egress`	RSVP tunnel egress
`A.B.C.D`	RSVP tunnel egress address
`l3vpn`	FEC type is MPLS VPN (L3-VPN)
`VRFNAME`	VPN instance name
`A.B.C.D./M`	VPN prefix
`ipv4`	FEC type generic; use for static/SNMP label switched paths
`A.B.C.D/M`	IPv4 prefix address
`X:X::X:X/M`	VPNv6 prefix
`reply-mode`	Reply mode, one of
`2`	Reply via UDP/IP packet (default)
`flags`	Validate FEC stack
`destination`	Destination address
`A.B.C.D`	IPv4 address of the destination
`source`	Source address
`A.B.C.D`	IPv4 address of the source
`timeout`	Time to wait before rejecting the probe as a failure, in seconds
`<1-500>`	Timeout value
`force-explicit-null`	Force Explicit NULL label
`detail`	Print detailed output of the trace probe

© 2021 IP Infusion Inc. Proprietary

Defaults

Default timeout value is 60 seconds.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#trace mpls ipv4 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 timeout 65 detail force-explicit-null

#trace mpls l3vpn vrfa 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3
source 10.10.0.1 timeout 65 detail force-explicit-null

#trace mpls ldp 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 timeout 65 detail force-explicit-null

#trace mpls rsvp egress 1.2.3.5 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 timeout 65 detail force-explicit-null

#trace mpls rsvp tunnel-name tun1 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 timeout 65 detail force-explicit-null
```

tunnel-id

Use this command to configure tunnel identifier for the MPLS transport tunnel to be used for the MPLS layer-2 virtual circuit.

Use the no parameter with this command to delete tunnel identifier from the MPLS layer-2 virtual circuit.

Command Syntax:

```
tunnel-id <1-5000>
no tunnel-id
```

Parameters

<1-5000>	Identifying value for Tunnel-id

Default

By default, tunnel-id is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#tunnel-id 22
```


© 2021 IP Infusion Inc. Proprietary

tunnel-name

Use this command to configure tunnel name for the MPLS transport tunnel to be used for the MPLS layer-2 virtual circuit.

Use the no parameter with this command to delete tunnel name from the MPLS layer-2 virtual circuit.

Command Syntax:

```
tunnel-name NAME
no tunnel-name
```

Parameters

NAME	Identifying name for MPLS Tunnel

Default

By default, tunnel-name is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#tunnel-name pe1-to-pe2
```

tunnel-select-policy

Use this command to configure tunnel selection policy name for the MPLS transport tunnel to be used for the MPLS layer-2 virtual circuit.

Use the no parameter with this command to delete tunnel selection policy name from the MPLS layer-2 virtual circuit.

Command Syntax

```
tunnel-select-policy POLICYNAME
no tunnel-select-policy
```

Parameters

POLICYNAME	Selection policy name for MPLS Tunnel

Default

By default, tunnel-select-policy is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#tunnel-select-policy policy1
```


© 2021 IP Infusion Inc. Proprietary

vccv cc-type

Use this command to configure the VCCV control channel for MPLS layer-2 virtual circuit.

Use the no parameter with this command to disable control channel from MPLS layer-2 virtual circuit.

Command Syntax

```
vccv cc-type (type-1|type-2|type-3)
no vccv cc-type (type-1|type-2|type-3)
```

Parameters

`type-1`	CC Type 1 - PWE3 Control Word with 0001b as first nibble
`type-2`	CC Type 2 - MPLS Router Alert Label
`type-3`	CC Type 3 - MPLS PW Label with TTL == 1

Default

By default, vccv is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)# vccv cc-type type-2
```

vccv cv-type

Use this command to configure the VCCV control verification for MPLS layer-2 virtual circuit.

Use the no parameter with this command to disable control verification from MPLS layer-2 virtual circuit.

Command Syntax:

```
vccv cv-type (type-1|type-2|type-3|type-4)
no vccv cv-type (type-1|type-2|type-3|type-4)
```

Parameters

type-1	BFD IP/UDP-encapsulated for PW Fault Detection only
type-2	BFD IP/UDP-encapsulated for PW Fault Detection and AC/PW Fault Status Signalling
type-3	BFD PW-ACH-encapsulated for PW Fault Detection only
type-4	BFD PW-ACH-encapsulated for PW Fault Detection and AC/PW Fault Status Signalling

Default

By default, vccv is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)# vccv cv-type type-1
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Differentiated Services Commands

This chapter describes the RSVP Differentiated Services (DiffServ) commands.

- map-route A.B.C.D
- override-diffserv
- primary class-to-exp-bit
- primary elsp-signaled
- primary llsp
- secondary map class
- secondary elsp-signaled
- secondary llsp
- show rsvp diffserv-info

map-route A.B.C.D

Use this command to map a IPv4 prefix route onto a trunk. This route is to be used for packets that are mapped to a specific RSVP trunk.

Use the `no` parameter with this command for unmapping routes from specified trunks.

Command Syntax

```
map-route A.B.C.D A.B.C.D
map-route A.B.C.D A.B.C.D CLASS
map-route A.B.C.D/M
map-route A.B.C.D/M CLASS
no map-route A.B.C.D A.B.C.D
no map-route A.B.C.D A.B.C.D CLASS
no map-route A.B.C.D/M
no map-route A.B.C.D/M CLASS
```

Parameters

`A.B.C.D`	Specify the IPV4 address to be mapped.
`A.B.C.D`	Specify a mask to be applied to the address being mapped.
`A.B.C.D/M`	Specify the IPV4 address to be mapped, with mask.
`CLASS`	Specify the DiffServ Class Name (for example, `be`, `ef` etc.) used for selecting incoming IP packets to be mapped to a specified RSVP trunk.

Default

By default, map route A.B.C.D is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#map-route 1.1.2.2/24 be
```


© 2021 IP Infusion Inc. Proprietary

override-diffserv

Use this command to enable the Differentiated Services (Diff-Serv) override configuration.

If a Path message is received without a Diff-Serv object by a Diff-Serv enabled node, it can be interpreted either as a request for an E-LSP (EXP-Inferred-PSC LSP) or as a request for Non-Diff-Serv LSP. This command supports the override option and when configured, the LSR interprets a path message without a Diff-Serv object as a request for Non-Diff-Serv LSP.

Use the `no` parameter with this command disable this feature.

Command Syntax

```
override-diffserv
```

```
no override-diffserv
```

Parameters

None

Default

By default, override diffserv is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router rsvp
(config-router)#override-diffserv
```

primary class-to-exp-bit

Use this command to configure a primary PHB-EXP (Per-Hop Behavior-Experimental) mapping to be used by an E-LSP (EXP-Inferred-PSC LSP). This mapping is different from the node level PHB-EXP mapping.

Use the `no` parameter with this command to remove a PHB-EXP mapping configuration from current E-LSP PHB-EXP mapping.

Command Syntax

```
primary class-to-exp-bit CLASS <0-7>
no primary class-to-exp-bit CLASS <0-7>
```

Parameters

`CLASS`	Specify the DiffServ Class Name (for example, be, ef etc.) used for selecting incoming IP packets to be mapped to a specified RSVP trunk.
`<0-7>`	Exp bit which is to be mapped to this PHB.

Default

By default, primary map class is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary class-to-exp-bit af12 3

(config)#rsvp-trunk T1
(config-trunk)#no primary class-to-exp-bit af12 3
```


© 2021 IP Infusion Inc. Proprietary

primary elsp-signaled

Use this command to configure a primary Diff-Serv (Differentiated Services) explicitly signaled E-LSP (EXP-Inferred-PSC LSP) interface.

The classes 1 to 7 are optional parameters that can be selected from node level PHB-EXP (Per-Hop Behavior) mapping as PHBs, which will then be used for an E-LSP. If you do not specify a class with this command, all classes will be selected for the E-LSP.

Use the no parameter with this command to remove the configuration.

Command Syntax

```
primary elsp-signaled
primary elsp-signaled CLASS1
primary elsp-signaled CLASS1 CLASS2
primary elsp-signaled CLASS1  CLASS2 CLASS3
primary elsp-signaled CLASS1  CLASS2 CLASS3 CLASS4
primary elsp-signaled CLASS1  CLASS2 CLASS3 CLASS4 CLASS5
primary elsp-signaled CLASS1  CLASS2 CLASS3 CLASS4 CLASS5 CLASS6
primary elsp-signaled CLASS1  CLASS2 CLASS3 CLASS4 CLASS5 CLASS6 CLASS7
no primary elsp-signaled
```

Parameter

CLASS<0-7>	Diffserv class alias. e.g.: be, ef, af11, etc.

Default

By default, primary elsp signaled is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary elsp-signaled cs2 cs5 cs6

(config)#rsvp-trunk T1
(config-trunk)#no primary elsp-signaled
```

primary llsp

Use this command to configure a primary Differentiated Services Label-Only-Inferred-PSC (Diff-Serv L-LSP) interface, which will use Diff-Serv Class as its PHB Scheduling Class (PSC).

Use the no parameter with this command to remove the Diff-Serv L-LSP configuration.

Command Syntax

```
primary llsp CLASS
no primary llsp
```

Parameters

CLASS<0-7>	Diffserv class alias. e.g: be, ef, af11, etc.

Default

By default, primary llsp is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on QUMRAN devices.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary llsp cs4

(config)#rsvp-trunk T1
(config-trunk)#no primary llsp
```


© 2021 IP Infusion Inc. Proprietary

secondary map class

Use this command to configure a secondary PHB-EXP (Per-Hop Behavior-Experimental) mapping to be used by an E-LSP (EXP-Inferred-PSC LSP). This mapping is different from the node level PHB-EXP mapping.

Use the no parameter with this command to remove a PHB-EXP mapping configuration from current E-LSP PHB-EXP mapping.

Command Syntax

```
secondary map class-to-exp-bit CLASS  <0-7>
no secondary map class-to-exp-bit CLASS  <0-7>
```

Parameters

CLASS	Diff-Serv class (queue) mapped to the particular PHB. Diffserv class alias e.g: be, ef, af11, etc.
<0-7>	Exp bit that is to be mapped to this PHB.

Default

By default, secondary map class is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary class-to-exp-bit cs4 3

(config)#rsvp-trunk T1
(config-trunk)#no secondary class-to-exp-bit cs4 3
```

secondary elsp-signaled

Use this command to configure a secondary Diff-Serv (Differentiated Services) explicitly signaled E-LSP (EXP-Inferred-PSC LSP) interface. The classes 1 to 7 are optional parameters can be selected from the node level PHB-EXP (Per-Hop Behavior) mapping as PHBs. They will then be used for an E-LSP. If you do not specify a class with this command, all classes will be selected for the E-LSP.

Use the no parameter with this command to remove the configuration.

Command Syntax

```
secondary elsp-signaled
secondary elsp-signaled CLASS1
secondary elsp-signaled CLASS1 CLASS2
secondary elsp-signaled CLASS1 CLASS2 CLASS3
secondary elsp-signaled  CLASS1 CLASS2 CLASS3 CLASS4
secondary elsp-signaled  CLASS1 CLASS2 CLASS3 CLASS4 CLASS5
secondary elsp-signaled CLASS1 CLASS2 CLASS3 CLASS4 CLASS5 CLASS6
secondary elsp-signaled CLASS1 CLASS2 CLASS3 CLASS4 CLASS5 CLASS6 CLASS7
no secondary elsp-signaled
```

Parameters

`CLASS<0-7>`	Diffserv class alias. e.g: be, ef, af11, etc.

Default

By default, secondary elsp signaled is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary elsp-signaled class cs3 cs6 cs2 cs5

(config)#rsvp-trunk T1
(config-trunk)#no secondary elsp-signaled
```


© 2021 IP Infusion Inc. Proprietary

secondary llsp

Use this command to configure a secondary Differentiated Services Label-Only-Inferred-PSC (Diff-Serv L-LSP) interface, which will use Diff-Serv Class as its PHB Scheduling Class (PSC).

Use the no parameter with this command to remove the Diff-Serv L-LSP configuration.

Command Syntax

```
secondary llsp CLASS
no secondary llsp
```

Parameters

CLASS<0-7>	Diffserv class alias. e.g: be, ef, af11, etc.

Default

By default, secondary llsp is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on QUMRAN devices.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary llsp class cs5

(config)#rsvp-trunk T1
(config-trunk)#no secondary llsp
```

show rsvp diffserv-info

Use this command to display node level Differentiated Services (Diff-Serv) configuration information. This information includes the node level PHB-EXP mapping configured for ELSP-signaled LSP.

Command Syntax

```
show rsvp diffserv-info
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Following is a sample output of the `show rsvp diffserv-info` command.

```
#show rsvp diffserv-info
CLASS-EXP mapping:
CLASS    DSCP_value
 c5  101000 0
 be  000000 1
 cs1 001000 2
 cs3 011000 3
 cs2 010000 4
 cs4 100000 5
 cs6 110000 6
 cs7 111000 7
```

Table 2-273 explains the show command output fields.

Table 2-273: show rsvp diffserv-info output fields

Field	Description
CLASS	MPLS class type that corresponds to the DiffServ traffic engineering class.
EXP_value	Exp value is initialized at the ingress routing device only and overrides the rewrite configuration established for that forwarding class.

© 2021 IP Infusion Inc. Proprietary

Label Distribution Protocol Command Reference

Contents

This document contains these chapters:

- Chapter 1, *LDP Commands*
- Chapter 2, *LDP Show Commands*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 LDP Commands

This chapter is a reference for the LDP commands:

- advertise-labels
- advertise-label-for-default-route
- advertisement-mode
- clear ldp adjacency
- clear ldp session
- clear ldp statistics
- clear ldp statistics advertise-labels
- control-mode
- debug ldp advertise-labels
- debug ldp all
- debug ldp dsm
- debug ldp events
- debug ldp fsm
- debug ldp hexdump
- debug ldp inter-area
- debug ldp nsm
- debug ldp packet
- debug ldp usm
- debug ldp vc usm
- disable-ldp
- enable-ldp
- explicit-null
- global-merge-capability
- graceful-restart
- hello-interval
- hold-time
- import-bgp-routes
- inter-area-lsp
- keepalive-interval
- label-retention-mode
- ldp advertisement-mode
- ldp hello-interval
- ldp hold-time
- ldp keepalive-interval
- ldp keepalive-timeout

© 2021 IP Infusion Inc. Proprietary

- ldp label-retention-mode
- ldp multicast-hellos
- ldp-optimization
- loop-detection
- loop-detection-hop-count
- loop-detection-path-vec-count
- mpls ldp-igp sync isis
- mpls ldp-igp sync ospf
- mpls ldp-igp sync-delay
- neighbor
- propagate-release
- pw-status-tlv
- request-labels-for
- request-retry
- request-retry-timeout
- restart ldp graceful
- router ldp
- router-id
- snmp restart ldp
- targeted-peer ipv4
- targeted-peer-hello-interval
- targeted-peer-hold-time
- transport-address ipv4

© 2021 IP Infusion Inc. Proprietary

advertise-labels

Use this command to prevent the distribution of any locally assigned labels.

Use the `no` parameter to enable the distribution of all locally assigned labels to all LDP neighbors.

Command Syntax

```
advertise-labels for any to none
 advertise-labels for PREFIX to (PEER|any)
no advertise-labels for any to none
no advertise-labels for PREFIX to (PEER|any)
```

Parameters

`for`	Specify the permitted destinations
`any`	Specify to permit any locally assigned labels
`PREFIX`	Specify the destinations which have labels are advertised
`to`	Specify the given neighbor
`PEER`	Specify the LDP neighbors which receive these advertisements
`none`	Specify that there are no LDP neighbors

Default

The labels of all destinations are advertised to all LDP neighbors.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#advertise-labels for any to none

#configure terminal
(config)#router ldp
(config-router)#advertise-labels for PREFIX to any

#configure terminal
(config)#router ldp
(config-router)#advertise-labels for PREFIX to PEER
```

advertise-label-for-default-route

Use this command to enable label advertisement for default route.

Use no form to disable the label advertisement for default route.

Command Syntax

```
advertise-label-for-default-route
```

Parameters

None

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-OTN version 4.2.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#advertise-label-for-default-route
```


© 2021 IP Infusion Inc. Proprietary

advertisement-mode

Use this command to set the label advertisement mode for all the interfaces for the current LSR. Specifying `downstream-on-demand` and `downstream-unsolicited` mode affects which LSR initiates mapping requests and mapping advertisements.

This command is a global command used to set the label advertisement mode for all interfaces for the current LSR. The advertisement mode set for a specific interface overrides the value set by this command (see ldp advertisement-mode). Use this command before starting the interface as it closes and restarts all sessions.

Use the `no` parameter to revert to the default advertisement mode value.

Command Syntax

```
advertisement-mode (downstream-on-demand|downstream-unsolicited)
no advertisement-mode (downstream-on-demand|downstream-unsolicited)
```

Parameters

`downstream-on-demand`

Sends label upon request. When a users uses this mode, a router distributes a label to a peer only if there is a pending label request from a peer. The reaction of the downstream router to this request depends on the label advertising mode supported on the next hop. This mode is typically used with the conservative label retention mode.

`downstream-unsolicited`

Sends label without waiting request. This mode distributes labels to peers without waiting for a label request, and is typically used with the liberal label retention mode.

Default

By default, advertisement mode is downstream-unsolicited

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, the LSR will use the downstream-unsolicited advertisement mode for an LDP session on its interfaces.

```
#configure terminal
(config)#router ldp
(config-router)#advertisement-mode downstream-unsolicited
```

clear ldp adjacency

Use this command to clear an adjacency with a specified peer, or to clear all adjacencies for the current LSR.

Command Syntax

```
clear ldp adjacency (A.B.C.D|*)
```

Parameters

`*`	Specify to clear all adjacencies.
`A.B.C.D`	Specify to clear IPv4 address of the peer.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ldp adjacency 123.123.123.33
```


© 2021 IP Infusion Inc. Proprietary

clear ldp session

Use this command to clear a session established with a specified peer, or to clear all sessions for the current LSR.

Command Syntax

```
clear ldp session (A.B.C.D|*)
```

Parameters

`*`	Specify to clear all sessions.
`A.B.C.D`	Specify to clear IPv4 address of the peer.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ldp session 123.123.123.33
```

clear ldp statistics

Use this command to clear LDP statistics. This command clears the count per each operation filtered by an advertisement list.

Command Syntax

```
clear ldp statistics
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ldp statistics
```


© 2021 IP Infusion Inc. Proprietary

clear ldp statistics advertise-labels

Use this command to clear LDP advertise-labels statistics. This command clears the count per each operation filtered by an advertisement list.

Command Syntax

```
clear ldp statistics advertise-labels
clear ldp statistics advertise-labels for PREFIX
clear ldp statistics advertise-labels for PREFIX to PEER
```

Parameters

`advertise-labels`	Specify the IP prefix list of advertise-labels.
`for`	Specify the permitted destinations.
`PREFIX`	Specify the destinations that have their labels advertised.
`to`	Specify the given neighbor.
`PEER`	Specify the LDP neighbors that receive these advertisements.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ldp statistics advertise-labels
```

control-mode

Use this command to set the control mode for label processing. Ordered processing sets the mode to strict chain-of-command; an LSR replies to a request packet from an LSR higher in the chain only after it receives a label from an LSR lower in the chain. Independent processing sets the mode to instant replies.

In independent control mode, each LSR might advertise label mappings to its neighbors at any time. In independent downstream-on-demand mode, an LSR might answer requests for label mappings immediately, without waiting for a label mapping from the next hop. In independent downstream unsolicited mode, an LSR might advertise a label mapping for an Forwarding Equivalence Class (FEC) to its neighbors whenever it is prepared to label-switch that FEC. In independent mode, an upstream label can be advertised before a downstream label is received.

In ordered control mode, an LSR may initiate the transmission of label mapping only for an FEC for which it has a label mapping for the FEC next hop, or for which the LSR is the egress. For each FEC for which the LSR is not the egress and no mapping exists, the LSR must wait until a label from a downstream LSR is received. An LSR may be an egress for some FECs and a non-egress for others. Changes in control mode only affect labels that were sent or received after the change was made.

Use the `no` parameter to revert to default control mode.

Note: Control mode "independent" is supported with advertisement mode "DU" only.
When the advertisement mode is set as "DU", control mode automatically sets to "independent".
Control mode "independent" is not supported with advertisement mode "DOD".
Control mode "ordered" is supported with advertisement mode "DOD" only.
Control mode "ordered" is not supported with advertisement mode "DU".
When the advertisement mode is set as "DOD", control mode automatically sets to "ordered".

Command Syntax

```
control-mode (ordered|independent)
no control-mode
```

Parameters

`independent`	Sets control mode to independent processing.
`ordered`	Sets control mode to ordered processing.

Command Mode

Router mode

Default

By default, control mode is independent

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#control-mode ordered
```


© 2021 IP Infusion Inc. Proprietary

debug ldp advertise-labels

Use this command to enable the debugging of LDP advertise-label events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use `log syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp advertise-labels
```

```
no debug ldp advertise-labels
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp advertise-labels
```

debug ldp all

Use this command to enable the debugging of all LDP events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp all
no debug ldp all
no debug all
undebug all
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp all
```


© 2021 IP Infusion Inc. Proprietary

debug ldp dsm

Use this command to enable the debugging of LDP DSM events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp dsm
```

```
no debug ldp dsm
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp dsm
```

debug ldp events

Use this command to enable the debugging of all LDP events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp events
```

```
no debug ldp events
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp advertise-labels
(config)#debug ldp all
(config)#debug ldp dsm
(config)#debug ldp events
```


© 2021 IP Infusion Inc. Proprietary

debug ldp fsm

Use this command to enable the debugging of LDP FSM events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp fsm
```

```
no debug ldp fsm
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp fsm
```

debug ldp hexdump

Use this command to enable the debugging of LDP hexdump events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp hexdump
```

```
no debug ldp hexdump
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp hexdump
```


© 2021 IP Infusion Inc. Proprietary

debug ldp inter-area

Use this command to enable the debugging of LDP inter-area events.

On using the debug command, the router continues to generate an output until the no parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the log syslog command in configure mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp inter-area
no debug ldp inter-area
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS-OTN version 4.2.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp inter-area
```

debug ldp nsm

Use this command to enable the debugging of LDP NSM events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp nsm
```

```
no debug ldp nsm
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp nsm
```


© 2021 IP Infusion Inc. Proprietary

debug ldp packet

Use this command to enable the debugging of LDP packet events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp packet
debug ldp packet (notification|hello|initialization|keepalive|address|label)
no debug ldp packet
no debug ldp packet (notification|hello|initialization|keepalive|address|label)
```

Parameters

`notification`	Debug LDP notification packets.
`hello`	Debug LDP hello packets.
`initialization`	Debug LDP initialization packets.
`keepalive`	Debug LDP keepalive packets.
`address`	Debug LDP address (withdraw) packets.
`label`	Debug LDP address label packets.

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp packet hello
```

debug ldp usm

Use this command to enable the debugging of LDP USM events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp usm
```

```
no debug ldp usm
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp usm
```


© 2021 IP Infusion Inc. Proprietary

debug ldp vc usm

Use this command to enable the debugging of LDP VC events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp vc dsm
debug ldp vc usm
no debug ldp vc dsm
no debug ldp vc usm
```

Parameters

`dsm`	Debug LDP downstream SM.
`usm`	Debug LDP upstream SM.

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp vc dsm
(config)#debug ldp vc usm
```

disable-ldp

Use this command to disable LDP IPv4 on a specified interface.

This command disables the transmission of Hello packets through the current interface, and clears all created sessions and adjacencies for this interface. Use `disable-ldp` alone to disable only LDP IPv4 on the interface.

Command Syntax

```
disable-ldp (ipv4|)
```

Parameters

`ipv4`	Disables IPv4 on the interface.

Default

By default, disable ldp is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example disables LDP IPv4 on interface eth0.

```
#configure terminal
(config)#interface eth0
(config-if)#disable-ldp
```

The following example disables LDP IPv4 on interface eth0.

```
#configure terminal
(config)#interface eth0
(config-if)#disable-ldp ipv4
```


© 2021 IP Infusion Inc. Proprietary

enable-ldp

Use this command to enable LDP IPv4 on a specified interface. This command enables the transmission of Hello packets through the current interface, so that LDP adjacencies and LDP sessions can be created.

Note: The corresponding interface must be enabled for label-switching using the label-switching command.

Command Syntax

```
enable-ldp ipv4
```

Parameters

None

Default

By default, enable ldp is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example enables LDP IPv4 on interface eth0.

```
#configure terminal
(config)#interface eth0
(config-if)#enable-ldp ipv4
```

explicit-null

Use this command to configure the router to send explicit-null labels for directly connected FECs instead of implicit-null labels. Implicit-nulls are the default labels.

This command controls the label value advertised on the egress router of an LSP. By default, implicit null label (label 3) is advertised for directly connected FECs. LDP advertises an Implicit Null label that causes the previous hop router to perform penultimate hop popping. Use the `explicit null` command to avoid the penultimate router from penultimate hop popping, and to force it to replace the incoming label with the explicit null label.

Note: Do not use this command if the LDP is concurrently used for MPLS/BGP VPNs.

Use the `no` parameter to stop sending explicit-null labels for directly connected FECs and resume sending implicit-null labels for them.

Command Syntax

```
explicit-null
no explicit-null
```

Parameters

None

Default

By default, sends implicit-null labels.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#explicit-null
```


© 2021 IP Infusion Inc. Proprietary

global-merge-capability

Use this command to override the default merge capability setting of all the interfaces for the current LSR.

The merge capability aggregates multiple incoming flows with the same destination address into a single outgoing flow. This reduces the label-space shortage by sharing labels for different flows with the same destination, or the same FEC (Forwarding Equivalence Class).

Use the `no` parameter to revert to the default merge capability settings of all the interfaces for this LSR.

Command Syntax

```
global-merge-capability (merge-capable|non-merge-capable)
no global-merge-capability
```

Parameters

`merge-capable` Maps all incoming labels that are destined for the same FEC to the same outgoing label (this is the Ethernet default.)

`non-merge-capable`

Maps all incoming labels, regardless of destination FEC to unique outgoing labels (this is the non-Ethernet default.)

Default

By default, global merge capability is merge capable.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#global-merge-capability merge-capable
```

graceful-restart

Use this command to enable the Graceful-Restart capability for LDP.

Use the `no` parameter to disable the GR capability for LDP.

Command Syntax

```
graceful-restart full
graceful-restart helper-only
graceful-restart timers max-recovery <15-600>
graceful-restart timers neighbor-liveness <5-300>
no graceful-restart
no graceful-restart timers max-recovery
no graceful-restart timers neighbor-liveness
```

Parameters

`full`	Configuring with full enable the complete GR capability
`helper-only`	Configuring with helper-only enables only helper mode
`timers`	Used to configure the non-default recovery and reconnect timer values.
`max-recovery`	Maximum recovery time
`<15-600>`	Interval until which LDP preserves route after peer restart
`neighbor-liveness`	Neighbor Liveness Time
`<5-300>`	Set the hold timer for a targeted LDP peer

Default

GR capability is not enbabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#router ldp
OcNOS(config-router)#graceful-restart full
OcNOS(config-router)#graceful-restart helper-only
OcNOS(config-router)#graceful-restart timers max-recovery 100
OcNOS(config-router)#graceful-restart timers neighbor-liveness 200
```


© 2021 IP Infusion Inc. Proprietary

hello-interval

Use this command to set the interval after which `hello` packets are sent out.

LDP defines a mechanism for discovering adjacent Label Switching Routers (LSRs) that participate in label switching (adjacencies). Hello messages are sent to the All Routers Multicast Group (224.0.0.2). Whenever a new router comes up, it sends out a hello packet to a specified, multicast address announcing itself to the network. Every router directly connected to the network receives the packet. Receipt of a hello packet from another LSR creates a `hello adjacency` with that LSR. Use this command to specify the interval after which the hello packets will be sent.

Used as a global command, the hello-interval value may be overridden by the hello-interval set on the interface (see ldp hello-interval). For optimum performance, set this value to no more than one-third the value of the hold-time specified.

Use the `no` parameter to revert to default hello interval.

Command Syntax

```
hello-interval <1-21845>
no hello-interval
```

Parameters

`<1-21845>`	Specify the interval in seconds. The default is 5 seconds.

Default

By default, hello interval is 5 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to set the hello-interval value for all interfaces of an LSR.

```
#configure terminal
(config)#router ldp
(config-router)#hello-interval 35

(config-router)#no hello-interval
```

hold-time

Use this command to set the global value for the hold-time after which the LSR rejects adjacencies.

An LSR maintains a record of `hellos` received from peers. `Hold-time` specifies the time an LSR maintains its record of hellos from a peer on not receiving another hello from that peer. A pair of LSRs negotiates the hold-time they use for hellos from each other. Each proposes a hold time value, and the LSR uses the lower of the two hold-time values. The hold-time value set on the interface overrides the hold-time value set by this command (see ldp hold-time). For optimum performance, set this value to no less than three times the value of the hello-interval specified.

Use the `no` parameter to revert to the default hold time.

Command Syntax

```
hold-time <3-65535>
no hold-time
```

Parameters

`<3-65535>`	Specify the hold-time value in seconds.

Default

By default, hold time is 15 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the hold-time value for all interfaces of an LSR.

```
#configure terminal
(config)#router ldp
(config-router)#hold-time 635

(config-router)#no hold-time
```


© 2021 IP Infusion Inc. Proprietary

import-bgp-routes

Use this command to import BGP routes into LDP. BGP routes are not imported into LDP by default.

Use the `no` parameter to flush out all BGP routes currently being used by LDP, and to reject any further BGP specific routing updates from OcNOS.

Command Syntax

```
import-bgp-routes
```

```
no import-bgp-routes
```

Parameters

None

Default

By default, import bgp route is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#import-bgp-routes
```

inter-area-lsp

Use this command to enable creation of inter-area LSPs.

Use the `no` form of the command to disable this configuration.

Command Syntax

```
inter-area-lsp (PREFIX_ACL|)(config-only|)
no inter-area-lsp
```

Parameters

`PREFIX_ACL`	Access-list name for Prefix Based inter-area lsp
`config-only`	Optional. When this option is used, existing LDP sessions are not torn down.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-OTN version 4.2.

Example

```
#configure terminal
(config)#router ldp
(config-router)#inter-area-lsp

#configure terminal
(config)#router ldp
(config-router)#inter-area-lsp config-only

#configure terminal
(config)#router ldp
(config-router)#inter-area-lsp acl1

#configure terminal
(config)#router ldp
(config-router)#inter-area-lsp acl1 config-only
```


© 2021 IP Infusion Inc. Proprietary

keepalive-interval

Use this command to set the global value for the interval after which keep-alive packets are sent out.

Each LSR must send keep-alive messages at regular intervals to its LDP peers to keep the sessions active. The keep-alive interval determines the time interval between successive keep-alive messages. Use this command to set this interval. This value is overridden by the keep-alive interval set on the interface. For optimum performance, set this value to no more than one-third the value of the specified keep-alive time-out value.

Use the `no` parameter to revert to default keep-alive interval.

Command Syntax

```
keepalive-interval <1-21845>
no keepalive-interval
```

Parameters

`<1-21845>`	Specify the value of interval in seconds.

Default

By default, keepalive interval is 10 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the keep-alive timer for all interfaces of an LSR.

```
#configure terminal
(config)#router ldp
(config-router)#keepalive-interval 635

(config-router)#no keepalive-interval
```

keepalive-timeout

Use this command to set the global value for the time-out after which sessions are rejected.

Use this command to set the time period for which an LSR must wait for successive keep-alive messages from LDP peers. The keep-alive time-out value is overridden by the keep-alive time-out set on the interface (see ldp keepalive-timeout). For optimum performance, set this value to no less than three times the value of the specified keep-alive interval value.

Use the `no` parameter to revert to default keep-alive time-out.

Command Syntax

```
keepalive-timeout <3-65535>
no keepalive-timeout
```

Parameters

`<3-65535>`	Specify the time-out value in seconds.

Default

By default, keepalive timeout is 30 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the keep-alive time-out value for all interfaces of an LSR.

```
#configure terminal
(config)#router ldp
(config-router)#keepalive-timeout 635

(config-router)#no keepalive-timeout
```


© 2021 IP Infusion Inc. Proprietary

label-retention-mode

Use this command to set the retention mode to be used for all labels exchanged.

When an LSR receives a label binding for a particular FEC (Forwarding Equivalence Class) from another LSR that is not its next hop for that FEC, it might keep track of such bindings or discard them. Use the `liberal` parameter to retain all labels binding to FEC received from label distribution peers, even if the LSR is not the current next-hop. Use the `conservative` parameter to maintain only the label bindings for valid next-hops in a LSP. Liberal label retention mode allows for quicker adaptation to routing changes, whereas conservative label retention mode requires an LSR to maintain fewer labels.

Note: label-retention-mode "liberal" is supported with advertisement mode "DU" only.
label-retention-mode "liberal" is not supported with advertisement mode "DOD".
When the advertisement mode is set as "DU", label-retention-mode automatically sets to "liberal".
label-retention-mode "conservative" is supported with advertisement mode "DOD" only.
label-retention-mode "conservative" is not supported with advertisement mode "DU".
When the advertisement mode is set as "DOD", label-retention-mode automatically sets to "conservative".

Use the `no` parameter to revert to default retention mode.

Command Syntax

```
label-retention-mode (conservative|liberal)
no label-retention-mode (conservative|liberal)
```

Parameters

`conservative`	Specify to delete all unused labels and FECs.
`liberal`	Specify to retain all labels, regardless of use.

Default

By default, label retention mode is liberal

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the retention mode for all interfaces of an LSR.

```
#configure terminal
(config)#router ldp
(config-router)#label-retention-mode liberal
```

ldp advertisement-mode

Use this command to set the label advertisement mode for an interface for the current LSR to either downstream-on-demand (label is sent only when requested) or downstream-unsolicited (label is sent unrequested). Specifying downstream-on-demand and downstream-unsolicited mode affects which LSR initiates mapping requests and mapping advertisements.

This is an interface-specific command; it overrides the advertisement mode set for an LSR using the advertisement-mode command (see advertisement-mode). Use this command after the advertisement-mode command sets all the interface advertisement modes. In addition, users should use this command before starting the interface, since all affected sessions will be closed and restarted.

Use the `no` parameter to revert to the advertisement mode value set for the main LDP process.

Command Syntax

```
ldp advertisement-mode (downstream-on-demand|downstream-unsolicited)
no ldp advertisement-mode (downstream-on-demand|downstream-unsolicited)
```

Parameters

`downstream-on-demand`

Indicates that the sent label was requested. When a user uses this parameter, a router distributes a label to a peer only if there is a pending label request from a peer. The reaction of the downstream router to this request depends on the label advertising mode supported on the next hop. The downstream-on-demand mode is typically used with the conservative label retention mode.

`downstream-unsolicited`

Indicates that the label was sent unrequested. This parameter distributes labels to peers without waiting for a label request. This mode is typically used with the liberal label retention mode.

Default

By default, ldp advertisement mode is downstream unsolicited mode

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ldp advertisement-mode downstream-on-demand
```


© 2021 IP Infusion Inc. Proprietary

ldp hello-interval

Use this command to set the interval for sending multicast Hello packets via an interface.

LDP defines a mechanism for discovering adjacent Label Switching Routers (LSR) that participate in label switching (adjacencies). Whenever a new router comes up, it sends out a hello packet to a specified, multicast address announcing itself to the network. Every router directly connected to the network receives the packet. Receipt of a hello packet from another LSR creates a hello adjacency with that LSR. Use this command to specify the interval after which the hello packets will be sent.

For optimum performance, set the hello-interval value to no more than one-third the hold-time value.

Note: This command is an interface-specific command and overrides the value set for an LSR using the global hello-interval command.

Use the `no` parameter with this command to revert to the hello-interval value set for the main LDP process.

Command Syntax

```
ldp hello-interval <1-21845>
no ldp hello-interval
```

Parameters

`<1-21845>`	Specify the interval in seconds.

Default

By default, ldp hello interval is 5 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to set the hello-interval for a specific interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ldp hello-interval 635

(config-if)#no ldp hello-interval
```

ldp hold-time

Use this command to set the hold-time value after which the LSR rejects adjacencies.

The hold-time timer is reset every time a hello packet is received from the peer in question. For optimum performance, set this value to no less than three times the hello-interval value.

Note: This command is an interface-specific command, and overrides the value set for an LSR using the global hold-time command.

Use the `no` parameter to revert to the hold-time value set for the main LDP process.

Command Syntax

```
ldp hold-time <3-65535>
no ldp hold-time
```

Parameters

`<3-65535>`	Specify the hold-time value in seconds.

Default

By default, ldp hold time is 15 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the hold-time for a specific interface:

```
#configure terminal
(config)#interface eth0
(config-if)#ldp hold-time 635

(config-if)#no ldp hold-time
```


© 2021 IP Infusion Inc. Proprietary

ldp keepalive-interval

Use this command to set the interval for sending keep-alive messages to the peer in order to maintain a session.

Each LSR must send keep-alive messages at regular intervals to its LDP peers to keep the sessions active. The keep-alive interval determines the time-interval between successive keep-alive messages. This command sets this interval.

Note: This command is an interface-specific command, and overrides the value set for an LSR using the global `keepalive-interval` command.

Use the `no` parameter to revert to the keep-alive interval set for the main LDP process.

Command Syntax

```
ldp keepalive-interval <1-21845>
no ldp keepalive-interval
```

Parameters

`<1-21845>`	Specify the interval in seconds.

Default

By default, ldp keepalive interval is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to set the hello-interval for a specific interface:

```
#configure terminal
(config)#interface eth0
(config-if)#ldp keepalive-interval 635

(config-if)#no ldp keepalive-interval
```

ldp keepalive-timeout

Use this command to set the keep-alive time-out value for rejecting a session with a peer.

Use this command to set the time period for which an LSR must wait for successive keep-alive messages from LDP peers. The keep-alive timer is reset every time a keep-alive packet is received from the peer in question. For optimum performance, set this value to no more than three times the keep-alive interval value.

Note: This command is an interface-specific command and overrides the value set for an LSR using the global `keepalive-timeout` command.

Use the `no` parameter to revert to the keep-alive time-out set for the main LDP process.

Command Syntax

```
ldp keepalive-timeout <3-65535>
no ldp keepalive-timeout
```

Parameters

`<3-65535>`	Specify the value in seconds.

Default

By default, ldp keepalive timeout is 30 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the keep-alive time-out timer for a specific interface:

```
#configure terminal
(config)#interface eth0
(config-if)#ldp keepalive-timeout 635

(config-if)#no ldp keepalive-timeout
```


© 2021 IP Infusion Inc. Proprietary

ldp label-retention-mode

Use this command to set the retention mode to be used for all labels exchanged via the given interface.

When an LSR receives a label binding for a particular FEC (Forwarding Equivalence Class) from another LSR that is not its next hop for that FEC, it might keep track of such bindings or discard them. Use the `liberal` parameter to retain all labels binding to FEC received from label distribution peers, even if the LSR is not the current next-hop. Use the `conservative` parameter to maintain only the label bindings for valid next-hops in a LSP. Liberal label retention mode allows for quicker adaptation to routing changes, whereas conservative label retention mode requires an LSR to maintain fewer labels.

Note: The retention mode value set on the interface (see label-retention-mode) overrides the value set by this command. This command is an interface-specific command, and overrides the setting for an LSR using the global `label-retention-mode` command.

Use the `no` parameter to revert to the retention mode set for the main LDP process.

Command Syntax

```
ldp label-retention-mode (conservative|liberal)
no ldp label-retention-mode (conservative|liberal)
```

Parameters

`conservative`	Specify to delete all unused labels and FECs.
`liberal`	Specify to retain all labels, regardless of use.

Default

By default, ldp label retention mode is liberal

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the label retention mode for a specific interface:

```
#configure terminal
(config)#interface eth0
(config-if)#ldp label-retention-mode liberal
```

© 2021 IP Infusion Inc. Proprietary

ldp multicast-hellos

Use this command to enable multicast hello exchange on a specified interface.

Use the `no` parameter to disable multicast hello exchange. R

Command Syntax

```
ldp multicast-hellos
no ldp multicast-hellos
```

Parameters

None

Default

By default, ldp multicast hello is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ldp multicast-hellos
```


© 2021 IP Infusion Inc. Proprietary

ldp-optimization

This command helps optimize the resetting of an LDP session by enabling the following two scalability features for LDP:

- Resets the session keepalive timer on receipt of a hello message
- Resets the hold timer on receipt of any LDP control message

Use the `no` parameter to disable the two previously listed scalability features.

Command Syntax

```
ldp-optimization
no ldp-optimization
```

Parameters

None

Default

By default, ldp optimization is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#ldp-optimization
```

loop-detection

Use this command to enable loop detection on the current LSR. This command detects looping LSPs, and prevent Label Request messages from looping because of non-merge capable LSRs. This loop detection mechanism is useful for networks of non time-to-live (non TTL) decrementing devices that can not allocate resources among traffic flows.

There are two methods supported for the loop detection mechanism: A Hop Count detection system, that is always enabled; and the Path Vector detection system, that can be toggled:

- Hop Count - During the setup of an LSP, the LSP passes a hop count with the LSP setup messages. This hop count is incremented by each node router participating in LSP establishment. If the hop count exceeds the maximum configured value, the LSP setup process is stopped, and a notification message is passed back to the message originator.
- Path Vector - A path vector contains a list of LSR identifiers. This is passed as a part of LSP setup messages. Each LSR participating in the LSP establishment adds its own LSR identifier to the path vector. If an LSR finds its own identifier in the path vector, it drops the message, and sends a message back to the originator.

The use of these messages ensures that a loop is detected while establishing a label switched path and before any data is passed over that LSP.

Use the `no` parameter to disable loop detection.

Command Syntax

```
loop-detection
no loop-detection
```

Parameters

None

Default

By default, loop detection is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#loop-detection
```


© 2021 IP Infusion Inc. Proprietary

loop-detection-hop-count

Use this command to set the loop detection hop count, which determines the maximum hop-count value.

This command sets the maximum hop count value, which specifies the permitted maximum permitted hop-count. An LSR that detects a maximum hop count behaves as if the containing message has traversed a loop. The use of this command ensures that a loop is detected while establishing a label switched path before any data is passed via LSP.

Use the `no` parameter to revert to the default loop detection count

Command Syntax

```
loop-detection-hop-count <1-255>
```

Parameters

`<1-255>`	Indicates the loop detection hop count.

Default

By default, loop detection hop is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#loop-detection-hop-count 128
```

loop-detection-path-vec-count

Use this command to set the loop detection vec (vector) count, which determines the maximum supported path vectors.

This command sets the maximum supported path vectors for loop detection, which specifies the permitted path vector length. An LSR that detects a path vector has reached the maximum length behaves as if the containing message has traversed a loop. This command ensures that a loop is detected while establishing a label switched path before any data is passed over that LSP.

Use the `no` parameter to revert to the default loop detection count

Command Syntax

```
loop-detection-path-vec-count <1-255>
```

Parameters

`<1-255>`	Indicates the loop detection hop count.

Default

By default, loop detection path vec count is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#loop-detection-path-vec-count 123
```


© 2021 IP Infusion Inc. Proprietary

mpls ldp-igp sync isis

Use this command to enable LDP ISIS synchronization and to set the holddown timer for synchronization.

Use the `no` parameter to disable the LDP ISIS synchronization.

Note: Holddown timer value should be higher than LDP IGP sync timer.

Command Syntax

```
mpls ldp-igp sync isis (level-1|level-2|level-1-2) (holddown-timer <1-2147483>| )
```

Parameters

`level-1|level-2|level-1-2`
The ISIS level.

`holddown-timer` How long IGP should wait for LDP to converge in seconds.

Default

None

Command Mode

Interface configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#int eth 1
#mpls ldp-igp sync isis level-1-2 holddown-timer 500
```

mpls ldp-igp sync ospf

Use this command to enable LDP-OSPF synchronization. This command also provides option to configure the hold-down timer for which OSPF will wait for LDP to converge and advertises Max cost. When the configured time expires, OSPF starts advertising the actual cost in the Router-LSA.

Note: Holddown timer value should be higher than LDP IGP sync timer.

Command Syntax

```
mpls ldp-igp sync ospf (holddown-timer <1-2147483>|)
```

Parameters

`holddown-timer`	Set holddown timer for the OSPF Sync
`<1-2147483>`	Hold down timer in seconds

Default

OSPF waits infinite when no hold-down timer is configured.

Command Mode

Interface configuration mode

Applicability

This command was introduced before OcNOS-OTN version 4.2.

Example

Enabling OSPF-LDP sync in interface eth3

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#int eth3
(config-if)#mpls ldp-igp sync ospf
(config-if)#end
```

Enabling OSPF-LDP sync with holdown-timer enabled

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#int eth3
(config-if)#mpls ldp-igp sync ospf holddown-timer 200
(config-if)#no mpls ldp-igp sync ospf
(config-if)#end
#
```


© 2021 IP Infusion Inc. Proprietary

mpls ldp-igp sync-delay

Use this command to set the time delay for LDP-IGP synchronization.

Use the `no` parameter to disable the time delay.

Command Syntax

```
mpls ldp-igp sync-delay <5-60>
no mpls ldp-igp sync-delay
```

Parameters

`sync-delay`	Time delay for LDP to converge in seconds.
`<5-60>`	Time delay for notification of LDP convergence to IGP, in seconds

Default

If not configured the delay will be 0 seconds.

Command Mode

Interface configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config-if)# interface eth0
(config-if)# mpls ldp-igp sync-delay 15
(config-if)# no mpls ldp-igp sync-delay
```

multicast-hellos

Use this command to enable multicast hello exchange on all interfaces enabled for LDP. This is used for auto-discovery of LDP peers on directly connected networks. This option is enabled by default.

Use the `no` parameter with this command to disable multicast hello exchange.

Command Syntax

```
multicast-hellos
no multicast-hellos
```

Parameters

None

Default

By default, multicast hello is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#multicast-hellos
```


© 2021 IP Infusion Inc. Proprietary

neighbor

Use this command to configure neighbors of LDP.

Use the `no` parameter with this command to unconfigure the LDP neighbor.

Command Syntax

```
neighbor A.B.C.D auth AUTH-TYPE password (0|7) WORD
no neighbor A.B.C.D auth AUTH-TYPE password (0|7)
```

Parameters

`A.B.C.D`	Neighbor address
`auth AUTH-TYPE`	Authentication Type md5
`password`	Set password to the neighbor
`(0|7)`	Password Type
`WORD`	Password

Default

By default, neighbor is disabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#neighbor 1.1.1.1 auth md5 password 0 myPass

(config-router)#no neighbor 1.1.1.1 auth md5 password 0
```

© 2021 IP Infusion Inc. Proprietary

propagate-release

Use this command to propagate the release of labels to downstream routers.

Use the `no` parameter to prevent the propagate-release of labels.

Command Syntax

```
propagate-release
no propagate-release
```

Parameters

None

Default

By default, propagate release is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#propagate-release
```


© 2021 IP Infusion Inc. Proprietary

pw-status-tlv

Use this command to enable the use of the PW Status TLV to signal the pseudowire status.

Use the `no` option with this command to disable the use of the PW Status TLV to signal the pseudowire status.

Command Syntax

```
pw-status-tlv
no pw-status-tlv
```

Parameters

None

Default

By default, pw status tlv is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#pw-status-tlv
```

request-labels-for

Use this command to request labels for the prefixes in the given IP prefix list. LDP request labels for the prefixes only if the valid and exact route is present for that prefix.

Use the no form of this command to disable multicast hello exchange.

Command Syntax

```
request-labels-for prefix-list-ipv4 NAME
no request-labels-for prefix-list-ipv4
```

Parameters

NAME	IPv4 prefix list name

Command Mode

LDP router mode

Applicability

This command was introduced in OcNOS-OTN version 4.2.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#request-labels-for prefix-list-ipv4 myPrefixList
```


© 2021 IP Infusion Inc. Proprietary

request-retry

Use this command to enable the retry of requests once a request for a label has been rejected for a valid reason. This command enables the LSR to send a maximum of five label requests if a label request is rejected by an LDP peer.

Use the `no` parameter to disable the retry of requests.

Command Syntax

```
request-retry
no request-retry
```

Parameters

None

Default

By default, request retry is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#request-retry
```

request-retry-timeout

Use this command to set the interval between retries. Before this time is over, a request is re-sent to a peer. This command changes the interval between request messages that are resent to a peer to account for routing changes.

Use the `no` parameter to revert to the default request-retry time-out set.

Command Syntax

```
request-retry-timeout <1-65535>
no request-retry-timeout
```

Parameter

`<1-65535>`	Specify the interval between retries in seconds.

Default

By default, timeout is 5 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#request-retry-timeout 512

(config-router)#no request-retry-timeout
```


© 2021 IP Infusion Inc. Proprietary

restart ldp graceful

Use this command to restart ldp gracefully.

Command Syntax

```
restart ldp graceful
```

Parameter

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Example

```
OcNOS#restart ldp graceful
% Warning : You may loose ldp configuration, if not saved
 Proceed for graceful restart? (y/n):y
%% Managed module is down or crashed
```

router ldp

This command is used to enter the LDP specific command-line mode in which global attributes for the LDP process can be set. Without this command, the LSR does not perform any LDP operations, such as sending `hello` packets.

Use the `no` parameter with this command to disable this configuration.

Command Syntax

```
router ldp
no router ldp
```

Parameters

None

Default

By default, router ldp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows the change in the prompt after using this `router ldp` command to enter router mode.

```
#configure router
(config)#router ldp
(config-router)#
```


© 2021 IP Infusion Inc. Proprietary

router-id

Use this command to set the router-id to the supplied IP address; the router uses this address to generate the LDP-ID.

OcNOS has three methods to choose the router-id of LDP. The first priority router-id is the configured router-id in router mode (local configured router-id). The second priority router-id is the configured router-id in configure mode (global configured router-id). The lowest priority router-id is chosen by OcNOS among interfaces (global computed router-id).

Use the `no` parameter with this command to revert to using the first IP address configured on the box as the router-id for LDP-ID generation purposes.

Command Syntax

```
router-id A.B.C.D
no router-id A.B.C.D
no router-id
```

Parameter

`A.B.C.D`	Indicates the LDP router ID value.

Default

By default, router id is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure router
(config)#router ldp
(config-router)#router-id 123.123.123.8
```

snmp restart ldp

Use this command to restart SNMP in Label Distribution Protocol (LDP)

Command Syntax

```
snmp restart ldp
```

Parameters

None

Default

By default, snmp restart ldp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart ldp
```


© 2021 IP Infusion Inc. Proprietary

targeted-peer ipv4

Use this command to enter a targeted IPv4 LDP peer mode.

A targeted session is an LDP session between non-directly connected LSRs. Set this command to send a targeted hello messages to specific IP addresses. This command is specific to a targeted IPv4 LDP peer.

Command Syntax

```
targeted-peer ipv4 A.B.C.D
no targeted-peer ipv4 A.B.C.D
```

Parameter

A.B.C.D	Specify the IPv4 address of the targeted peer.

Default

By default, targeted peer IPv4 is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#targeted-peer ipv4 10.10.10.10
(config-router-targeted-peer)#
```

targeted-peer-hello-interval

Use this command to set the interval for sending unicast `hello` packets to targeted peers.

Use the `no` parameter with this command to revert to the default targeted-peer hello-interval value.

Command Syntax

```
targeted-peer-hello-interval <1-21845>
no targeted-peer-hello-interval
```

Parameter

`<1-21845>`	Specify the interval in seconds.

Default

By default, targeted peer hello interval is 15 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#targeted-peer-hello-interval 1
```


© 2021 IP Infusion Inc. Proprietary

targeted-peer-hold-time

Use this command to set the time-out value that is the time that the router waits before rejecting an adjacency with targeted peers.

Use the `no` parameter to revert to the default targeted-peer hold-time value.

Command Syntax

```
targeted-peer-hold-time <3-65535>
no targeted-peer-hold-time
```

Parameter

`<3-65535>`	Specify the interval in seconds.

Default

By default, hold time is 45 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#targeted-peer-hold-time 555

(config-router)#no targeted-peer-hold-time
```

transport-address ipv4

Use this command to configure the IPv4 transport address for a label space.

The transport address is the address used for the TCP session over which LDP is running. Use this command to manually configure the transport address. Transport addresses may either be bound to a loopback interface, or to a physical interface that is bound to the label space in question. A transport address can also be manually configured using the CLI with the loopback address as the transport address.

Note: The CLI accepts only the loopback address to be configured as the transport address.

Use the `no` parameter to stop using the transport address as the IPv4 transport address. If the label space is not specified for either form of this command, a label space of zero is assumed.

Command Syntax

```
transport-address ipv4 A.B.C.D
transport-address ipv4 A.B.C.D ((0)|)
no transport-address ipv4 A.B.C.D
no transport-address ipv4 A.B.C.D LABELSPACE
```

Parameters

`A.B.C.D`	Specify the IPv4 address to be used as the transport address. Only addresses bound to a loopback interface are valid for manual transport address configuration.
`0`	Platform-wide label space (0) is supported.

Default

Transport addresses are chosen for label spaces. By default, the loopback address is selected as the transport address. If a loopback address is not configured, the label space value is examined. The IP address of the interface is bound to the same label space is chosen as the transport address.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure router
(config)#router ldp
(config-router)#transport-address ipv4 10.10.0.5 20
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 LDP Show Commands

This chapter provides an alphabetized reference for each of the LDP commands. It includes the following commands:

- show debugging ldp
- show ldp
- show ldp adjacency
- show ldp advertise-labels
- show ldp downstream
- show ldp fec
- show ldp igp sync
- show ldp lsp
- show ldp mpls-l2-circuit
- show ldp routes
- show ldp session
- show ldp statistics
- show ldp statistics advertise-labels
- show ldp targeted-peers
- show ldp upstream
- show mpls ldp discovery
- show mpls ldp neighbor
- show mpls ldp parameter

© 2021 IP Infusion Inc. Proprietary

show debugging ldp

Use this command to display the status of the debugging of the LDP system.

Command Syntax

```
show debugging ldp
```

Parameter

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show debugging ldp` command.

```
#show debugging ldp
LDP debugging status:
  LDP event debugging is on
  LDP packet debugging is on
  LDP finite state machine debugging is on
  LDP pdu hexdump debugging is on
  LDP downstream state machine debugging is on
  LDP upstream state machine debugging is on
  LDP trunk state machine debugging is on
  LDP QoS debugging is on
  LDP CSPF debugging is on
  LDP VC USM debugging is on
  LDP VC DSM debugging is on
  LDP NSM debugging is on
  LDP Advertise-labels debugging is on
#
```

Table 2-274 explains the show command output fields.

Table 2-274: show debugging ldp output fields details

Field	Description
LDP debugging status	Status of the LDP debugging protocol.

© 2021 IP Infusion Inc. Proprietary

show ldp

Use this command to display basic LDP attributes defined for the current LSR.

Command Syntax

```
show ldp
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is a sample output from the `show ldp` command displaying basic LDP attributes.

```
#show ldp
Router ID                : 20.1.1.1
LDP Version              : 1
Global Merge Capability  : Merge Capable
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode     : Liberal
Label Control Mode       : Independent
Instance Loop Detection  : On
Instance Hop Count Limit : 255
Instance Path Vec Count  : 255
Request Retry            : Off
Propagate Release        : Disabled
Graceful Restart         : Disabled
Hello Interval           : 5
Targeted Hello Interval  : 15
Hold time                : 15
Targeted Hold time       : 45
Keepalive Interval       : 10
Keepalive Timeout        : 30
Request retry Timeout    : 5
Transport Address data   :
Labelspace 0           : 20.1.1.1 (in use)
Import BGP routes        : No
#
```

Table 2-275 explains the show command output fields.

Table 2-275: show ldp output fields details:

Field	Description
Router ID	Router identifier in IP address format for this system.
LDP Version	Details of Link Layer Discovery Protocol (LLDP) version.
Global Merge Capability	Used to override the default merge capability setting of all the interfaces for the current LSR.
Label Advertisement Mode	Used to set the label advertisement mode for an interface for the current LSR to either downstream-on-demand (label is sent only when requested) or downstream-unsolicited (label is sent unrequested).
Label Retention Mode	Used for all labels exchanged via the given interface.
Label Control Mode	LSR generates a local label for a FEC which the router learned from routing table independently from other LSRs.
Loop Detection	Used to enable loop detection on the current LSR.
Loop Detection Count	Indicates the loop detection hop count.
Request Retry	Enables the LSR to send a maximum of five label requests.
Propagate Release	Used to propagate the release of labels to downstream routers.
Hello Interval	Sets the interval for sending unicast hello packets to peers.
Targeted Hello Interval	Sets the interval for sending unicast hello packets to targeted peers.
Hold time	Sets the time-out value to peers.
Targeted Hold time	Sets the time-out value that is the time that the router waits before rejecting an adjacency with targeted peers.
Keepalive Interval	Used to set the interval for sending keep-alive messages to the peer in order to maintain a session.
Keepalive Timeout	Time-out value for rejecting a session with a peer.
Request retry Timeout	Used to set the interval between retries.
Targeted Hello Receipt	Status of the hello receipt.
Transport Address	The transport address is the address used for the TCP session over which LDP is running.
Transport Interface	Interface is used for the TCP session over which LDP is running.
Import BGP routes	Used to import BGP routes into LDP.

© 2021 IP Infusion Inc. Proprietary

show ldp adjacency

Use this command to display all the adjacencies for the current LSR.

Command Syntax

```
show ldp adjacency
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp adjacency` command displaying all the adjacencies for this LSR.

```
#show ldp adjacency
IP AddressInterface NameHoldtimeLDP ID
192.168.3.5eth11510.10.0.18:0
192.168.4.5  eth2   15 10.10.0.18:0
```

Table 2-276 explains the show command output fields.

Table 2-276: show ldp adjacency output fields details

Field	Description
IP Address	IP address of the interface.
Interface Name	Name of the interface.
Hold time	Sets the time-out value to peers.
LDP ID	LDP identifier for this protocol.

show ldp advertise-labels

Use this command to display the IP access list of LDP advertise-labels.

Command Syntax

```
show ldp advertise-labels
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp advertise-labels` command.

```
#show ldp statistics advertise-labels
Advertisement spec:
Prefix list = prefix1; Peer plist = peer1
Deny : Label Mapping = 1
Label Request = 0
```

Table 2-277 explains the show command output fields.

Table 2-277: show ldp advertise-labels output fields details

Field	Description
Advertisement spec	Details of the advertisement spec.
Prefix list	The label is advertised to all peers permitted by the peer plist.
Peer plist	The prefix list permits the prefix and there is a peer plist.

© 2021 IP Infusion Inc. Proprietary

show ldp downstream

Use this command to display the status of all downstream sessions and the label information exchanged.

Command Syntax

```
show ldp downstream
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is an output from the `show ldp downstream` command showing the status of all downstream sessions.

```
#show ldp downstream
Session peer 1.1.1.1:
  FEC                         Nexthop Addr       State            Label
Req.ID   Attr
  20.0.0.0/24                  connected      Established       impl-null  0
  10.0.2.0/24                  connected      Established       impl-null  0
  1.1.1.1/32                    20.0.0.1      Established       impl-null  0
Session peer 3.3.3.3:
  FEC                         Nexthop Addr       State            Label
Req.ID   Attr
  60.0.0.0/24                  connected      Established          52481  0
  50.0.0.0/24                   30.0.0.2      Established       impl-null  0
  30.0.0.0/24                  connected      Established       impl-null  0
  10.0.2.0/24                  connected      Established       impl-null  0
  5.5.5.5/32                    30.0.0.2      Established          52480  0
  3.3.3.3/32                    30.0.0.2      Established       impl-null  0
Session peer 4.4.4.4:
  FEC                         Nexthop Addr       State            Label
Req.ID   Attr
  50.0.0.0/24                  connected      Established          52483  0
  40.0.0.0/24                  connected      Established       impl-null  0
  10.0.2.0/24                  connected      Established       impl-null  0
  5.5.5.5/32                    40.0.0.2      Established          52480  0
  60.0.0.0/24                   40.0.0.2      Established       impl-null  0
  4.4.4.4/32                    40.0.0.2      Established       impl-null  0
Session peer 1.1.1.1:
  FEC                           State             Label     Req.ID    Attr
  60.0.0.0/24                Established           52486        0     None
  4.4.4.4/32                 Established           52484        0     None
  50.0.0.0/24                Established           52483        0     None
  40.0.0.0/24                Established       impl-null        0     None
  30.0.0.0/24                Established       impl-null        0     None
  20.0.0.0/24                Established       impl-null        0     None
```

```
    10.0.2.0/24              Established       impl-null         0     None
    5.5.5.5/32               Established           52482         0     None
    3.3.3.3/32               Established           52481         0     None
    2.2.2.2/32               Established       impl-null         0     None
  Session peer 3.3.3.3:
    FEC                        State              Label     Req.ID    Attr
    60.0.0.0/24              Established           52487         0     None
    4.4.4.4/32               Established           52485         0     None
    1.1.1.1/32               Established           52480         0     None
    40.0.0.0/24              Established       impl-null         0     None
    30.0.0.0/24              Established       impl-null         0     None
    20.0.0.0/24              Established       impl-null         0     None
    10.0.2.0/24              Established       impl-null         0     None
    2.2.2.2/32               Established       impl-null         0     None
  Session peer 4.4.4.4:
    FEC                        State              Label     Req.ID    Attr
    50.0.0.0/24              Established           52483         0     None
    40.0.0.0/24              Established       impl-null         0     None
    30.0.0.0/24              Established       impl-null         0     None
    20.0.0.0/24              Established       impl-null         0     None
    10.0.2.0/24              Established       impl-null         0     None
    3.3.3.3/32               Established           52481         0     None
    2.2.2.2/32               Established       impl-null         0     None
    1.1.1.1/32               Established           52480         0     None
```

Table 2-278 explains the show command output fields.

Table 2-278: show ldp downstream output fields details

Field	Description
Session peer	Used to group and apply the configuration of general session commands to groups of neighbors that share common session configuration elements.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
Nexthop addr	Displays the IP address of the next hop.
State	Displays the current status of the ldp.
Label	Details of the ldp downstream labels.
Req.ID	Request identifier for the protocol.
Attr	The attribute is used to sent to a customer router.

© 2021 IP Infusion Inc. Proprietary

show ldp fec

Use the following command to display all FECs (Forwarding Equivalence Classes) known to this LSR.

Command Syntax

```
show ldp fec
show ldp fec (prefix)
show mpls ldp fec
show mpls ldp fec (prefix|)
```

Parameter

`prefix`	Display prefix FEC information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ldp fec
LSR codes    : E/N - LSR is egress/non-egress for this FEC,
               L - LSR received a label for this FEC,
               > - LSR will use this route for the FEC
FEC                    Code    Session         Out Label       Nexthop Addr
1.1.1.1/32             NL>     1.1.1.1         impl-null       20.0.0.1
2.2.2.2/32             E >     non-existent    none            connected
3.3.3.3/32             NL>     3.3.3.3         impl-null       30.0.0.2
4.4.4.4/32             NL>     4.4.4.4         impl-null       40.0.0.2
5.5.5.5/32             NL>     4.4.4.4         impl-null       40.0.0.2
                       NL>     3.3.3.3         impl-null       30.0.0.2
20.0.0.0/24            NL      1.1.1.1         impl-null       invalid
                       E >     non-existent    none            connected
30.0.0.0/24            NL      3.3.3.3         impl-null       invalid
                       E >     non-existent    none            connected
40.0.0.0/24            NL      4.4.4.4         impl-null       invalid
                       E >     non-existent    none            connected
50.0.0.0/24            NL      4.4.4.4         impl-null       invalid
                       NL>     3.3.3.3         impl-null       30.0.0.2
60.0.0.0/24            NL>     4.4.4.4         impl-null       40.0.0.2
                       NL      3.3.3.3         impl-null       invalid
```

Table 2-279 shows the codes at the end of each route entry that indicate where the route originated.

Table 2-279: Origin Codes

Origin Code	Description	Comments
E/N	Egress/Non-egress	LSR is egress/non-egress for this FEC.
L	LSR	LSR received a label for this FEC.
>		LSR will use this route for the FEC.

Table 2-280 explains the show command output fields.

Table 2-280: show ldp fec output fields details

Field	Description
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
Session	Reports the current session state.
Out Label	Label received from downstream neighbor for route.
Nexthop addr	Displays the IP address of the next hop.

© 2021 IP Infusion Inc. Proprietary

show ldp igp sync

Use the following command to display the LDP synchronization status.

Command Syntax

```
show ldp igp sync
show mpls ldp igp sync
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ldp igp sync
eth1
LDP configured; LDP-IGP Synchronization enabled.
Sync status: sync achieved
Delay timer: Not Configured , Not Running
```

show ldp interface

Table 2-281: show ldp fec output fields details

Field	Description
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
Session	Reports the current session state.
Out Label	Label received from downstream neighbor for route.
Nexthop addr	Displays the IP address of the next hop.

Use this command to display the list of all interfaces on the current LSR, and to indicate whether a given interface is label-switching or not.

Command Syntax

```
show ldp interface
show ldp interface IFNAME
```

Parameter

`IFNAME` Displays the name of the interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following output displays a list of all interfaces on the LSR.

```
#show ldp interface
Interface    LDP Identifier          Label-switching    Merge Capability
eth0         10.10.0.11:0            Disabled           N/A
lo           10.10.0.11:0            Disabled           N/A
eth1         10.10.0.11:0            Enabled            Merge capable
eth2         10.10.0.11:0            Enabled            Merge capable
vmnet1        10.10.0.11:0           Disabled            N/A
```

The following is a sample output from the `show ldp interface IFNAME` command displaying information about the specified interface `eth1`.

```
#show ldp interface eth1
Status                  : Enabled
Primary IP Address      : 192.168.3.4
Interface Type          : Ethernet
Label Merge Capability  : Merge Capable
Hello Interval          : 5
Targeted Hello Interval : 15
Hold Time               : 15
Targeted Hold Time      : 45
```

 © 2021 IP Infusion Inc. Proprietary

```
Keepalive Interval      : 10
Keepalive Timeout       : 30
Advertisement Mode      : Downstream On Demand
Label Retention Mode    : Liberal
Administrative Groups   : myGroup
```

Table 2-282 explains the show command output fields.

Table 2-282: show ldp interface output fields details

Field	Description
Interface	Name of the interface.
LDP Identifier	LDP identifier for this protocol.
Label-switching	Status of the label-switching on interface..
Merge Capability	Used to override the default merge capability setting of all the interfaces.
Status	Status of the ldp interface.
Primary IP Address	Address of the primary Internet protocol in the interface.
Interface Type	Type of interface.
Label Merge Capability	Used to override the default merge capability setting of all the interfaces for the label.
Hello Interval	Sets the interval for sending unicast hello packets to peers.
Targeted Hello Interval	Sets the interval for sending unicast hello packets to targeted peers.
Hold time	Sets the time-out value to peers.
Targeted Hold time	Sets the time-out value that is the time that the router waits before rejecting an adjacency with targeted peers.
Keepalive Interval	Used to set the interval for sending keep-alive messages to the peer in order to maintain a session.
Keepalive Timeout	Time-out value for rejecting a session with a peer.
Label Advertisement Mode	Used to set the label advertisement mode for an interface for the current LSR to either downstream-on-demand (label is sent only when requested) or downstream-unsolicited (label is sent unrequested).
Label Retention Mode	Used for all labels exchanged via the given interface.
Administrative Groups	Administrative group to be used for links.

show ldp lsp

Use this command to display LDP LSP and, optionally, advertise-label information.

Command Syntax

```
show ldp lsp
show ldp lsp prefix detail
show ldp lsp (prefix|detail)
```

Parameter

`prefix`	Displays advertise-label information in addition to LDP LSP information.
`detail`	Displays advertise-label information in addition to LDP LSP information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp lsp prefix detail` command displaying LDP LSP prefix information with advertise-label information.

```
#show ldp lsp prefix detail
Advertisement spec:
    Prefix list = pfx1; Peer plist = pfx1
    Prevent the distribution of any assigned labels

FEC IPV4:1.1.1.0/30 -> 0.0.0.0
  Downstream state: Established Label: impl-null RequestID: 0 Peer:
50.50.50.50
Attr:
  Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:3.3.3.0/30 -> 0.0.0.0
  Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:10.30.0.0/24 -> 0.0.0.0
  Downstream state: Established Label: impl-null RequestID: 0 Peer:
50.50.50.50
Attr:
  Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:50.50.50.50/32 -> 1.1.1.1
  Advert acl(s): Prefix list = pfx1; Peer plist = pfx1
FEC IPV4:55.55.55.55/32 -> 3.3.3.2
  Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:169.254.0.0/16 -> 0.0.0.0
  Downstream state: Established Label: impl-null RequestID: 0 Peer:
50.50.50.50
Attr:
  Advert acl(s): Prevent the distribution of any assigned labels
```

Table 2-283 explains the show command output fields.

© 2021 IP Infusion Inc. Proprietary

Table 2-283: show ldp lsp output fields details

Field	Description
Advertisement spec	Details of the advertisement spec.
Prefix list	The label is advertised to all peers permitted by the peer plist.
Peer plist	The prefix list permits the prefix and there is a peer plist.
Downstream state	Details of the downstream state.
Established Label	LSP established by the Downstream on Demand method of label distribution.
Req.ID	Request identifier for the protocol.
Peer	Details of the peer.
Attr	The attribute is used to sent packets to a customer router.

show ldp mpls-l2-circuit

Use this command to display summarized Layer-2 Virtual Circuit information about all MPLS virtual circuits configured on the current LSR. When the Virtual Circuit ID is specified, this command displays summarized information for the Virtual Circuit matching the specified ID only.

Command Syntax

```
show ldp mpls-l2-circuit
show ldp mpls-l2-circuit <1-4294967295>
show ldp mpls-l2-circuit detail
show ldp mpls-l2-circuit count
show ldp mpls-l2-circuit <1-4294967295> detail
```

Parameter

`<1-4294967295>`	Indicates the virtual circuit ID.
`detail`	Displays detailed LDP information.
`count`	Count of PWs from LDP standpoint.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command displaying summarized information of VID 1000:

```
#show ldp mpls-l2-circuit 1000
Transport Client     VC     Trans    Local       Remote      Destination
VC ID     Binding    State  Type     VC Label    VC Label    Address
1000      eth2       UP     ethernet 640         640         192.168.0.80

#show ldp mpls-l2-circuit
Transport Client     VC     Trans    Local       Remote      Destination
VC ID     Binding    State  Type     VC Label    VC Label    Address
1000      eth2       UP     ethernet 640         640         192.168.0.80
2000      eth3       UP     ethernet 641         648         192.168.0.80
3000      eth4       UP     ethernet 642         645         192.168.0.90
```

The following is a sample output of this command when using the `detail` parameter:

```
#show ldp mpls-l2-circuit detail
vcid: 100, type: ethernet, local groupid: 4, remote groupid: 4 (vc is up)
destination: 10.0.0.2, Peer LDP Ident: 10.0.0.2
Local label: 53120, remote label: 53120
Access IF: eth3, Network IF: eth4
Local MTU: 1500, Remote MTU: 1500
Local Control Word: 0, Remote Control Word: 0
Local PW Status Capability : enabled
```

 © 2021 IP Infusion Inc. Proprietary

```
Remote PW Status Capability : enabled
Current PW Status TLV : enabled
Local PW Status :
Not Forwarding
Remote PW Status :
Not Forwarding
Standby
```

Table 2-284 explains the show command output fields.

Table 2-284: show ldp mpls-l2-circuit output fields details

Field	Description
Transport VC ID	Transport VC identifier for the protocol.
Client Binding	Show whether the interface is client bound and (if bound) with which client.
VC State	State of the VC.
Trans Type	Type of transmit.
Local VC Label	Incoming VC label details.
Remote VC Label	Outgoing VC label details.
Destination Address	Destination IP address for the protocol.
VCid	Address for the VC.
Type	Type of Ethernet interface.
local groupid	Address for the local group.
remote groupid	Address for the remote group.
destination	Destination IP address.
Peer LDP Ident	Identification for the peer LDP.
Local label	Number of Local label
remote label	Number remote label.
Access IF	Map the access port.
Network IF	Map the network port in the interface.
Local MTU	Number of local MTU., Remote MTU - Number of local MTU.
Local Control Word	Number of local control word.
Remote Control Word	Number of local control word.
Local PW Status Capability	PW Status capability of Local end of PW.

Table 2-284: show ldp mpls-l2-circuit output fields details (Continued)

Field	Description
Remote PW Status Capability	PW Status capability of Remote end of PW.
Current PW Status TLV	A data structure used to encode optional information in a data communications protocol.
Local PW Status	PW Status of Local end of PW.
Remote PW Status	PW Status of Remote end of PW.

© 2021 IP Infusion Inc. Proprietary

show ldp routes

Use this command to display LDP routes.

Command Syntax

```
show ldp routes
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ldp routes
Prefix: 0.0.0.0/0   Nexthop: 10.0.2.2   IFINDEX: 2
Prefix: 1.1.1.1/32   Nexthop: 20.0.0.1   IFINDEX: 3
Prefix: 2.2.2.2/32   Nexthop: 0.0.0.0   IFINDEX: 1
Prefix: 3.3.3.3/32   Nexthop: 30.0.0.2   IFINDEX: 4
Prefix: 4.4.4.4/32   Nexthop: 40.0.0.2   IFINDEX: 5
Prefix: 5.5.5.5/32   Nexthop: 30.0.0.2   IFINDEX: 4
                     Nexthop: 40.0.0.2   IFINDEX: 5
Prefix: 20.0.0.0/24   Nexthop: 0.0.0.0   IFINDEX: 3
Prefix: 30.0.0.0/24   Nexthop: 0.0.0.0   IFINDEX: 4
Prefix: 40.0.0.0/24   Nexthop: 0.0.0.0   IFINDEX: 5
Prefix: 50.0.0.0/24   Nexthop: 30.0.0.2   IFINDEX: 4
Prefix: 60.0.0.0/24   Nexthop: 40.0.0.2   IFINDEX: 5
```

Table 2-285 explains the show command output fields.

Table 2-285: show ldp routes output fields details

Field	Description
Prefix	Details of the network address prefix.
Nexthop	Displays the IP address of the next hop.
IFINDEX	Displays an interface index.

show ldp session

Use this command to display sessions established between this LSR and other LSRs.

Command Syntax

```
show ldp session
show ldp session A.B.C.D
show ldp session X:X::X:X
show mpls ldp session
show mpls ldp session A.B.C.D
show mpls ldp session X:X::X:X
```

Parameter

A.B.C.D	IPv4 address of the peer.
X:X::X:X	IPv6 address of the peer.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ldp session 192.168.3.5
Session state         : OPERATIONAL
Session role          : Passive
TCP Connection        : Established
IP Address for TCP    : 192.168.3.5
Interface being used  : eth1
Peer LDP ID           : 10.10.0.18:0
Peer Password : mypwd
Authentication type: MD5
Adjacencies           : 192.168.3.5
                        192.168.4.5
Advertisement mode    : Downstream Unsolicited
Label retention mode  : Liberal
Keepalive Timeout     : 30
Reconnect Interval    : 15
Address List received : 192.168.3.5
                        192.168.4.5
Received Labels :      Fec       Label       Maps To
                       IPV4:10.10.0.0/24    impl-null none
                       IPV4:192.168.3.0/24  impl-null none
                       IPV4:192.168.4.0/24  impl-null none
                       IPV4:192.168.5.0/24  impl-null none
Sent Labels :          Fec                  LabelMaps To
                       IPV4:10.10.0.0/24    impl-null none
                       IPV4:192.168.3.0/24  impl-null none
                       IPV4:192.168.4.0/24  impl-null  none
```


© 2021 IP Infusion Inc. Proprietary

Table 2-286 explains the show command output fields.

Table 2-286: show ldp session output fields details

Field	Description
Session state	Reports the current session state.
Session role	Displays the status of the session role.
TCP Connection	Details of the TCP connection.
IP Address for TCP	Transmission control protocol IP address for the network.
Interface	Name of interface used in the network.
Peer LDP ID	Identifier for the peer LDP.
Peer Password	Credential details for the neighbor.
Authentication type	Type of authentication.
Adjacencies	IP address for the neighbor adjacencies.
Advertisement mode	Details of the advertisement mode.
Label retention mode	Details of the label retention mode.
Keepalive Interval	Used to set the interval for sending keep-alive messages to the peer in order to maintain a session.
Keepalive Timeout	Time-out value for rejecting a session with a peer.
Address List received	List of address that is received from neighbor.
Received Labels	Number of labels received from neighbor session.
Sent Labels	Number of labels transmitted to neighbor session.

© 2021 IP Infusion Inc. Proprietary

show ldp statistics

Use this command to display LDP statistics.

Command Syntax

```
show ldp statistics
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp statistics` command.

```
#show ldp statistics

=========================================================
 LSR ID = 0.0.0.0:0 : TARGETED PEER: 10.10.10.10
=========================================================
  PacketType                      Total
                             Sent       Received
  Notification                 0            0
  Hello                        0            0
  Initialization               0            0
  Keepalive                    0            0
  Address                      0            0
  Address Withdraw             0            0
  Label Mapping                0            0
  Label Request                0            0
  Label Withdraw               0            0
  Label Release                0            0
  Request Abort                0            0
=========================================================
#
```

Table 2-287 explains the show command output fields.

Table 2-287: show ldp statistics output fields details

Field	Description
LSR ID	Identifier of the LSR.
Targeted Peer	Targeted LDP neighbor can improve the label convergence time compared to the convergence time with directly connected LDP peers when there are flapping links.

© 2021 IP Infusion Inc. Proprietary

Table 2-287: show ldp statistics output fields details (Continued)

Field	Description
Packet Type	Type of packet in the interface that has been received or transmitted to the neighbors.
Total	Number of total packets that has been received and transmitted.

show ldp statistics advertise-labels

Use this command to display the count per each operation filtered by an advertisement list.

Command Syntax

```
show ldp statistics advertise-labels
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp statistics advertise-labels` command.

```
#show ldp statistics advertise-labels
Advertisement spec:
    Prefix list = pfx1; Peer plist = pfx1
      Deny : Label Mapping = 2
             Label Request = 0
    Prevent the distribution of any assigned labels
      Deny : Label Mapping = 9
             Label Request = 3
#
```

Table 2-288 explains the show command output fields.

Table 2-288: show ldp statistics advertise-labels output fields details

Field	Description
Advertisement spec	Details of the advertisement spec.
Prefix list	It is an ordered list and entries are evaluated in order of increasing sequence number.
Peer plist	The peer keyword enables the device to receive time requests and used to synchronize itself to the servers specified in the access list.
Label Mapping	Number of label mapping that is denied.
Label Request	Number of label request that is denied.

© 2021 IP Infusion Inc. Proprietary

show ldp targeted-peers

Use this command to display the list of targeted peers configured on the current LSR.

Command Syntax

```
show ldp targeted-peers
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp targeted-peers` command.

```
#show ldp targeted-peers
IP Address          Interface

192.168.201.2       eth1
```

Table 2-289 explains the show command output fields.

Table 2-289: show ldp targeted-peers output fields details

Field	Description
IP Address	Internet protocol address for the interface.
Interface	Name of the interface.

show ldp upstream

Use this command to display the status of all upstream sessions and label information exchanged.

Command Syntax

```
show ldp upstream
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ldp upstream` command showing the status of all upstream sessions.

```
#show ldp upstream
Session peer 1.1.1.1:
  FEC                       State              Label     Req.ID    Attr
  60.0.0.0/24               Established         52486        0     None
  4.4.4.4/32                Established         52484        0     None
  50.0.0.0/24               Established         52483        0     None
  40.0.0.0/24               Established      impl-null       0     None
  30.0.0.0/24               Established      impl-null       0     None
  20.0.0.0/24               Established      impl-null       0     None
  10.0.2.0/24               Established      impl-null       0     None
  5.5.5.5/32                Established         52482        0     None
  3.3.3.3/32                Established         52481        0     None
  2.2.2.2/32                Established      impl-null       0     None
Session peer 3.3.3.3:
  FEC                       State              Label     Req.ID    Attr
  60.0.0.0/24               Established         52487        0     None
  4.4.4.4/32                Established         52485        0     None
  1.1.1.1/32                Established         52480        0     None
  40.0.0.0/24               Established      impl-null       0     None
  30.0.0.0/24               Established      impl-null       0     None
  20.0.0.0/24               Established      impl-null       0     None
  10.0.2.0/24               Established      impl-null       0     None
  2.2.2.2/32                Established      impl-null       0     None
Session peer 4.4.4.4:
  FEC                       State              Label     Req.ID    Attr
  50.0.0.0/24               Established         52483        0     None
  40.0.0.0/24               Established      impl-null       0     None
  30.0.0.0/24               Established      impl-null       0     None
  20.0.0.0/24               Established      impl-null       0     None
  10.0.2.0/24               Established      impl-null       0     None
  3.3.3.3/32                Established         52481        0     None
  2.2.2.2/32                Established      impl-null       0     None
  1.1.1.1/32                Established         52480        0     None
```


© 2021 IP Infusion Inc. Proprietary

Table 2-290 explains the show command output fields.

Table 2-290: show ldp upstream output fields details

Field	Description
Session peer	Details of the session peers.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
State	Reports the current session state.
Label	Number of Label received from upstream neighbor for route.
Req.ID	Requested session identifier for the protocol.
Attr	The attribute is used to sent packets to a customer router.

show mpls ldp discovery

Use this command to display the sources for locally generated LDP Discovery Hello PDUs, and to indicate whether an interface is label-switching.

Command Syntax

```
show mpls ldp discovery
show mpls ldp discovery IFNAME
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls ldp discovery
Interface           LDP Identifier          Label-switching Merge Capability
eth0                10.10.0.11:0            Disabled        N/A
lo                  10.10.0.11:0            Disabled        N/A
eth1                10.10.0.11:0            Enabled         Merge capable
eth2                10.10.0.11:0            Enabled         Merge capable
vmnet1              10.10.0.11:0            Disabled         N/A
```

Table 2-291 explains the show command output fields.

Table 2-291: show ldp discovery output fields details

Field	Description
Interface	Name of the interface.
LDP Identifier	LDP identifier for this protocol.
Label-switching	Status of the label-switching on interface.
Merge Capability	Used to override the default merge capability setting of all the interfaces.

© 2021 IP Infusion Inc. Proprietary

show mpls ldp neighbor

Use this command to display LDP neighbor information.

Command Syntax

```
show mpls ldp neighbor
show mpls ldp neighbor detail
```

Parameter

`detail`	Details for adjacencies.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls ldp neighbor detail
IP Address            Interface Name    Holdtime    LDP ID
192.168.3.5           eth1              15          10.10.0.18:0
192.168.4.5           eth2              15          10.10.0.18:0
```

Table 2-292 explains the show command output fields.

Table 2-292: show mpls ldp neighbor output fields

Field	Description
IP Address	Address of the interface.
Interface Name	Name of the interface.
Holdtime	The amount of time this device waits between SPFs.
LDP ID	Local label space ID. The first four bytes of an LDP ID is a platform IP address called the LDP router ID. The last two bytes are called the local label space ID.

show mpls ldp parameter

Use this command to display LDP configuration parameters.

Command Syntax

```
show mpls ldp parameter
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls ldp parameter
Router ID                 : 0.0.0.0
LDP Version               : 1
Global Merge Capability   : Merge Capable
Label Advertisement Mode  : Downstream Unsolicited
Label Retention Mode      : Liberal
Label Control Mode        : Independent
Instance Loop Detection   : Off
Request Retry             : Off
Propagate Release         : Disabled
Graceful Restart          : Disabled
Hello Interval            : 5
Targeted Hello Interval   : 15
Hold time                 : 15
Targeted Hold time        : 45
Keepalive Interval        : 10
Keepalive Timeout         : 30
Request retry Timeout     : 5
Transport Address data    :
  Labelspace 0            : 192.168.201.2 (not in use)
Import BGP routes         : No
```

Table 2-293 explains the show command output fields.

Table 2-293: show mpls ldp parameters output fields

Field	Description
Router ID	A preferred interface address for LDP router.
LDP Version	Latest LDP version details.

© 2021 IP Infusion Inc. Proprietary

Table 2-293: show mpls ldp parameters output fields

Field	Description
Global Merge Capability	Override the default merge capability setting of all the interfaces.
Label Advertisement mode	Label advertisement mode details in the interface.
Label retention mode	Label retention mode details in the interface.
Label Control Mode	Controls the mode used for handling label binding requests on interfaces.
Instance Loop Detection	Disables the LDP optional loop detection mechanism.
Request Retry	Request causes the target peer to respond with targeted Hello messages.
Propagate Release	Propagate release is disabled in the interface.
Graceful Restart	Graceful Restart (GR) is a mechanisms to prevent routing protocol re-convergence during a processor switchover. Hello Interval - Hello interval sets the interval for sending unicast hello packets to peers.
Targeted Hello Interval	Targeted hello interval sets the interval for sending unicast hello packets to targeted peers.
Hold time	Hold time sets the time-out value to peers.
Targeted Hold time	Time-out value is the time that the router waits before rejecting an adjacency with targeted peers.
Keepalive Interval	Keepalive interval sets the interval for sending keep-alive messages to the peer in order to maintain a session.
Keepalive Timeout	Time-out value for rejecting a session with a peer.
Request retry Timeout	Request for the maximum retry duration (the number of retries times the length of the timeout).
Transport Address data	Transport address advertised in LDP Discovery Hello messages sent on an interface.
Label space	Label used in a label binding is allocated from a set of possible labels called a label space.
Import BGP routes	The BGP Support for IP Prefix Import from Global Table into a VRF Table feature introduces the capability to import IPv4 unicast prefixes from the global routing table into a Virtual Private Network (VPN) routing/forwarding (VRF) instance table using an import route map.

© 2021 IP Infusion Inc. Proprietary

RSVP-TE Command Reference

Contents

This document contains these chapters:

- Chapter 1, *RSVP-TE Commands*
- Chapter 2, *Fast Reroute Commands*
- Chapter 3, *Refresh Reduction Commands*
- Chapter 4, *Differentiated Services Commands*
- Chapter 5, *DiffServ-TE Commands*
- Chapter 6, *Point-to-Multipoint Commands*
- Chapter 7, *Show Commands*

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

CHAPTER 1 RSVP-TE Commands

This chapter describes the RSVP-TE commands.

- A.B.C.D
- clear rsvp session
- clear rsvp trunk
- cspf
- debug rsvp all
- debug rsvp cspf
- debug rsvp events
- debug rsvp fsm
- debug rsvp hexdump
- debug rsvp nsm
- debug rsvp packet
- disable-rsvp
- elsp-signal-map
- enable-rsvp
- explicit-null
- ext-tunnel-id A.B.C.D
- ext-tunnel-id X:X::X:X
- from A.B.C.D
- from X:X::X:X
- graceful-restart
- graceful-restart recovery-time
- graceful-restart restart-time
- hello-interval
- hello-receipt
- hello-timeout
- keep-multiplier
- loop-detection
- map-route A.B.C.D
- map-route X:X::X:X
- neighbor A.B.C.D
- neighbor X:X::X:X

- no-cspf
- no-loop-detection
- no-php
- no-refresh-path-parsing
- no-refresh-path-parsing
- no-refresh-resv-parsing
- php
- primary ADMIN-GROUP-NAMEprimary affinity
- primary bandwidth
- primary cspf
- primary cspf-retry-limit
- primary cspf-retry-timer
- primary filter
- primary hold-priority
- primary hop-limit
- primary label-record
- primary local-protection
- primary no-affinity
- primary no-cspf
- primary no-record
- primary path
- primary policer
- primary record
- primary retry-limit
- primary retry-timer
- primary reuse-route-record
- primary setup-priority
- primary traffic
- refresh-time
- refresh-path-parsing
- refresh-resv-parsing
- restart rsvp graceful
- router rsvp
- rsvp hello-interval
- rsvp hello-receipt
- rsvp hello-timeout

© 2021 IP Infusion Inc. Proprietary

- rsvp keep-multiplier
- rsvp refresh-time
- rsvp-path
- rsvp-trunk
- rsvp-trunk-restart
- secondary ADMIN-GROUP-NAME
- secondary bandwidth
- secondary bandwidth
- secondary cspf
- secondary cspf-retry-limit
- secondary cspf-retry-timer
- secondary filter
- secondary hold-priority
- secondary hop-limit
- secondary label-record
- secondary local-protection
- secondary no-affinity
- secondary no-cspf
- secondary no-record
- secondary path
- secondary policer
- secondary record
- secondary retry-limit
- secondary retry-timer
- secondary reuse-route-record
- secondary setup-priority
- secondary traffic
- snmp restart rsvp
- to A.B.C.D
- to X:X::X:X
- update-type
- X:X::X:X

A.B.C.D

Use this command to configure an explicit IPv4 route sub-object as either loose or strict. A list of sub-objects specifies an explicit route to the egress router for an LSP.

- For the strict type of route addresses, the route taken from the previous router to the current router must be a directly connected path and a message exchanged between the two routers should not pass any intermediate routers. This ensures that routing is enforced on the basis of each link.
- For the loose type of route addresses, the route taken form the previous router to the current router need not be a direct path and a message exchanged between the two routers can pass other routers.

Use the `no` parameter with this command to disable the configuration.

Note: Refer to X:X::X:X to configure an explicit IPv6 route sub-object as either loose or strict.

Command Syntax

```
A.B.C.D
A.B.C.D (loose|strict)
no A.B.C.D
no A.B.C.D (loose|strict)
```

Parameters

`loose`	Make this node loose
`strict`	Make this node strict

Default

By default, A.B.C.D is disabled

Command Mode

Path mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-path mypath
(config-path)#10.10.0.5 strict
```


© 2021 IP Infusion Inc. Proprietary

clear rsvp session

Use this command to reset either all or specified sessions originating from a specific ingress and terminating on the specific egress.

Note: If the affected session originates from the router where the command is issued, it is stopped and started. If the affected session does not originate from the router where the command is issued, it is stopped and deleted.

Command Syntax

```
clear rsvp session TUNNEL-ID LSP-ID INGRESS EGRESS
```

Parameters

`TUNNELID`	Clear tunnel ID sessions
`LSP-ID`	Clear LSP ID sessions
`INGRESS`	Clear ingress sessions
`EGRESS`	Clear egress sessions

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear rsvp session 1 1 1.2.3.4 192.168.1.1
```

clear rsvp trunk

Use this command to clear an RSVP trunk or to clear all RSVP trunks.

Clearing a trunk also kills any session associated with the trunk. This command is useful when a trunk is missing required data such as routing information. When data is missing, the trunk is in an incomplete state, and clearing it correctly re-initializes the session.

Note: If this command is given in the session on the ingress router, the session stops and restarts. If this command is given in the session on the egress router, the session is not cleared.

Command Syntax

Note: Use the following commands to clear standard RSVP Trunks:

```
clear rsvp trunk *
clear rsvp trunk ingress (TRUNKNAME|*)
clear rsvp trunk non-ingress (TRUNKNAME|*)
clear rsvp trunk (TRUNKNAME|*)
clear rsvp trunk (TRUNKNAME|*) primary
clear rsvp trunk (TRUNKNAME|*) secondary
```

Parameters

`*`	Clear all RSVP trunks configured
`TRUNKNAME`	Name of a specific trunk to be cleared
`ingress`	Clear an RSVP ingress trunk
`non-ingress`	Clear an RSVP non-Ingress trunk
`primary`	Clear all primary sessions configured for this trunk
`secondary`	Clear all secondary sessions configured for this trunk

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear rsvp trunk mytrunk
#clear rsvp trunk *
#clear rsvp trunk ingress mytrunk
#clear rsvp trunk ingress *
#clear rsvp trunk non-ingress mytrunk
#clear rsvp trunk non-ingress *
#clear rsvp trunk mytrunk primary
#clear rsvp trunk * primary
#clear rsvp trunk mytrunk secondary
#clear rsvp trunk * secondary
```


© 2021 IP Infusion Inc. Proprietary

cspf

Use this command to enable the use of Constrained Shortest Path First (CSPF) server for all RSVP sessions. If CSPF is turned off globally, it cannot be enabled for any LSP.

The CSPF server computes paths for LSPs that are subject to various constraints such as bandwidth, hop count, administrative groups, priority, and explicit routes. When computing paths for LSPs, CSPF considers not only the topology of the network and the attributes defined for the LSP but also the links. It attempts to minimize congestion by intelligently balancing the network load.

Use the no-cspf command to disable this configuration.

Command Syntax

```
cspf
```

Parameters

None

Default

By default, CSPF server is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows using the `no-cspf` command in Router mode to disable CSPF for all RSVP sessions.

```
#configure terminal
(config)#router rsvp
(config-router)#cspf
```

© 2021 IP Infusion Inc. Proprietary

debug rsvp all

Use this command to enable all debugging options for an RSVP daemon.

Use the `no` parameter with this command to stop logging all debugging information.

Command Syntax

```
debug rsvp (all|)
no debug rsvp (all|)
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp all
```


© 2021 IP Infusion Inc. Proprietary

debug rsvp cspf

Use this command to enable the exchange of debugging messages between the RSVP module and the CSPF module.

Use the `no` parameter with this command to stop logging CSPF debugging information.

Command Syntax

```
debug rsvp cspf
no debug rsvp cspf
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp cspf
```

debug rsvp events

Use this command to enable debugging of events that were generated from an RSVP daemon.

Use the `no` parameter with this command to stop logging RSVP debugging information.

Command Syntax

```
debug rsvp events
no debug rsvp events
```

Parameters

None

Command Mode

Privileged Exec and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp events
```


© 2021 IP Infusion Inc. Proprietary

debug rsvp fsm

Use these commands to enable debugging of events related to RSVP finite state machines (FSM). Commands are available to log debugging information for the egress FSM, the ingress FSM, the transit FSM, the transit upstream FSM, or the transit downstream FSM.

Use the `no` parameter with these commands to stop logging FSM debugging information.

Command Syntax

```
debug rsvp fsm
debug rsvp fsm egress
debug rsvp fsm ingress
debug rsvp fsm transit
debug rsvp fsm transit upstream
debug rsvp fsm transit downstream
no debug rsvp fsm
no debug rsvp fsm egress
no debug rsvp fsm ingress
no debug rsvp fsm transit
no debug rsvp fsm transit upstream
no debug rsvp fsm transit downstream
```

Parameters

None

Command Mode

Privileged Exec and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#debug rsvp fsm transit upstream
```

debug rsvp hexdump

Use this command to enable the hexdump debugging option for an RSVP daemon.

Use the `no` parameter with this command to stop logging hexdump debugging information.

Command Syntax

```
debug rsvp hexdump
no debug rsvp hexdump
```

Parameters

None

Command Mode

Privileged Exec and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp hexdump
```


© 2021 IP Infusion Inc. Proprietary

debug rsvp nsm

Use this command to enable the NSM debugging option for an RSVP daemon.

Use the `no` parameter with this command to stop logging NSM debugging information.

Command Syntax

```
debug rsvp nsm
no debug rsvp nsm
```

Parameters

None

Command Mode

Privileged Exec and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp nsm
```

debug rsvp packet

Use this command to enable packet debugging options for an RSVP daemon. Using the `in` option command enables debugging for incoming packets. Using the `out` option command enables debugging for outgoing packets.

Use the `no` parameter with these commands to stop logging debugging information.

Command Syntax

```
debug rsvp packet
debug rsvp packet in
debug rsvp packet out
no debug rsvp packet
no debug rsvp packet in
no debug rsvp packet out
```

Parameters

None

Command Mode

Privileged Exec and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp packet in
#debug rsvp packet out
```


© 2021 IP Infusion Inc. Proprietary

disable-rsvp

Use this command to disable RSVP message exchange on an interface.

RSVP can be enabled using the enable-rsvp command.

Command Syntax

```
disable-rsvp
```

Parameters

None

Default

By default, RSVP message exchange is disabled on an interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#disable-rsvp
```

elsp-signal-map

Use this command to configure node-level PHB-EXP mapping for e-lsp signaled LSP.

Use the no parameter with this command to remove a PHB-EXP mapping.

Command Syntax

```
elsp-signal-map class <0-7> exp <0-7>
no elsp-signal-map class <0-7> exp <0-7>
```

Parameters

<0-7>	Diffserv class (queue) mapped to a PHB (per-hop behavior)
<0-7>	EXP bit mapped to the PHB

Command Mode

Router mode

Default

By default, elsp signal map is disabled

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router rsvp
(config-router)#elsp-signal-map class 0 exp 1
(config-router)#elsp-signal-map class 1 exp 4
(config-router)#elsp-signal-map class 3 exp 6
(config-router)#no elsp-signal-map class 1 exp 4
```


© 2021 IP Infusion Inc. Proprietary

enable-rsvp

Use this command to enable RSVP message exchange on an interface.

Note: To use this command, the corresponding interface in the NSM needs to be enabled for label-switching using the label-switching command.

See disable-rsvp to undo the effects of this command.

Command Syntax

```
enable-rsvp
```

Parameters

None

Default

By default, RSVP message exchange is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#enable-rsvp
```

explicit-null

Use this command to send explicit-null labels for directly-connected forwarding equivalency classes (FECs) instead of implicit-null labels.

This command controls the label value advertised to an egress router of an LSP. By default, implicit null label (label 3) is advertised for directly connected FECs. If implicit-null label is advertised, the penultimate hop removes the label and sends the packet as a plain IP packet to the egress router. The explicit-null command advertises label 0 and retains the label so the egress router can pop it. For details about usage of explicit-null, please refer to *RFC 3032*.

Use the `no` parameter with this command to stop sending explicit-null labels for directly-connected FECs and resume sending implicit-null labels.

Command Syntax

```
explicit-null
no explicit-null
```

Parameters

None

Default

By default implicit-null labels are advertised.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#explicit-null
```


© 2021 IP Infusion Inc. Proprietary

ext-tunnel-id A.B.C.D

Use this command to configure an extended-tunnel identifier as an IPv4 address. These identifiers are used in RSVP messages. If no extended-tunnel ID is specified, the LSR-ID for the router is used as the extended-tunnel ID for all LSPs. The extended-tunnel ID is a simple way of identifying all LSPs belonging to the same trunk.

Use the `no` parameter with this command to remove a configured extended-tunnel ID.

Command Syntax

```
ext-tunnel-id A.B.C.D
no ext-tunnel-id A.B.C.D
no ext-tunnel-id
```

Parameters

`A.B.C.D`	Extended tunnel identifier for this trunk in IPv4 address format

Default

By default, the LSR-ID of the router is used as the extended-tunnel ID for all sessions.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk t1
(config-trunk)#ext-tunnel-id 10.10.10.30

(config)#rsvp-trunk t1
(config-trunk)#no ext-tunnel-id 10.10.10.30
```

ext-tunnel-id X:X::X:X

Use this command to configure an extended-tunnel identifier as an IPv6 address. These identifiers are used in RSVP messages. If no extended-tunnel ID is specified, the LSR-ID for the router is used as the extended-tunnel ID for all LSPs. The extended-tunnel ID is a simple way of identifying all LSPs belonging to the same trunk.

Use the `no` parameter with this command to remove a configured extended-tunnel ID.

Command Syntax

```
ext-tunnel-id X:X::X:X
no ext-tunnel-id X:X::X:X
no ext-tunnel-id
```

Parameters

`X:X::X:X`	Extended tunnel identifier for this trunk in IPv6 address format

Default

By default, the LSR-ID of the router is used as the extended-tunnel ID for all sessions.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk t1
(config-trunk)#ext-tunnel-id 1:2::3:4


(config)#rsvp-trunk t1
(config-trunk)#no ext-tunnel-id 1:2::3:4
```


© 2021 IP Infusion Inc. Proprietary

from A.B.C.D

Use this command to specify a “from” IPv4 address for the RSVP daemon. This command can be invoked from either the router rsvp mode or from the rsvp-trunk mode. In the RSVP router mode, this command defines the source address as an IPv4 packet sent out by the RSVP daemon. In the RSVP trunk mode, this command indicates a sender’s address in the sender template object that is used in path messages.

Use the `no` parameter with this command to revert to the default settings.

Command Syntax

```
from A.B.C.D
no from A.B.C.D
no from
```

Parameters

`A.B.C.D`	When in trunk mode, this is the IPv4 address of a tunnel ingress node
`A.B.C.D`	When in router mode, this is the loopback IPv4 address

Default

By default, from A.B.C.D is enabled

Command Mode

Router or Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#from 10.10.0.5

#configure terminal
(config)#router rsvp
(config-router)#from 10.10.0.5
```

from X:X::X:X

Use this command to specify a “from” IPv6 address for the RSVP daemon. This command can be invoked from either the router rsvp mode or from the rsvp-trunk mode. In the router rsvp mode, this command defines the source address as an IPv4 packet being sent out by the RSVP daemon. In the rsvp trunk mode, this command indicates a sender’s address in the sender template object that is used in path messages.

Use the `no` parameter with this command to revert to the default settings.

Command Syntax

```
from X:X::X:X
no from X:X::X:X
```

Parameters

`X:X::X:X`	In trunk mode, this is the address of a tunnel ingress
`X:X::X:X`	In router mode, this is the loopback address

Default

By default, from X:X::X:X is enabled

Command Mode

Router or Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk ipv6
(config-trunk)#from 3ffe::3:34

#configure terminal
(config)#router rsvp
(config-router)#from 3ffe::3:34
```


© 2021 IP Infusion Inc. Proprietary

graceful-restart

Use this command to enable RSVP-TE Graceful Restart capability on a router. This is a global parameter. RSVP-TE determines whether or not to send the graceful restart capability object in its hello message. However, this capability also depends on support for graceful restart on the neighbor router.

The following conditions must be met in order to activate RSVP-TE Graceful Restart:

- This command is used on the local router.
- The neighbor router is explicitly set with a neighbor command (refer to either the neighbor A.B.C.Dor neighborX:X::X:X command for details).
- The neighbor router supports Graceful Restart, and it is activated.

Command Syntax

```
graceful-restart
no graceful-restart
```

Parameters

None

Default

Graceful restart is disabled by default

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#graceful-restart
(config-router)#no graceful-restart
```

graceful-restart recovery-time

Use this command to set a recovery time for an RSVP-TE graceful restart configuration.

Use the `no` parameter with this command to reset the recovery time.

Command Syntax

```
graceful-restart recovery-time <60000-3600000>
no graceful-restart recovery-time
```

Parameters

`<60000-3600000>`Recovery time value in milliseconds

Default

Default value is 360000 ms.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#graceful-restart recovery-time 600000
```


© 2021 IP Infusion Inc. Proprietary

graceful-restart restart-time

Use this command to set a restart time for an RSVP-TE graceful restart configuration.

Use the `no` parameter with this command to reset the restart time.

Command Syntax

```
graceful-restart restart-time <10000-600000>
no graceful-restart restart-time
```

Parameters

`<10000-600000>` Restart time value in milliseconds

Default

Default value is 180000 ms.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#graceful-restart restart-time 100000
```

hello-interval

Use this command to set an interval between Hello packets.

Used as a global command, this value is over-ridden by the hello-interval set on the interface (see rsvp hello-interval). For optimum performance, set this value no more than one-third of the hello-timeout value.

Use the `no` parameter with this command to return to the default hello interval value.

Command Syntax

```
hello-interval <1-65535>
no hello-interval
```

Parameter

`<1-65535>`	The time in seconds after which hello packets are sent

Default

By default, hello interval is 2 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#hello-interval 5

(config)#router rsvp
(config-router)#no hello-interval
```


© 2021 IP Infusion Inc. Proprietary

hello-receipt

Use this command to enable the receipt of Hello messages from peers.

Use the `no` parameter with this command to disable the exchange of Hello messages.

Command Syntax

```
hello-receipt
no hello-receipt
```

Parameters

None

Default

By default, hello receipt is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#hello-receipt
```

hello-timeout

If an LSR has not received a Hello message from a peer within the number of seconds set with this command, all sessions shared with this peer are reset. The hello-timeout determines how long an RSVP node waits for a hello message before declaring a neighbor to be down.

Use the `no` parameter with this command to return to the default hello timeout value.

Command Syntax

```
hello-timeout <1-65535>
no hello-timeout
```

Parameter

`<1-65535>`	Time set to receive a Hello message, in seconds

Default

By default, hello-timeout value is 10 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#hello-timeout 12

(config)#router rsvp
(config-router)#no hello-timeout
```


© 2021 IP Infusion Inc. Proprietary

keep-multiplier

Use this command to configure the constant to be used to calculate a valid reservation lifetime for a Labeled Switched Path (LSP).

The refresh time and keep multiplier are two interrelated timing parameters used to calculate the valid reservation lifetime for an LSP. Use the following formula to calculate the reservation lifetime for an LSP:

```
L >= (K + 0.5)* 1.5 * R
```

`K` = keep-multiplier

`R` = refresh timer

The router sends refresh messages periodically so that the neighbors do not timeout.

Use the `no` parameter with this command to return to the default keep-multiplier setting.

Command Syntax

```
keep-multiplier <1-255>
no keep-multiplier <1-255>
```

Parameters

`<1-255>`	The keep-multiplier value

Default

By default, keep-multiplier value is 3

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#keep-multiplier 2
```

loop-detection

Use this command to turn on loop detection for Path and Reservation messages exchanged between LSRs.

Use the no-loop-detection command to return to default settings.

Command Syntax

```
loop-detection
```

Parameters

None

Default

By default, loop detection is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#loop-detection
```


© 2021 IP Infusion Inc. Proprietary

map-route A.B.C.D

Use this command to map a route using an IPv4 to an RSVP trunk. If the primary LSP for a trunk goes down, all mapped routes are sent automatically to a secondary LSP configured as backup for a primary LSP.

Use the `no` parameter with this command to unmap routes from specified trunks.

Command Syntax

```
map-route A.B.C.D/M
map-route A.B.C.D/M CLASS
map-route A.B.C.D A.B.C.D
map-route A.B.C.D A.B.C.D CLASS
no map-route A.B.C.D/M
no map-route A.B.C.D/M CLASS
no map-route A.B.C.D A.B.C.D
no map-route A.B.C.D A.B.C.D CLASS
```

Parameters

`A.B.C.D/M`	Prefix to map, plus mask
`A.B.C.D`	Prefix to be mapped
`A.B.C.D`	Prefix mask
`CLASS`	Incoming DiffServ Class (for example, be, ef, etc.) to map to the RSVP trunk

Default

By default, map route A.B.C.D/M is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#map-route 2.2.2.2/16
```

map-route X:X::X:X

Use this command to map a route using an IPv6 to an RSVP trunk. If the primary LSP for a trunk goes down, all mapped routes are sent automatically to a secondary LSP configured as backup for a primary LSP.

Use the `no` parameter with this command to unmap routes from specified trunks.

Command Syntax

```
map-route X:X::X:X/M
map-route X:X::X:X/M CLASS
map-route X:X::X:X X:X::X:X
map-route X:X::X:X X:X::X:X CLASS
no map-route X:X::X:X/M
no map-route X:X::X:X/M CLASS
no map-route X:X::X:X X:X::X:X
no map-route X:X::X:X X:X::X:X CLASS
```

Parameters

`X:X::X:X/M`	Prefix to be mapped, plus mask
`X:X::X:X`	Prefix to be mapped
`X:X::X:X`	Prefix map
`CLASS`	Incoming DiffServ Class (for example, be, ef, etc.) to map to the trunk

Default

By default, map route X:XX::X:X/M is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#map-route 1:2::3:4/16
```


© 2021 IP Infusion Inc. Proprietary

neighbor A.B.C.D

Use this command to designate a neighbor IPv4 address to use when exchanging hello messages. Any neighbor hello message that is not explicitly identified is rejected.

Use the `no` parameter with this command to remove an IP neighbor from the system.

Command Syntax

```
neighbor A.B.C.D
no neighbor A.B.C.D
```

Parameters

None

Default

By default, neighbor A.B.C.D is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#neighbor 10.10.0.5
```

neighbor X:X::X:X

Use this command to designate a neighbor IPv6 address to use when exchanging hello messages. Any neighbor hello message that is not explicitly identified is rejected.

Use the `no` parameter with this command to remove an IP neighbor from the system.

Command Syntax

```
neighbor X:X::X:X
no neighbor X:X::X:X
```

Parameters

None

Default

By default, neighbor X:X::X:X is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#neighbor 3ffe::3:34
```


© 2021 IP Infusion Inc. Proprietary

no-cspf

Use this command to disable the use of the Constrained Shortest Path First (CSPF) server for all RSVP sessions. Disable CSPF when no nodes support the required traffic engineering extensions.

When this command is executed in Router mode, CSPF is disabled for all configured RSVP sessions, and all RSVP sessions configured from this point forward. If the default CSPF per RSVP session is enabled, it will be disabled. The CSPF status for RSVP sessions can be verified using the show rsvp session command with the detail option.

Use the cspf command to revert to the default settings.

Command Syntax

```
no-cspf
```

Parameters

None

Default

By default, no cspf is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows using the `no-cspf` command in Router mode to disable CSPF for all RSVP sessions.

```
#configure terminal
(config)#router rsvp
(config-router)#no-cspf
```

no-loop-detection

Use this command to turn off loop detection for Path and Reservation messages exchanged between LSRs. When a Path or Resv message is received, the primary IP address of the incoming interface is compared with the received route record list.

Use the loop-detection command to revert to default settings.

Command Syntax

```
no-loop-detection
```

Parameters

None

Default

By default, no loop detection is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#no-loop-detection
```


© 2021 IP Infusion Inc. Proprietary

no-php

Use this command to disable Penultimate-Hop-Popping (PHP) for the router. An egress router sends either the implicit-null or the explicit-null label for LSPs. hen the `no-php` command is used, the egress router sends non-reserved labels (those labels in the label pool range allotted to RSVP) to the upstream router.

Note: Use the show rsvp command to display the status of Penultimate-Hop-Popping.

Use the php command to revert to default settings.

Command Syntax

```
no-php
```

Parameters

None

Default

By default, Penultimate-Hop-Popping is enabled for standard RSVP LSP.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#no-php
```

no-refresh-path-parsing

Use this command to disable parsing of Refresh PATH messages received from upstream nodes. Enable this command to minimize message processing by RSVP, if you are sure that a particular router does not need to parse Refresh-PATH messages to check for changes because LSPs passing through this router are not required to be updated, simultaneously.

Use the refresh-path-parsing command to revert to the default settings.

Command Syntax

```
no-refresh-path-parsing
```

Parameters

None

Default

By default, refresh-path-parsing is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
Router#configure terminal
Router(config)#router rsvp
Router(config-router)#no-refresh-path-parsing
```


© 2021 IP Infusion Inc. Proprietary

no-refresh-resv-parsing

Use this command to disable parsing of Refresh RESV messages received from upstream nodes. Enable this command to minimize message processing by RSVP, if you are sure that a particular router does not need to parse Refresh RESV messages to check for changes because LSPs passing through this router are not required to be updated simultaneously.

Command Syntax

```
no-refresh-resv-parsing
```

Parameters

None

Default

By default, refresh reservation parsing is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
Router#configure terminal
Router(config)#router rsvp
Router(config-router)#no-refresh-resv-parsing
```

php

Use this command to enable Penultimate-Hop-Popping for the router. An egress router sends either the implicit-null or the explicit-null label for LSPs. If the `no-php` command has been enabled, the egress router sends `non-reserved` labels (those labels in the label pool range allotted to RSVP) to the upstream router.

Note: Use the show rsvp command to display the status of Penultimate-Hop-Popping.

Use the no-php command to disable this setting.

Command Syntax

```
php
```

Parameters

None

Default

By default, Penultimate-Hop-Popping is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#php
```


© 2021 IP Infusion Inc. Proprietary

primary ADMIN-GROUP-NAME

Use this command to configure primary administrative groups. Administrative groups are manually assigned attributes that describe the color of links, so that links with the same color are in one class. These groups are used to implement different policy-based LSP setups. Administrative group attributes can be included or excluded for an LSP or for a path's primary and secondary paths.

Note: A link can be added to a specific Administrative Group via the Network Services Module. Refer to the *Network Services Module Command Reference* for details.

Use the `no` parameter to remove a previously configured group from an administrative group list.

Command Syntax

```
primary (include-any|include-all|exclude-any) ADMIN-GROUP-NAME
primary (include-any|exclude-any) ADMIN-GROUP-NAME
primary (include-any|include-all|exclude-any) ADMIN-GROUP-NAME
primary (include-any|exclude-any) ADMIN-GROUP-NAME
```

Parameters

`include-any`	Include any attributes
`include-all`	Include all attributes
`exclude-any`	Exclude any attribute
`ADMIN-GROUP-NAME`	Administrative group name

Default

By default, primary admin group name is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary exclude-any myadmingroup

#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary include-all admingrp2

#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary include-any admingrp2
```

primary affinity

Use this command to enable sending of session attribute objects with resource affinity data.

Use the primary no-affinity command to disable sending of session attribute objects.

Command Syntax

```
primary affinity
```

Parameters

None

Default

By default, primary affinity is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary affinity
```


© 2021 IP Infusion Inc. Proprietary

primary bandwidth

Use this command to reserve the primary bandwidth in bits per second for the current trunk.

Each LSP has an associated bandwidth attribute. The bandwidth value is included in the sender's RSVP Path message and specifies the bandwidth to be reserved for the LSP. It is specified in bits per second, with a higher value indicating a greater user traffic volume. A zero bandwidth reserves no resources, although exchanges labels.

Use the `no` parameter to remove configured bandwidth information.

Command Syntax

```
primary bandwidth BANDWIDTH
no primary bandwidth BANDWIDTH
```

Parameter

`BANDWIDTH`	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Default

The default bandwidth is 0 bits per second, which allows data to flow through but does not reserve bandwidth.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary bandwidth 100m
```

primary cspf

Use this command to enable the use of Constrained Shortest Path First (CSPF) server for an explicit route to the egress, or all RSVP sessions. When CSPF is turned off globally, it cannot be enabled for any LSP.

The CSPF server computes paths for LSPs that are subject to constraints such as bandwidth, hop count, administrative groups, priority, and explicit routes. When computing paths for LSPs, CSPF considers not only the topology of the network and the attributes defined for the LSP, but also the links. It attempts to minimize congestion by intelligently balancing the network load.

Use the primary no-cspf command to revert to the default settings.

Command Syntax

```
primary cspf
```

Parameters

None

Default

By default, primary cspf is enabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary cspf
```


© 2021 IP Infusion Inc. Proprietary

primary cspf-retry-limit

Use this command to specify the number of retries that CSPF should carry out for a request received from RSVP.

Use the `no` parameter with this command to disable this configuration.

Command Syntax

```
primary cspf-retry-limit <1-65535>
no primary cspf-retry-limit <1-65535>
no primary cspf-retry-limit
```

Parameter

`<1-65535>`	Set the number of times CSPF should retry for this LSP

Default

By default, retry-limit is 0.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary cspf-retry-limit 535

(config)#rsvp-trunk T1
(config-trunk)#no primary cspf-retry-limit
```

© 2021 IP Infusion Inc. Proprietary

primary cspf-retry-timer

Use this command to specify the time between each retry that CSPF might carry out for a request received from RSVP.

Use the `no` parameter with this command to disable this configuration.

Command Syntax

```
primary cspf-retry-timer <1-600>
no primary cspf-retry-timer <1-600>
no primary cspf-retry-timer
```

Parameter

`<1-600>`	Timeout between successive retries, in seconds

Default

By default, retry-timer is 0

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary cspf-retry-timer 45

(config)#rsvp-trunk T1
(config-trunk)#no primary cspf-retry-timer 45
```


© 2021 IP Infusion Inc. Proprietary

primary filter

Use this command to set the filter to the fixed or shared style for an LSP.

- The shared filter style identifies a shared reservation environment. It creates a single reservation into which flows from all senders are mixed.
- The fixed filter style designates a distinct reservation. A distinct reservation request is created for data packets from a particular sender. The fixed filter style is also used style to prevent rerouting of an LSP and to prevent another LSP from using this bandwidth.

Use the `no` parameter to reset the configured filter to the default.

Command Syntax

```
primary filter (fixed|shared-explicit)
no primary filter (fixed|shared-explicit)
```

Parameters

`fixed`	Use a fixed filter for this LSP
`shared-explicit`	Use a shared-explicit filter for this LSP

Default

By default, primary filter is fixed

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary filter shared-explicit
```

primary hold-priority

Use this command to configure the hold priority value for the selected trunk. In case of insufficient bandwidth, remove less important existing LSPs to free up a portion of the bandwidth. This can be done by preempting one or more of the signaled LSPs. Hold priority determines the degree to which an LSP holds onto its reservation for a session after the LSP has been configured successfully. When the hold priority is high, the existing LSP is less likely to give up its reservation.

Use the `no` parameter to reset the trunk to the default hold-priority value.

Command Syntax

```
primary hold-priority <0-7>
no primary hold-priority <0-7>
no primary hold-priority
```

Parameter

`<0-7>`	Set a hold priority for the LSP

Default

The default hold-priority value is 0, which is the highest. Once a session is configured with a hold priority of 0, no other session can preempt it.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary hold-priority 2
```


© 2021 IP Infusion Inc. Proprietary

primary hop-limit

Use this command to specify a limit of hops for an RSVP trunk. Hop-limit data is sent to the CSPF server if CSPF is used.

Upon configuration of an arbitrary hop-limit, the hop-limit is compared with the number of hops configured in the primary path, if a primary path has been configured. If the number of hops in the primary path exceeds the hop-limit configured, no `Path` messages are sent, and any existing session is torn down. If no primary path is configured, the trunk is processed normally and Path messages are sent.

Use the `no` parameter to reset the trunk to the default hop-limit value.

Command Syntax

```
primary hop-limit <1-255>
no primary hop-limit <1-255>
no primary hop-limit
```

Parameters

`<1-255>`	Set the number of acceptable hops for the LSP

Default

By default, primary hop limit is 255

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary hop-limit 23
```

primary label-record

Use this command to record all labels exchanged between RSVP-enabled routers during the reservation setup process.

Use the `no` parameter with this command to turn off recording.

Command Syntax

```
primary label-record
no primary label-record
```

Parameters

None

Default

By default, primary label record is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary label-record
```


© 2021 IP Infusion Inc. Proprietary

primary local-protection

Use this command to enable the local repair of explicit routes for which this router is a transit node.

Use the `no` parameter with this command to disable local repair of explicit routes.

Command Syntax

```
primary local-protection
no primary local-protection
```

Parameters

None

Default

By default, primary local protection is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary local-protection
```

primary no-affinity

Use this command to disable the use of sending out session attribute objects with resource affinity data.

Use the primary affinity command to return to the default settings.

Command Syntax

```
primary no-affinity
```

Parameters

None

Default

By default, primary no affinity is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary no-affinity
```


© 2021 IP Infusion Inc. Proprietary

primary no-cspf

Use this command to disable the use of Constrained Shortest Path First (CSPF) server for an explicit route to the egress, or all RSVP sessions. When CSPF is turned off globally it cannot be enabled for any LSP. If used per LSP, it can be used to turn off CSPF computation for a specific LSP.

Disable CSPF when all nodes do not support the required traffic engineering extensions, and configure LSPs manually to use an explicit path. The LSP is then established only along the path specified by the operator.

Use the primary cspf command to enable this setting.

Command Syntax

```
primary no-cspf
```

Parameters

None

Default

By default, primary no cspf is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows using the `no-cspf` command in Trunk mode to disable CSPF for the primary LSP.

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary no-cspf
```

© 2021 IP Infusion Inc. Proprietary

primary no-record

Use this command to disable recording of the route taken by Path and Reservation Request (Resv) messages to confirm establishment of reservations and identify errors. Routes are recorded by means of the Route Record Object (RRO) in RSVP messages.

Use the primary record command to return to the default settings.

Command Syntax

```
primary no-record
```

Parameters

None

Default

By default, routes are recorded

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary no-record
```


© 2021 IP Infusion Inc. Proprietary

primary path

Use this command to specify an RSVP path to be used. The `PATHNAME` in this command is the string (name) used to identify an RSVP path defined for the node (refer to `rsvp-path` command).

Use the `no` parameter with this command to remove a configured RSVP path.

Command Syntax

```
primary path PATHNAME
no primary path PATHNAME
no primary path
```

Parameters

`PATHNAME`	The name of the path to use

Default

By default, primary path is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary path mypath
```

primary policer

Use this command to configure policing in hardware for the configured primary bandwidth.

Use the no parameter with this command to remove a policing from hardware.

Command Syntax

```
primary policer
no primary policer
```

Parameters

None

Default

By default, primary policer is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary bandwidth 100m
(config-trunk)#primary policer
(config-trunk)#no primary policer
```


© 2021 IP Infusion Inc. Proprietary

primary record

Use this command to enable recording of the route taken by Path and Reservation Request (Resv) messages to confirm establishment of reservations and identify errors. Routes are recorded by means or the Route Record Object (RRO) in RSVP messages.

Use the primary no-record command to disable recording of routes.

Command Syntax

```
primary record
```

Parameters

None

Default

By default, routes are recorded

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary record
```

primary retry-limit

Use this command to specify a retry count this RSVP Trunk.

If a session is in a `nonexistent` state due to a path error message, the system tries to recreate the LSP for the number of times specified by the `retry-limit` command.

Although the same retry command controls both the trunk and the session, the retry-limit value affects only the session and not the trunk. If the trunk is in an `incomplete` state, the code keeps trying forever to bring it to a `complete` state regardless of the retry-limit value.

Use the `no` parameter with this command to revert to the default retry-limit value.

Command Syntax

```
primary retry-limit <1-65535>
no primary retry-limit <1-65535>
no primary retry-limit
```

Parameter

`<1-65535>`	The set number of times the system should try setting up the LSP

Default

By default, the retry-limit value is 0, and the trunk and session try to create the LSP indefinitely.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary retry-limit 256
```


© 2021 IP Infusion Inc. Proprietary

primary retry-timer

Use this command to specify a retry interval for an RSVP Trunk. When an ingress node tries to configure an LSP and the setup fails due to the receipt of a Path Error message, the system waits for the time configured with this command, before retrying the LSP setup process.

Use the `no` parameter with this command to revert to the default retry-time value.

Command Syntax

```
primary retry-timer <1-600>
no primary retry-timer <1-600>
no primary retry-timer
```

Parameter

`<1-600>`	Time in seconds after which the system should retry setting up the LSP

Default

By default, retry-timer value is 30 seconds.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary retry-timer 12
```

primary reuse-route-record

Use this command to use the updated Route Record List as an Explicit Route (with all strict nodes) when a path message is sent out at the next refresh.

The ERO list contains the hops to be taken to reach the egress from the current LSR. If CSPF is not available, to place an ERO with all strict routes, use this command to modify the ERO after receiving the Resv message. The future Path messages have the ERO with all strict nodes, identifying each and every node to be traversed.

Use the `no` parameter with this command to disable the use of the Route Record List as the explicit route.

Command Syntax

```
primary reuse-route-record
no primary reuse-route-record
```

Parameters

None

Default

By default, primary reuse route record is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary reuse-route-record
```


© 2021 IP Infusion Inc. Proprietary

primary setup-priority

Use this command to configure a setup priority value for a trunk. In case of insufficient bandwidth, users must remove less important LSPs to free up the bandwidth. This can be done by preempting one or more of the existing LSPs. The primary setup priority determines if a new LSP can preempt an existing LSP.

The setup priority of the new LSP must be higher than the hold priority of an existing LSP for the existing LSP to be preempted. Note that for a trunk, the setup priority should not be higher than the hold priority.

Use the `no` parameter with this command to revert to the default primary setup priority value.

Command Syntax

```
primary setup-priority <0-7>
no primary setup-priority <0-7>
no primary setup-priority
```

Parameters

`<0-7>`	Set the priority value

Default

By default, setup priority is 7, which is the lowest.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary setup-priority 2
```

primary traffic

Use this command to specify the traffic type for this RSVP Trunk.

Use the `no` parameter with this command to reset the configured traffic type.

Command Syntax

```
primary traffic (guaranteed|controlled-load)
no primary traffic (guaranteed|controlled-load)
no primary traffic
```

Parameters

`controlled-load` Controlled loaded traffic

`guaranteed` Guaranteed traffic

Default

By default, primary traffic type is controlled-load

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary traffic guaranteed
```


© 2021 IP Infusion Inc. Proprietary

refresh-time

Use this command to configure RSVP refresh interval timer. The timer specifies the interval after which Path and/ or Reservation Request (Resv) messages will be sent out.

The refresh time and keep multiplier are two interrelated timing parameters used to calculate the valid Reservation Lifetime for an LSP. Refresh time regulates the interval between Refresh messages which include Path and Reservation Request (Resv) messages. Refresh messages are sent periodically so that reservation does not timeout in the neighboring nodes. Each sender and receiver host sends Path and Resv messages, downstream and upstream respectively, along the paths.

Use the `no` parameter with this command to return to the default refresh-time interval.

Command Syntax

```
refresh-time <1-65535>
no refresh-time <1-65535>
no refresh-time
```

Parameter

`<1-65535>`	The duration for which messages are sent, in seconds

Default

By default, refresh-time interval is 30 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#refresh-time 20
```

refresh-path-parsing

Use this command to disable parsing of Refresh PATH messages received from upstream nodes. Use this command to minimize message processing by RSVP when you are sure that a particular router does not need to parse Refresh-PATH messages to check for changes, because LSPs passing through this router are not required to be updated simultaneously.

Use the no-refresh-path-parsing command to disable this setting.

Command Syntax

```
refresh-path-parsing
```

Parameters

None

Default

By default, refresh-path-parsing is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
Router#configure terminal
Router(config)#router rsvp
Router(config-router)#refresh-path-parsing
```


© 2021 IP Infusion Inc. Proprietary

refresh-resv-parsing

Use this command to disable parsing of Refresh RESV messages received from upstream nodes. Use this command to minimize message processing by RSVP when you are sure that a particular router does not need to parse Refresh RESV messages to check for changes because LSPs passing through this router are not required to be updated simultaneously.

Use the no-refresh-resv-parsing command to disable this setting.

Command Syntax

```
refresh-resv-parsing
```

Parameters

None

Default

By default, refresh reservation parsing is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
Router#configure terminal
Router(config)#router rsvp
Router(config-router)#refresh-resv-parsing
```

restart rsvp graceful

Use this command to restart RSVP gracefully.

To restart RSVP gracefully, you must give the graceful-restart command to enable graceful restart capability on the device in RSVP router mode.

Command Syntax

```
restart rsvp graceful
```

Parameter

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Example

```
#restart rsvp graceful
% Warning : You may loose rsvp configuration, if not saved
Proceed for graceful restart? (y/n):y
%% Managed module is down or crashed
```


© 2021 IP Infusion Inc. Proprietary

router rsvp

Use this command to enter router mode from configure mode and to enable the RSVP daemon, if it is not already enabled.

Use the `no` parameter with this command to disable RSVP on the node.

Command Syntax

```
router rsvp
```

```
no router rsvp
```

Parameters

None

Default

RSVP is started only if this command is executed.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The command prompt changes from config to config-router, as illustrated below:

```
#configure terminal
(config)#router rsvp
(config-router)#

(config-router)#exit
(config)#no router rsvp
```

rsvp hello-interval

Use this command to enable the sending of Hello packets on the interface and to set the interval value between successive Hello packets to neighbor. For optimum performance, set this value to less than one-third the value of the configured RSVP hello-timeout. See the rsvp hello-timeout command for more information.

Note: This is an interface-specific command and when not used, the global hello-interval state applies.

Use the `no` parameter with this command to return to the default hello interval value.

Command Syntax

```
rsvp hello-interval <1-65535>
no rsvp hello-interval
```

Parameter

`<1-65535>`	RSVP hello interval in seconds

Default

By default, RSVP hello interval is 2 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp hello-interval 110

(config)#interface eth0
(config-if)#no rsvp hello-interval
```


© 2021 IP Infusion Inc. Proprietary

rsvp hello-receipt

Use this command to enable the receipt of hello messages from peers connected through this interface. This is an interface-specific command and when not used, the global hello-receipt command applies.

Use the `no` parameter with this command to disable the exchange of hello messages for this interface.

Command Syntax

```
rsvp hello-receipt
no rsvp hello-receipt
```

Parameters

None

Default

By default, rsvp hello receipt is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp hello-receipt
```

rsvp hello-timeout

This command determines how long an RSVP node should wait for a hello message before declaring a neighbor to be down. If an LSR does not received a hello message from a peer connected to an interface within the specified duration, the LSR resets all sessions that are shared with this particular peer. This is an interface-specific command and when not used, the global hello-timeout command applies.

Use the `no` parameter to revert to the default hello timeout value.

Command Syntax

```
rsvp hello-timeout <1-65535>
no rsvp hello-timeout
```

Parameters

`<1-65535>`	Time to receive a hello message, in seconds

Default

By default, hello-timeout value is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp hello-timeout 550

(config)#interface eth0
(config-if)#no rsvp hello-timeout
```


© 2021 IP Infusion Inc. Proprietary

rsvp keep-multiplier

This command sets the constant for calculating a valid reservation lifetime for an LSP, which allows messages to be exchanged through this interface. This is an interface-specific command and when not specified, the global keep-multiplier command applies.

Reservation lifetime is the duration of bandwidth reservation for the LSP. The refresh time and keep multiplier are two interrelated timing parameters used to calculate the valid reservation lifetime for an LSP. Use the following formula to calculate the reservation lifetime for an LSP:

```
L >= (K + 0.5)* 1.5 * R
```

`K` = keep-multiplier

`R` = refresh timer

Refresh messages are sent periodically so that neighbors do not timeout.

Use the `no` parameter with this command to return to the global keep-multiplier value.

Command Syntax

```
rsvp keep-multiplier <1-255>
no rsvp keep-multiplier <1-255>
```

Parameter

`<1-255>`	Set a value for the lifetime constant

Default

By default RSVP keep-multiplier value is 3

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp keep-multiplier 3

(config)#interface eth0
(config-if)#no rsvp keep-multiplier 3
```

rsvp refresh-time

Use this command to configure RSVP refresh interval timer for the current interface. This is an interface-specific command and when not used, the global refresh-time command applies.

The refresh time and keep multiplier are two interrelated timing parameters used to calculate the valid reservation lifetime for an LSP. Refresh time regulates the interval between refresh messages that include path and reservation request (Resv) messages. Refresh messages are sent periodically so that the reservation does not timeout in the neighboring nodes. Each sender and receiver host sends path and resv messages, downstream and upstream respectively, along the paths.

Use the `no` parameter with this command to revert to the refresh-time value set in RSVP mode.

Command Syntax

```
rsvp refresh-time <1-65535>
no rsvp refresh-time <1-65535>
```

Parameter

`<1-65535>`	The duration for which messages are sent, in seconds

Default

By default, refresh interval is 30 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp refresh-time 5055

(config)#interface eth0
(config-if)#no rsvp refresh-time 5055
```


© 2021 IP Infusion Inc. Proprietary

rsvp-path

Use this command to create a new RSVP path or to enter the `Path` command mode. In this mode, you can add or delete paths and also specify the path to be loose or strict.

Use the `no` parameter with this command to delete the path and its specified hops.

Command Syntax

```
rsvp-path PATHNAME
no rsvp-path PATHNAME
```

Parameter

`PATHNAME`	Name of the path

Default

By default, rsvp path is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-path mypath
(config-path)#
```

rsvp-trunk

Use this command to create a new RSVP trunk. When the trunk is created, the attributes required to configure an explicitly-routed or traditionally-routed LSP are set. Once a trunk is configured with the required attributes, an RSVP session (and PSB) is created for this trunk, which enables the exchange of messages and completes the LSP setup.

This command also modifies an existing RSVP path to configure an explicitly-routed or traditionally-routed LSP. In addition, this command can be used to set the address family (IPv4 or IPv6) of an RSVP trunk. If no address family is assigned, the default value is used. If the address family is already set, a check is made to see whether the address family configured and the one already in the database are the same. An error message is returned if the two do not match.

Use the `no` parameter with this command to remove an RSVP trunk and all configured attributes, except the primary path.

Note: The RSVP trunk's name (`TRUNKNAME`) is limited to 32 characters.

Command Syntax

```
rsvp-trunk TRUNKNAME (ipv4|ipv6)
no rsvp-trunk TRUNKNAME
```

Parameters

`TRUNKNAME`	Name to use for the trunk
`ipv4`	IPv4 address family trunk
`ipv6`	IPv6 address family trunk

Default

By default, rsvp trunk is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The command prompt changes from `config` to `config-trunk` as illustrated below:

```
#configure terminal
(config)#rsvp-trunk mytrunk ipv4
(config-trunk)#
```


© 2021 IP Infusion Inc. Proprietary

rsvp-trunk-restart

Use this command to restart the RSVP trunk. This command “kills” an existing LSP and restarts the LSP setup process.

Command Syntax

```
rsvp-trunk-restart
```

Parameters

None

Default

By default, rsvp trunk restart is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#rsvp-trunk-restart
```

secondary ADMIN-GROUP-NAME

Use this command to configure secondary administrative groups. Administrative groups are manually assigned attributes that describe the color of links, so that links with the same color are in one class. These groups are used to implement different policy-based LSP setups. Administrative group attributes can be included or excluded for an LSP or for a path's primary and secondary paths.

Note: A link can be added to a specific Administrative Group via NSM. Refer to the *Network Services Module Command Reference* for details.

Use the `no` parameter to remove a previously set group from an administrative group list.

Command Syntax

```
secondary (include-any|include-all|exclude-any) ADMIN-GROUP-NAME
secondary (include-any|exclude-any) ADMIN-GROUP-NAME
no secondary (include-any|include-all|exclude-any) ADMIN-GROUP-NAME
no secondary (include-any|exclude-any) ADMIN-GROUP-NAME
```

Parameters

`include-any`	Include any attribute
`include-all`	Include all attribute
`exclude-any`	Exclude any attribute
`ADMIN-GROUP-NAME`	Administrative group name

Default

By default, secondary admin group name is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary exclude-any myadmingroup

#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary include-any myadmingroup

#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary include-all myadmingroup
```


© 2021 IP Infusion Inc. Proprietary

secondary bandwidth

Use this command to reserve the bandwidth in bits per second for the current trunk.

Each LSP has an associated bandwidth attribute. The bandwidth value is included in the sender's RSVP Path message and specifies the bandwidth to be reserved for the LSP. It is set in bits per second, with a higher value indicating a greater user traffic volume. A zero bandwidth reserves no resources, although label exchanges are possible.

Use the `no` parameter with this command to unset the configured bandwidth information.

Command Syntax

```
secondary bandwidth BANDWIDTH
no secondary bandwidth BANDWIDTH
no secondary bandwidth
```

Parameter

`BANDWIDTH`	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Default

By default, bandwidth is 0 bits per second, which allows data to flow through but does not reserve bandwidth.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary bandwidth 100m
```

secondary cspf

Use this command to enable the use of Constrained Shortest Path First (CSPF) server for an explicit route to the egress, or all RSVP sessions.

The CSPF server computes paths for LSPs that are subject to constraints such as bandwidth, hop count, administrative groups, priority, and explicit routes. When computing paths for LSPs, CSPF considers not only the topology of the network and the attributes defined for the LSP, but also the links. It attempts to minimize congestion by intelligently balancing the network load.

Use the secondary no-cspf command to revert to the default settings.

Command Syntax

```
secondary cspf
```

Parameters

None

Default

By default, secondary cspf is enabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows using the `no-cspf` command in Trunk mode to disable CSPF for the primary LSP.

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary cspf
```


© 2021 IP Infusion Inc. Proprietary

secondary cspf-retry-limit

Use this command to specify the number of retries that CSPF should carry out for a request received from RSVP.

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
secondary cspf-retry-limit <1-65535>
no secondary cspf-retry-limit <1-65535>
no secondary cspf-retry-limit
```

Parameter

`<1-65535>`	The number of times CSPF should retry for this LSP

Default

By default, no retry limit for CSPF route calculations is configured, so the value is 0.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary cspf-retry-limit 535
```

secondary cspf-retry-timer

Use this command to specify the time between each retry that CSPF might carry out for a request received from RSVP.

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
secondary cspf-retry-timer <1-600>
no secondary cspf-retry-timer <1-600>
no secondary cspf-retry-timer
```

Parameters

`<1-600>`	Timeout between successive retries, in seconds

Default

By default, no retry-timer configuration is defined for CSPF calculations, so the value is set to 0.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary cspf-retry-timer 45
```


© 2021 IP Infusion Inc. Proprietary

secondary filter

Use this command to set the filter to fixed or shared filter style for RSVP trunk.

- The shared filter style identifies a shared reservation environment. It creates a single reservation into which flows from all senders are mixed.
- The fixed filter style designates a distinct reservation. A distinct reservation request is created for data packets from a particular sender. The fixed filter style is also used style to prevent rerouting of an LSP and to prevent another LSP from using this bandwidth.

Use the `no` parameter to reset the configured filter to the default style.

Command Syntax

```
secondary filter (fixed|shared-explicit)
no secondary filter (fixed|shared-explicit)
no secondary filter
```

Parameters

`fixed`	Use a Fixed Filter for this RSVP Trunk.
`shared-explicit`	Use a Shared Explicit Filter for this RSVP Trunk.

Default

By default, secondary filter is fixed style

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Usage

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary filter shared-explicit
```

secondary hold-priority

Use this command to configure the hold priority value for the selected trunk.

In case of insufficient bandwidth, the user must remove any less important existing LSP to free up the bandwidth. This can be done by preempting one or more of the signaled LSPs. Hold priority determines the degree to which an LSP holds onto its reservation for a session after the LSP has been configured successfully. When the hold priority is high, the existing LSP is less likely to give up its reservation.

Use the `no` parameter to revert to the default hold-priority value.

Command Syntax

```
secondary hold-priority <0-7>
no secondary hold-priority <0-7>
no secondary hold-priority
```

Parameter

`<0-7>`	Specify a value for hold priority

Default

The default hold-priority is 0, the highest value. Once a session is configured with a 0 hold priority value, no other session can preempt it.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary hold-priority 2
```


© 2021 IP Infusion Inc. Proprietary

secondary hop-limit

Use this command to specify a limit of hops for an RSVP trunk.

Upon configuration of an arbitrary hop-limit, the hop-limit is compared with the number of hops configured in the primary path, if a primary path has been configured. If the number of hops in the primary path exceed the hop-limit configured, no path messages are sent out and any existing session is torn down. If no primary path is configured, the trunk is processed normally and the path messages are sent out. The hop-limit data is sent to the CSPF server, if CSPF is being used.

Use the `no` parameter to revert to the default hop-limit value.

Command Syntax

```
secondary hop-limit <1-255>
no secondary hop-limit <1-255>
no secondary hop-limit
```

Parameter

`<1-255>`	The number of acceptable hops

Default

By default, secondary hop limit is 255

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary hop-limit 23
```

secondary label-record

Use this command to record all labels exchanged between RSVP enabled routers during the reservation setup process. This command records all labels exchanged for an LSP from the ingress to the egress, and helps with debugging.

Use the `no` parameter to turn off recording.

Command Syntax

```
secondary label-record
```

```
no secondary label-record
```

Default

By default, secondary label record is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary label-record
```


© 2021 IP Infusion Inc. Proprietary

secondary local-protection

Use this command to enable the local repair of explicit routes for which this router is a transit node.

Use the `no` parameter with this command to disable local repair of explicit routes.

Command Syntax

```
secondary local-protection
no secondary local-protection
```

Parameters

None

Default

By default, secondary local protection is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary local-protection
```

secondary no-affinity

Use this command to disable the use of sending out session attribute objects with resource affinity data.

Use the secondary bandwidth command to revert to the default settings.

Command Syntax

```
secondary no-affinity
```

Parameters

None

Default

By default, secondary no affinity is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary no-affinity
```


© 2021 IP Infusion Inc. Proprietary

secondary no-cspf

Use this command to disable the use of Constrained Shortest Path First (CSPF) server for an explicit route to the egress, or all RSVP sessions.

If CSPF is turned off globally, it cannot be enabled for any LSP. If used per LSP, it can be used to turn off CSPF computation for a specific LSP. The CSPF server computes paths for LSPs that are subject to various constraints such as bandwidth, hop count, administrative groups, priority, and explicit routes. When computing paths for LSPs, CSPF considers not only the topology of the network and the attributes defined for the LSP, but, also the links. It attempts to minimize congestion by intelligently balancing the network load.

Disable CSPF when all nodes do not support the required traffic engineering extensions and configure LSPs manually to use an explicit path. The LSP is then established only along the path specified by the operator.

Use the secondary cspf command to revert to the default settings.

Command Syntax

```
secondary no-cspf
```

Parameters

None

Default

By default, secondary no cspf is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows using the `no-cspf` command in Trunk mode to disable CSPF for the primary LSP.

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary no-cspf
```

secondary no-record

This command is used to disable recording of the route taken by path and resv messages and confirms the establishment of reservations and to identify errors. Routes are recorded by means of the route record object (RRO) in an RSVP message.

Use the secondary record command to revert to the default settings.

Command Syntax

```
secondary no-record
```

Parameters

None

Default

By default, routes are recorded

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary no-record
```


© 2021 IP Infusion Inc. Proprietary

secondary path

Use this command to specify an RSVP path to be used.

Use the `no` parameter with this command to remove a configured RSVP path.

Command Syntax

```
secondary path PATHNAME
no secondary path PATHNAME
no secondary path
```

Parameters

`PATHNAME`	The name of the path to be used. `PATHNAME` is a string (name) used to identify an RSVP path defined for the node (refer to the rsvp-path command).

Default

By default, secondary path is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary path mypath
```

secondary policer

Use this command to configure policing in hardware for the configured secondary bandwidth.

Use the no parameter with this command to remove a policing from hardware.

Command Syntax

```
secondary policer
no secondary policer
```

Parameters

None

Default

By default, secondary policer is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary bandwidth 200m
(config-trunk)#secondary policer
(config-trunk)#no secondary policer
```


© 2021 IP Infusion Inc. Proprietary

secondary record

This command is used to enable recording of the route taken by path and resv messages to confirm the establishment of reservations and to identify errors. Routes are recorded by means of the route record object (RRO) in RSVP messages.

Use the secondary no-record command to revert to the default settings.

Command Syntax

```
secondary record
```

Parameters

None

Default

By default, routes are recorded

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary record
```

secondary retry-limit

Use this command to specify a retry count this RSVP Trunk.

If a session is in a nonexistent state due to the receipt of a path error message, it tries to recreate the LSP for the number of times specified by primary retry-limit. Although the same retry command controls both the trunk and the session, the retry-limit value affects only the session and not the trunk. If the trunk is in an incomplete state, the code keeps trying to bring it to a complete state, irrespective of the retry-limit value.

Use the `no` parameter to revert to the default retry-limit value.

Command Syntax

```
secondary retry-limit <1-65535>
no secondary retry-limit <1-65535>
```

Parameter

`<1-65535>`	The set number of times the system should try setting up the LSP

Default

By default, the retry-limit value is 0 so the trunk and session try to create the LSP indefinitely.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary retry-limit 256
```


© 2021 IP Infusion Inc. Proprietary

secondary retry-timer

Use this command to specify a retry interval for an RSVP Trunk. When the ingress tries to configure an LSP and the setup fails due to the receipt of a path error message, the system waits for the time configure by this command before retrying the LSP setup process.

Use the `no` parameter to revert to the default.

Command Syntax

```
secondary retry-timer <1-600>
no secondary retry-timer <1-600>
no secondary retry-timer
```

Parameter

`<1-600>`	Interval after which the system should retry setting up the LSP, in seconds

Default

By default, retry time is 30 seconds

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary retry-timer 12
```

secondary reuse-route-record

Use this command to use the updated route record list as an explicit route (with all strict nodes) when a path message is sent out at the next refresh.

An explicit route object (ERO) list contains the hops to be taken to reach the egress from the current LSR. If CSPF can not place an ERO with all strict routes, then this command helps modify the ERO after receiving resv messages. Future path messages have the ERO with all strict nodes, which identify each and every node to be traversed.

Use the `no` parameter to disable the use of the route record list as the explicit route.

Command Syntax

```
secondary reuse-route-record
no secondary reuse-route-record
```

Parameters

None

Default

By default, secondary reuse route record is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary reuse-route-record
```


© 2021 IP Infusion Inc. Proprietary

secondary setup-priority

Use this command to configure a setup priority value for this trunk.

In case of insufficient bandwidth, the user must remove any less important LSPs to free up bandwidth. This can be done by preempting one or more of the existing LSPs. The setup priority determines whether a new LSP that preempts an existing LSP may be established. The setup priority of the new LSP must be higher than the hold priority of an existing LSP for the existing LSP to be preempted. Note that for a trunk, the setup priority should not be higher than the hold priority.

Use the `no` parameter with this command to revert to the default setup priority value.

Command Syntax

```
secondary setup-priority <0-7>
no secondary setup-priority <0-7>
```

Parameters

`<0-7>`	The priority value

Default

By default, setup value is 7 (the lowest).

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary setup-priority 2
```

secondary traffic

Use this command to identify the traffic type for this RSVP Trunk.

Use the `no` parameter with this command to unset the configured traffic type.

Command Syntax

```
secondary traffic (guaranteed|controlled-load)
no secondary traffic (guaranteed|controlled-load)
no secondary traffic
```

Parameters

`guaranteed`	Guaranteed traffic
`controlled-load`	Controlled load traffic

Default

Controlled load is the default traffic type.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary traffic guaranteed
```


© 2021 IP Infusion Inc. Proprietary

snmp restart rsvp

Use this command to restart SNMP in Resource Reservation Protocol -Traffic Engineering (RSVP-TE)

Command Syntax

```
snmp restart rsvp
```

Parameters

None

Default

By default, snmp restart rsvp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart rsvp
```

to A.B.C.D

Use this command to specify an IPv4 egress for an LSP. When configuring an LSP, you must specify the address of the egress router by using this command in the trunk node. An egress definition is a mandatory attribute; no RSVP session is created when an egress is not defined.

Use the `no` parameter with this command to unset the configured egress address.

Command Syntax

```
to A.B.C.D
```

```
no to A.B.C.D
```

Parameters

None

Default

The operator must specify an egress for LSP initialization to begin.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#to 10.10.0.5
```


© 2021 IP Infusion Inc. Proprietary

to X:X::X:X

Use this command to specify an IPv6 egress for an LSP. When configuring an LSP, you must specify the address of the egress router by using this command in the trunk node. An egress definition is a mandatory attribute; no RSVP session is created when an egress is not defined.

Use the `no` parameter with this command to unset the configured egress address.

Command Syntax

```
to X:X::X:X
no to X:X::X:X
```

Parameters

None

Default

The operator must specify an egress for LSP initialization to begin.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk ipv6
(config-trunk)#to 3ffe::3:34
```

update-type

Use this command to change the method of updating attributes for sessions (primary/ secondary) for this trunk.

- If make-before-break is configured (default type), a new LSP is created for each attribute update. When the new LSP becomes operational, the original LSP is torn down.
- If break-before-make is configured, the existing LSP is torn down and restarted for each attribute update.

Use the `no` parameter with this command to remove an update type.

Command Syntax

```
update-type (make-before-break|break-before-make)
update-type (make-before-break|break-before-make)
no update-type (make-before-break|break-before-make)
no update-type (make-before-break|break-before-make)
no update-type
```

Parameters

`make-before-break`

Make before break update

`break-before-make`

Break before make update

Default

By default, make-before-break types of updates are carried out.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#update-type break-before-make

#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#update-type make-before-break
```


© 2021 IP Infusion Inc. Proprietary

X:X::X:X

Use this command to define an explicit IPv6 route sub-object as either loose or strict. A list of sub-objects specifies an explicit route to the egress router for an LSP.

- For the strict type of route addresses, the route taken from the previous router to the current router must be a directly-connected path and a message exchanged between the two routers should not pass any intermediate routers. This ensures that routing is enforced on the basis of each link.
- For the loose type of route addresses, the route taken form the previous router to the current router need not be a direct path and a message exchanged between the two routers can pass other routers.

Use the `no` parameter with this command to disable the configuration.

Command Syntax

```
X:X::X:X
X:X::X:X (loose|strict)
no X:X::X:X
no X:X::X:X (loose|strict)
```

Parameters

`loose`	Make this node loose
`strict`	Make this node strict

Default

By default, X:X::X:X is disabled

Command Mode

Path mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-path mypath
(config-path)#3ffe::3:34 strict
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 2 Fast Reroute Commands

This chapter describes the RSVP-TE Fast Reroute commands.

- detour-identification
- from X:X::X:X
- primary fast-reroute bandwidth
- primary fast-reroute hold-priority
- primary fast-reroute hop-limit
- primary fast-reroute node-protection
- primary fast-reroute protection
- primary fast-reroute setup-priority

detour-identification

Use this command to set a path-specific detour LSP identification method, using the detour object.

Use the no parameter with this command to unset the detour LSP identification method.

Note: This command helps identify the backup LSP identification method for one-to-one protection only.

Command Syntax

```
detour-identification (path|sender-template)
no detour-identification (path|sender-template|)
```

Parameters

`path`	Set a path-specific detour identification method
`sender-template`	Set a sender template-specific detour identification method

Default

By default, detour identification is sender template

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#detour-identification path

#configure terminal
(config)#router rsvp
(config-router)#detour-identification sender-template

#configure terminal
(config)#router rsvp
(config-router)#no detour-identification path

#configure terminal
(config)#router rsvp
(config-router)#no detour-identification sender-template
```


© 2021 IP Infusion Inc. Proprietary

from X:X::X:X

Use this command to specify a “from” IPv6 address for tunnel ingress.

Use the `no` parameter with this command to remove an IPv6 address from tunnel ingress.

Command Syntax

```
from X:X::X:X
no from X:X::X:X
no from
```

Parameters

None

Default

By default, from X:X::X:X is disabled

Command Mode

Router mode or Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#from 3ffe::3:34

#configure terminal
(config)#router rsvp
(config-router)#from 3ffe::3:34
```

© 2021 IP Infusion Inc. Proprietary

primary fast-reroute bandwidth

Use this command to set the detour LSP bandwidth.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to unset fast-reroute LSP bandwidth.

Command Syntax

```
primary fast-reroute bandwidth BANDWIDTH
no primary fast-reroute bandwidth BANDWIDTH
no primary fast-reroute BANDWIDTH
```

Parameter

`BANDWIDTH`	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Default

By default, primary fast reroute bandwidth is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute bandwidth 10000000
```


© 2021 IP Infusion Inc. Proprietary

primary fast-reroute hold-priority

Use this command to set the hold-priority for a detour LSP.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to unset the detour LSP hold-priority.

Command Syntax

```
primary fast-reroute hold-priority <0-7>
no primary fast-reroute hold-priority (<0-7>|)
```

Parameter

`<0-7>`	Set the value for hold-priority

Default

By default, primary fast reroute hold priority is 0

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute hold-priority 3
```

primary fast-reroute hop-limit

Use this command to set the hop-limit for a detour LSP.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to unset the detour LSP hop-limit.

Command Syntax

```
primary fast-reroute hop-limit <1-255>
no primary fast-reroute hop-limit (<1-255>|)
```

Parameter

`<1-255>`	Set the number of hops

Default

By default, primary fast reroute hop limit is 255

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute hop-limit 25
```


© 2021 IP Infusion Inc. Proprietary

primary fast-reroute node-protection

Use this command to set node protection.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to remove node protection.

Command Syntax

```
primary fast-reroute node-protection
no primary fast-reroute node-protection
```

Parameters

None

Default

By default, primary fast reroute node protection is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute node-protection
```

primary fast-reroute protection

Use this command to create an Fast Reroute backup and to set an LSP one-to-one protection mechanism.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to remove LSP protection mechanism.

Parameters

None

Command Syntax

```
primary fast-reroute protection (one-to-one)
no primary fast-reroute protection (one-to-one)
```

Parameters

`one-to-one`	Set the one-to-one protection mechanism

Default

By default, primary fast reroute protection is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute protection one-to-one
```


© 2021 IP Infusion Inc. Proprietary

primary fast-reroute setup-priority

Use this command to configure a setup-priority for the detour LSP.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to remove the detour LSP setup-priority.

Command Syntax

```
primary fast-reroute setup-priority <0-7>
no primary fast-reroute setup-priority (<0-7>|)
```

Parameter

`<0-7>`	Set a value for setup priority

Default

By default, primary fast reroute setup priority is 0

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute setup-priority 2
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 3 Refresh Reduction Commands

This chapter describes the RSVP-TE Refresh Reduction commands:

- ack-wait-timeout
- message-ack
- refresh-reduction
- rsvp ack-wait-timeout
- rsvp message-ack
- rsvp refresh-reduction

ack-wait-timeout

Use this command to configure the acknowledgement wait timeout for all RSVP-TE neighbors.

Use the `no` parameter with this command to revert to the default acknowledgement wait timeout.

Command Syntax

```
ack-wait-timeout <1-65535>
no ack-wait-timeout <1-65535>
no ack-wait-timeout
```

Parameter

`<1-65535>`	Specify a value for the acknowledgement wait timeout in seconds. The default timeout value is 10 seconds.

Default

By default, ack wait timeout is 10 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#ack-wait-timeout 5

(config)#router rsvp
(config-router)#no ack-wait-timeout 5
```


© 2021 IP Infusion Inc. Proprietary

message-ack

Use this command to enable message acknowledgment for all messages being sent to neighbors that are known to support refresh reduction.

Use the `no` parameter with this command to disable message acknowledgment for all messages being sent to neighbors.

Command Syntax

```
message-ack

no message-ack
```

Parameters

None

Default

By default, Message Acknowledgment is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#message-ack

(config)#router rsvp
(config-router)#no message-ack
```

refresh-reduction

Use this command to enable refresh reduction capability advertisement for all interfaces.

Use the `no` parameter with this command disable refresh reduction capability advertisement for all interfaces.

Command Syntax

```
refresh-reduction
no refresh-reduction
```

Parameters

None

Default

By default, Refresh reduction mechanism is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#refresh-reduction

(config)#router rsvp
(config-router)#no refresh-reduction
```


© 2021 IP Infusion Inc. Proprietary

rsvp ack-wait-timeout

Use this command to configure the acknowledgment wait timeout for all neighbors detected via the specific interface.

Use the `no` parameter with this command to revert to the default acknowledgment wait timeout for the specified interface.

Command Syntax

```
rsvp ack-wait-timeout <1-65535>
no rsvp ack-wait-timeout <1-65535>
no rsvp ack-wait-timeout
```

Parameters

`<1-65535>`	Specify a value for the acknowledgment wait timeout in seconds. The default timeout value is 10 seconds.

Default

By default, rsvp ack wait timeout is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp ack-wait-timeout 5

(config)#interface eth0
(config-if)#no rsvp ack-wait-timeout 5
```

rsvp message-ack

Use this command to enable message acknowledgment for all messages being sent to the neighbors that have been detected via the specific interface.

Use the `no` parameter with this command to disable message acknowledgment for all messages being sent to the neighbors that have been detected via the specified interface.

Command Syntax

```
rsvp message-ack
```

```
no rsvp message-ack
```

Parameters

None

Default

By default, Message Acknowledgment is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp message-ack

(config)#interface eth0
(config-if)#no rsvp message-ack
```


© 2021 IP Infusion Inc. Proprietary

rsvp refresh-reduction

Use this command to enable Refresh Reduction capability advertisement for a specific interface.

Use the `no` parameter with this command disable Refresh Reduction capability advertisement for the specified interface.

Command Syntax

```
rsvp refresh-reduction
```

```
no rsvp refresh-reduction
```

Parameters

None

Default

Refresh Reduction mechanism is enabled by default for all interfaces.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp refresh-reduction

(config)#interface eth0
(config-if)#no rsvp refresh-reduction
```

© 2021 IP Infusion Inc. Proprietary

CHAPTER 4 Differentiated Services Commands

This chapter describes the RSVP Differentiated Services (DiffServ) commands.

- map-route A.B.C.D
- map-route X:X::X:X
- override-diffserv
- primary map class
- primary elsp-signaled
- primary llsp
- secondary map class
- secondary elsp-signaled
- secondary llsp
- show rsvp diffserv-info

map-route A.B.C.D

Use this command to map a IPv4 prefix route onto a trunk. This route is to be used for packets that are mapped to a specific RSVP trunk.

Use the `no` parameter with this command for unmapping routes from specified trunks.

Command Syntax

```
map-route A.B.C.D A.B.C.D
map-route A.B.C.D A.B.C.D CLASS
map-route A.B.C.D/M
map-route A.B.C.D/M CLASS
no map-route A.B.C.D A.B.C.D
no map-route A.B.C.D A.B.C.D CLASS
no map-route A.B.C.D/M
no map-route A.B.C.D/M CLASS
```

Parameters

`A.B.C.D`	Specify the IPV4 address to be mapped.
`A.B.C.D`	Specify a mask to be applied to the address being mapped.
`A.B.C.D/M`	Specify the IPV4 address to be mapped, with mask.
`CLASS`	Specify the DiffServ Class Name (for example, `be`, `ef` etc.) used for selecting incoming IP packets to be mapped to a specified RSVP trunk.

Default

By default, map route A.B.C.D is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#map-route 1.1.2.2/24 be
```


© 2021 IP Infusion Inc. Proprietary

map-route X:X::X:X

Use this command to map a IPv6 prefix route onto a trunk. This route is to be used for packets that are mapped to a specific RSVP trunk.

Use the `no` parameter with this command for unmapping routes from specified trunks.

Command Syntax

```
map-route X:X::X:X X:X::X:X
map-route X:X::X:X X:X::X:X CLASS
map-route X:X::X:X/M
map-route X:X::X:X/M CLASS
no map-route X:X::X:X X:X::X:X
no map-route X:X::X:X X:X::X:X CLASS
no map-route X:X::X:X/M
no map-route X:X::X:X/M CLASS
```

Parameters

`X:X::X:X`	Specify the IPV6 address to be mapped.
`X:X::X:X`	Specify a mask to be applied to the address being mapped.
`X:X::X:X/M`	Specify the IPV6 address to be mapped, with mask.
`CLASS`	Specify the DiffServ Class Name (for example, `be`, `ef` etc.) used for selecting incoming IP packets to be mapped to a specified RSVP trunk.

Default

By default, map route X:X::X:X is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#map-route 1.1.2.2/24 be
```

override-diffserv

Use this command to enable the Differentiated Services (Diff-Serv) override configuration.

If a Path message is received without a Diff-Serv object by a Diff-Serv enabled node, it can be interpreted either as a request for an E-LSP (EXP-Inferred-PSC LSP) or as a request for Non-Diff-Serv LSP. This command supports the override option and when configured, the LSR interprets a path message without a Diff-Serv object as a request for Non-Diff-Serv LSP.

Use the `no` parameter with this command disable this feature.

Command Syntax

```
override-diffserv
no override-diffserv
```

Parameters

None

Default

By default, override diffserv is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router rsvp
(config-router)#override-diffserv
```


© 2021 IP Infusion Inc. Proprietary

primary map class

Use this command to configure a primary PHB-EXP (Per-Hop Behavior-Experimental) mapping to be used by an E-LSP (EXP-Inferred-PSC LSP). This mapping is different from the node level PHB-EXP mapping.

Use the `no` parameter with this command to remove a PHB-EXP mapping configuration from current E-LSP PHB-EXP mapping.

Command Syntax

```
primary map class <0-7> exp <0-7>
no primary map class <0-7> exp <0-7>
```

Parameters

`<0-7>`	Diff-Serv class (queue) mapped to the particular PHB.
`<0-7>`	Exp bit which is to be mapped to this PHB.

Default

By default, primary map class is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary map class 4 exp 3

(config)#rsvp-trunk T1
(config-trunk)#no primary map class 4 exp 3
```

primary elsp-signaled

Use this command to configure a primary Diff-Serv (Differentiated Services) explicitly signaled E-LSP (EXP-Inferred-PSC LSP) interface.

The classes 1 to 7 are optional parameters that can be selected from node level PHB-EXP (Per-Hop Behavior) mapping as PHBs, which will then be used for an E-LSP. If you do not specify a class with this command, all classes will be selected for the E-LSP.

Use the no parameter with this command to remove the configuration.

Command Syntax

```
primary elsp-signaled
primary elsp-signaled class <0-7>
primary elsp-signaled class <0-7> <0-7>
primary elsp-signaled class <0-7> <0-7> <0-7>
primary elsp-signaled class <0-7> <0-7> <0-7> <0-7>
primary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7>
primary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>
primary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>
no primary elsp-signaled
```

Parameter

CLASS<0-7>	Diff-Serv class (queue).

Default

By default, primary elsp signaled is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary elsp-signaled 2 5 0 6

(config)#rsvp-trunk T1
(config-trunk)#no primary elsp-signaled
```


© 2021 IP Infusion Inc. Proprietary

primary llsp

Use this command to configure a primary Differentiated Services Label-Only-Inferred-PSC (Diff-Serv L-LSP) interface, which will use Diff-Serv Class as its PHB Scheduling Class (PSC).

Use the no parameter with this command to remove the Diff-Serv L-LSP configuration.

Command Syntax

```
primary llsp class <0-7>
no primary llsp
```

Parameters

<0-7>	Diff-Serv class (queue).

Default

By default, primary llsp is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary llsp class 4

(config)#rsvp-trunk T1
(config-trunk)#no primary llsp
```

secondary map class

Use this command to configure a secondary PHB-EXP (Per-Hop Behavior-Experimental) mapping to be used by an E-LSP (EXP-Inferred-PSC LSP). This mapping is different from the node level PHB-EXP mapping.

Use the no parameter with this command to remove a PHB-EXP mapping configuration from current E-LSP PHB-EXP mapping.

Command Syntax

```
secondary map class <0-7> exp <0-7>
no secondary map class <0-7> exp <0-7>
```

Parameters

<0-7>	Diff-Serv class (queue) mapped to the particular PHB.
<0-7>	Exp bit that is to be mapped to this PHB.

Default

By default, secondary map class is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary map class 4 exp 3

(config)#rsvp-trunk T1
(config-trunk)#no secondary map class 4 exp 3
```


© 2021 IP Infusion Inc. Proprietary

secondary elsp-signaled

Use this command to configure a secondary Diff-Serv (Differentiated Services) explicitly signaled E-LSP (EXP-Inferred-PSC LSP) interface. The classes 1 to 7 are optional parameters can be selected from the node level PHB-EXP (Per-Hop Behavior) mapping as PHBs. They will then be used for an E-LSP. If you do not specify a class with this command, all classes will be selected for the E-LSP.

Use the no parameter with this command to remove the configuration.

Command Syntax

```
secondary elsp-signaled
secondary elsp-signaled class <0-7>
secondary elsp-signaled class <0-7> <0-7>
secondary elsp-signaled class <0-7> <0-7> <0-7>
secondary elsp-signaled class <0-7> <0-7> <0-7> <0-7>
secondary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7>
secondary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>
secondary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>
no secondary elsp-signaled
```

Parameters

CLASS<0-7>	Diff-Serv class (queue).

Default

By default, secondary elsp signaled is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary elsp-signaled class 3 6 2 0 5

(config)#rsvp-trunk T1
(config-trunk)#no secondary elsp-signaled
```

secondary llsp

Use this command to configure a secondary Differentiated Services Label-Only-Inferred-PSC (Diff-Serv L-LSP) interface, which will use Diff-Serv Class as its PHB Scheduling Class (PSC).

Use the no parameter with this command to remove the Diff-Serv L-LSP configuration.

Command Syntax

```
secondary llsp class <0-7>
no secondary llsp
```

Parameters

CLASS<0-7>	Diff-Serv class (queue).

Default

By default, secondary llsp is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary llsp class 5

(config)#rsvp-trunk T1
(config-trunk)#no secondary llsp
```


© 2021 IP Infusion Inc. Proprietary

show rsvp diffserv-info

Use this command to display node level Differentiated Services (Diff-Serv) configuration information. This information includes the node level PHB-EXP mapping configured for ELSP-signaled LSP.

Command Syntax

```
show rsvp diffserv-info
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Following is a sample output of the `show rsvp diffserv-info` command.

```
#show rsvp diffserv-info
E-LSP SIGNAL CLASS-EXP mapping:
CLASS    EXP_value
    5      0
    0      1
    1      2
    3      3
    2      4
    4      5
    6      6
    7      7
```

Table 4-294 explains the show command output fields.

Table 4-294: show rsvp diffserv-info output fields

Field	Description
CLASS	MPLS class type that corresponds to the DiffServ traffic engineering class.
EXP_value	Exp value is initialized at the ingress routing device only and overrides the rewrite configuration established for that forwarding class.

© 2021 IP Infusion Inc. Proprietary

CHAPTER 5 DiffServ-TE Commands

This chapter describes the RSVP Differentiated Services-Traffic Engineering (DiffServ-TE) commands.

- primary class-type
- secondary class-type
- show rsvp dste-info

primary class-type

Use this command to configure a primary Class-Type for an LSP session.

Use the `no` parameter with this command to remove the Class-Type configuration.

Command Syntax

```
primary class-type CT-NAME
no primary class-type NAME
```

Parameters

`CT-NAME`	Class-type name to add
`NAME`	Class-type name to remove

Default

By default, primary class type is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary class-type a1
```


© 2021 IP Infusion Inc. Proprietary

secondary class-type

Use this command to configure a secondary Class-Type for an LSP session.

Use the `no` parameter with this command to remove the Class-Type configuration.

Command Syntax

```
secondary class-type NAME
no secondary class-type NAME
```

Parameters

`NAME`	Class-type name

Default

By default, secondary class type is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary class-type a1
```

show rsvp dste-info

Use this command to display the DiffServ-TE configuration information configured in NSM.

Command Syntax

```
show rsvp dste-info
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This command only displays the ready-to-use TE classes and the related class types. When a class type is configured in NSM but is not used by any TE class, this command does not display it.

The following is a sample output of the `show rsvp dste-info` command displaying DiffServ-TE configuration information configured in NSM.

```
#show rsvp dste-info
te0 : {a1, 4}
te1 : {a2, 5}
te3 : {default, 6}
ct0 : default
ct1 : a2
ct2 : a2
#
```

Table 5-295 explains the show command output fields.

Table 5-295: show rsvp dste-info output fields

Field	Description
TE	DiffServ traffic engineering class.
ct	MPLS class type that corresponds to the DiffServ traffic engineering class: ct0—Best effort ct1—Assured forwarding ct2—Expedited forwarding

© 2021 IP Infusion Inc. Proprietary

CHAPTER 6 Point-to-Multipoint Commands

This chapter describes the command for managing Point-to-Multipoint (P2MP) Label Switched Paths (LSPs) in RSVP-TE.

- affinity
- bandwidth
- class-type
- clear rsvp p2mp-session
- destination
- exit-p2mp-lsp
- ext-tunnel-id
- filter
- from
- hold-priority
- hop-limit
- label-record
- pack-affinity
- primary-lsp
- retry-limit
- retry-timer
- route-record
- rsvp-trunk
- secondary-lsp
- setup-priority
- traffic

© 2021 IP Infusion Inc. Proprietary

affinity

Use this command to configure an administrative group and set affinity attributes for a P2MP LSP

Use the no parameter with this command to modify attributes or remove an administrative group from a P2MP LSP.

Command Syntax

Note: The first syntax example is used when Constrained Shortest Path First (CSPF) enabled. The second example is used when CSPF is not enabled.

```
affinity (include-any|exclude-any) ADMIN-GROUP-NAME
affinity (include-any|exclude-any|include-all) ADMIN-GROUP-NAME
no affinity (include-any|exclude-any) ADMIN-GROUP-NAME
no affinity (include-any|exclude-any|include-all) ADMIN-GROUP-NAME
```

Parameters

`include-any`	Include any attribute
`exclude-any`	Exclude any attribute
`include-all`	Include all attributes
`ADMIN-GROUP-NAME`	Name of the administrative group

Command Mode

P2MP LSP mode

Examples

```
#configure terminal
(config-p2mp-lsp)#affinity exclude-any abcd
(config-p2mp-lsp)#no affinity exclude-any abcd

(config-p2mp-lsp)#affinity include-any defg
(config-p2mp-lsp)#no affinity include-any defg
```


© 2021 IP Infusion Inc. Proprietary

bandwidth

Use this command to configure the bandwidth to reserve for a P2MP LSP.

Use the no parameter with this command to remove a bandwidth reservation.

Command Syntax

```
bandwidth BANDWIDTH
no bandwidth
```

Parameters

BANDWIDTH	Maximum bandwidth in bits per second in the range 1 to 10000000000 bits. Usable units include kilobits (k), megabits (m), and gigabits (g).

Command Mode

P2MP LSP mode

Examples

```
(config-p2mp-lsp)#bandwidth 1m
(config-p2mp-lsp)#no bandwidth(config-p2mp-lsp)#bandwidth 1m
(config-p2mp-lsp)#no bandwidth
```

class-type

Use this command to set a DiffServ Traffic Engineering (DSTE) class type for a P2MP LSP when DSTE is enabled.

Use the no parameter with this command to remove a DSTE class type.

Command Syntax

```
class-type CT-NAME
no class-type
```

Parameters

CT-NAME	Class type name

Command Mode

P2MP LSP mode

Examples

```
(config-p2mp-lsp)#class-type ct0
(config-p2mp-lsp)#no class-type
```


© 2021 IP Infusion Inc. Proprietary

clear rsvp p2mp-session

Use this command to clear a P2MP RSVP session.

Command Syntax

```
clear rsvp p2mp-session P2MP-ID TUNNEL-ID EXT-ID LSP-ID INGRESS EGRES
```

Parameters

P2MP-ID	P2MP ID of the session
TUNNEL-ID	Tunnel ID of the session
EXT-ID	Extended tunnel ID of the session
LSP-ID	LSP ID of the session
INGRESS	Ingress of the session
EGRESS	Egress of the session

Command Mode

Privileged Exec and Exec modes

Example

```
#clear rsvp p2mp-session 101 101 1.1.1.1 102 1.1.1.1 4.4.4.4
#
```

destination

Use this command to identify a destination address for a P2MP LSP and set CSPF routing or hop-by-hop routing.

Use the no parameter with this command to remove a destination address.

Note: The default is NO path and CSPF.

Command Syntax

```
destination A.B.C.D (path PATHNAME|) (cspf|no-cspf|)
no destination
```

Parameters

A.B.C.D	Destination address
PATHNAME	Path to use
cspf	Use CSPF for Path computation
no-cspf	Use hop-by-hop routing

Command Mode

P2MP LSP mode

Examples

```
(config-p2mp-lsp)#destination 4.4.4.4
(config-p2mp-lsp)#destination 5.5.5.5 no-cspf
(config-p2mp-lsp)#destination 6.6.6.6 path P1 no-cspf

(config-p2mp-lsp)#no destination 5.5.5.5
(config-p2mp-lsp)#
```


© 2021 IP Infusion Inc. Proprietary

exit-p2mp-lsp

Use this command to exit the P2MP LSP mode and return to Trunk mode. Upon successful execution of this command, the mode is changed to P2MP Trunk mode.

Command Syntax

```
exit-p2mp-lsp
```

Parameters

None

Command Mode

P2MP LSP mode

Examples

```
(config)#rsvp-trunk T1 ipv4 p2mp
(config-p2mp-trunk)#primary-lsp
(config-p2mp-lsp)#exit-p2mp-lsp
(config-p2mp-trunk)#
```

ext-tunnel-id

Use this command to configure an extended tunnel identifier for a P2MP trunk.

Command Syntax

```
ext-tunnel-id A.B.C.D
```

Parameters

A.B.C.D	IPv4 address value of the trunk

Command Mode

RSVP P2MP Trunk mode

Examples

```
(config-p2mp-trunk)#ext-tunnel-id 1.1.1.1
```


© 2021 IP Infusion Inc. Proprietary

filter

Use this command to configure the reservation style to use.

Command Syntax

```
filter (fixed|shared-explicit)
```

Parameters

`fixed`	Use a fixed filter for this trunk
`shared-explicit`	Use a shared-explicit filter for this trunk

Command Mode

P2MP Trunk mode

Examples

```
(config)#rsvp-trunk T1 ipv4 p2mp
(config-p2mp-trunk)#filter shared-explicit
(config-p2mp-trunk)#filter fixed
```

from

Use this command to configure a P2MP tunnel ingress.

Command Syntax

```
from A.B.C.D
```

Parameters

A.B.C.D	IPv4 address of tunnel ingress

Command Mode

P2MP Trunk mode

Examples

```
(config)#rsvp-trunk T1 ipv4 p2mp
(config-p2mp-trunk)#from 1.1.1.1
```


© 2021 IP Infusion Inc. Proprietary

hold-priority

Use this command to configure a hold priority for the P2MP LSP.

Use the no parameter with this command to remove the hold priority for the P2MP LSP.

Command Syntax

```
hold-priority <0-7>
no hold-priority
```

Parameters

<0-7>	Value for hold priority

Command Mode

P2MP LSP Mode

Examples

```
(config-p2mp-lsp)#hold-priority 4

(config-p2mp-lsp)#no hold-priority
(config-p2mp-lsp)#
```

hop-limit

Use this command to set a hop limit for a P2MP LSP

Use the no parameter with this command to remove a configured hop limit.

Command Syntax

```
hop-limit <1-255>
no hop-limit
```

Parameters

<1-255>	Number of acceptable hops

Command Mode

P2MP LSP mode

Examples

```
(config-p2mp-lsp)#hop-limit 55

(config-p2mp-lsp)#no hop-limit
(config-p2mp-lsp)#
```


© 2021 IP Infusion Inc. Proprietary

label-record

Use this command to record labels exchanged by all peers.

Use the no parameter with this command to stop recording labels exchanged by all peers.

Command Syntax

```
label-record
no label-record
```

Parameters

None

Command Mode

P2MP LSP mode

Examples

```
(config-p2mp-lsp)#label-record

(config-p2mp-lsp)#no label-record
(config-p2mp-lsp)#
```

pack-affinity

Use this command to enable affinity packing for session attribute information. When this command is used, affinity information is packed into the session attribute object.

Use the no parameter with this command to disable affinity packing of session attributes.

Command Syntax

```
pack-affinity
no pack-affinity
```

Parameters

None

Command Mode

P2MP LSP mode

Examples

```
(config-p2mp-lsp)#pack-affinity

(config-p2mp-lsp)#no pack-affinity
(config-p2mp-lsp)#
```


© 2021 IP Infusion Inc. Proprietary

primary-lsp

Use this command to configure a primary P2MP LSP. When this command is executed successfully, the mode changes from P2MP Trunk mode to P2MP LSP mode for subsequent configuration of Primary LSP properties.

Use the no parameter with this command to remove a primary P2MP LSP.

Command Syntax

```
primary-lsp
no primary-lsp
```

Parameters

None

Command Mode

P2MP Trunk mode

Examples

```
(config)#rsvp-trunk T1 ipv4 p2mp
(config-p2mp-trunk)# primary-lsp
(config-p2mp-lsp)#
```

retry-limit

Use this command to set a retry count for a P2MP LSP. If you have CSPF enabled, the retry limit you set with this command also becomes the CSPF retry limit, which is the number of times to probe CSPF in case of unsuccessful path computation.

Use the no parameter with this command to reset the retry count to its default value.

Command Syntax

```
retry-limit <1-65535>
no retry-limit
```

Parameters

<1-65535>	Number of times to retry a Path message

Command Mode

P2MP LSP mode

Examples

```
(config-p2mp-lsp)#retry-limit 100

(config-p2mp-lsp)#no retry-limit
(config-p2mp-lsp)#
```


© 2021 IP Infusion Inc. Proprietary

retry-timer

Use this command to set a retry timer for a P2MP LSP. If you have CSPF enabled, the retry timer set with this command also becomes the CSPF retry timer, which is the periodicity of subsequent CSPF probes in case of unsuccessful path computation.

Use the no parameter with this command to reset the retry timer to its default value.

Command Syntax

```
retry-timer <1-600>
no retry-timer
```

Parameters

<1-600>	Timeout, in seconds, between successive Path message retries.

Command Mode

P2MP LSP mode

Examples

```
(config-p2mp-lsp)#retry-timer 200

(config-p2mp-lsp)#no retry-timer
(config-p2mp-lsp)#
```

route-record

Use this command to record the route on the path.

Use the no parameter with this command to stop recording the route on the path.

Command Syntax

```
route-record
no route-record
```

Parameters

None

Command Mode

P2MP LSP mode

Examples

```
(config-p2mp-lsp)#route-record
(config-p2mp-lsp)#no route-record
(config-p2mp-lsp)#
```


© 2021 IP Infusion Inc. Proprietary

rsvp-trunk

Use this command to set up an P2MP trunk for RSVP LSP. Upon successful execution of this command, the mode is changed from RSVP P2MP mode to P2MP Trunk mode for subsequent configuration of trunk properties.

Command Syntax

```
rsvp-trunk TRUNKNAME (ipv4 p2mp|ipv6 p2mp)
rsvp-trunk TRUNKNAME (ipv4|ipv6)
```

Parameters

TRUNKNAME	Name to use for the P2MP trunk
ipv4	IPv4 address family trunk
p2mp	P2MP-enabled trunk
ipv6	IPv6 address family trunk
p2mp	P2MP-enabled trunk

Command Mode

RSVP P2MP mode

Examples

```
(config)#rsvp-trunk T1 ipv4 p2mp
(config-p2mp-trunk)#
```

secondary-lsp

Use this command to configure a secondary P2MP LSP. When this command is executed successfully, the mode changes from P2MP Trunk mode to P2MP LSP mode for subsequent configuration of Primary LSP properties.

Use the no parameter with this command to remove a secondary P2MP LSP.

Command Syntax

```
secondary-lsp
no secondary-lsp
```

Parameters

None

Command Mode

P2MP Trunk mode

Examples

```
(config)#rsvp-trunk T1 ipv4 p2mp
(config-p2mp-trunk)# secondary-lsp
(config-p2mp-lsp)#
```


© 2021 IP Infusion Inc. Proprietary

setup-priority

Use this command to configure a setup priority for the LSP.

Use the no parameter with this command to remove a setup priority.

Command Syntax

```
setup-priority <0-7>
no setup-priority
```

Parameters

<0-7>	Value of setup priority

Command Mode

P2MP LSP mode

Examples

```
(config-p2mp-lsp)#setup-priority 4

(config-p2mp-lsp)#no setup-priority
(config-p2mp-lsp)#
```

traffic

Use this command to set the traffic type for a P2MP LSP.

Use the no parameter with this command to remove a configured traffic type.

Command Syntax

```
traffic (guaranteed|controlled-load)
no traffic
```

Parameters

`guaranteed`	Set traffic type to guaranteed
`controlled-load`	Set traffic type to controlled-load

Command Mode

P2MP LSP mode

Examples

```
(config-p2mp-lsp)#traffic controlled-load

(config-p2mp-lsp)#traffic guaranteed

(config-p2mp-lsp)#no traffic
(config-p2mp-lsp)#
```


© 2021 IP Infusion Inc. Proprietary

CHAPTER 7 Show Commands

This chapter describes the RSVP-TE show commands.

- show debugging rsvp
- show rsvp
- show rsvp admin-groups
- show rsvp control-adjacency
- show rsvp data-link
- show rsvp graceful-restart
- show rsvp dste-info
- show rsvp interface
- show rsvp neighbor
- show rsvp local-addresses
- show rsvp nexthop-cache
- show rsvp path
- show rsvp session
- show rsvp session count
- show rsvp session egress
- show rsvp session ingress
- show rsvp session LSP-NAME
- show rsvp session transit
- show rsvp summary-refresh
- show rsvp trunk
- show rsvp version

show debugging rsvp

This command displays the status of the options selected by the `debug RSVP` command.

Command Syntax

```
show debugging rsvp
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging rsvp
NSM debugging status:
  RSVP event debugging is on
  RSVP packet debugging is on
  RSVP incoming packet debugging is on
  RSVP outgoing packet debugging is on
  RSVP hexadecimal dump debugging is on
#
```

Table 7-296 explains the show command output fields.

Table 7-296: show debugging rsvp output fields

Field	Description
`NSM debugging status`	Debugging is enabled or disabled on a per-interface basis, using the commands.

© 2021 IP Infusion Inc. Proprietary

show rsvp

Use this command to display data about the RSVP daemon.

Command Syntax

```
show rsvp
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp
RSVP Version                  : 1
Process uptime                : 8 minutes
RSVP Refresh Reduction        : Enabled
RSVP Message Acknowledgement  : Disabled
Bundle Send                   : Disabled
NSM Connection                : Up
CSPF Connection               : Up
CSPF usage                    : Enabled
RSVP Refresh Timer            : 5
Keep Multiplier               : 3
Acknowledgement Await Timeout : 10
Explicit-Null For Direct Conn : Disabled
Local Protection              : Disabled
Hello Receipt                 : Disabled
Hello Interval                : 2
Hello Timeout                 : 10
Loop detection                : Enabled (all interface)
Override Diffserv             : Disabled
Ingress                       : 1.1.1.1
Penultimate Hop Popping       : Enabled
Refresh PATH msg parsing      : Enabled
Refresh RESV msg parsing      : Enabled
Detour identification         : Sender-Template

#
```

Table 7-297 explains the show command output fields.

Table 7-297: show rsvp output fields

Field	Description
RSVP Version	Version number associated with the RSVP ingress route.
Process uptime	Duration of the process running time.
RSVP Refresh Reduction	Measure of processing over head requests of refresh messages. Refresh reduction detail extensions improve routing device performance by reducing the process overhead, thus increasing the number of LSPs a routing device can support.
RSVP Message Acknowledgement	Acknowledge message for refresh reductions.
Bundle Send	Disables sending of Bundle Messages for a system.
NSM Connection	The Network Services Module (NSM) sends unsolicited messages to, or receives unsolicited messages from, the QoS (quality of service) module.
CSPF Connection	NSM passes the information to CSPF.
CSPF usage	CSPF finds the shortest path toward the LSP's egress router, taking into account explicit-path constraints.
RSVP Refresh Timer	Time interval used to generate periodic RSVP messages.
Keep Multiplier	Number of RSVP messages that can be lost before an RSVP state is declared stale.
Acknowledgment Await Timeout	The router that initiates the acknowledgment messages for an RSVP session waits for the timeout.
Explicit-Null For Direct Conn	Advertise label 0 to the egress routing device of an LSP. Explicit null: enabled or disabled.
Local Protection	A local repair mechanism is in use to maintain this tunnel.
Hello Receipt	To exchange Hello messages among neighbors.
Hello Interval	Frequency at which RSVP hellos are sent on this interface (in seconds).
Hello Timeout	RSVP Hello State Timer feature detects when a neighbor is down and triggers faster state timeout.
Loop detection	Loop back Detection (LBD) provides protection against loops by transmitting loop protocol packets out of ports where loop protection has been enabled.
Override Diffserv	Diffserv helps to carry the EXP-to-PHB mapping for signaled E-LSP or the PSC value for L-LSP.
Ingress	Information about ingress RSVP sessions.
Penultimate Hop Popping	Removes the label one hop before its destination.
Refresh PATH msg parsing	Refresh message supports the refreshing of RSVP state without the transmission of conventional Path messages.
Refresh RESV msg parsing	Refresh message supports the refreshing of RSVP state without the transmission of conventional Resv messages.
Detour identification	Detours are calculated to avoid the immediate downstream link and node.

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

show rsvp admin-groups

Use this command to display all known administrative groups configured through the NSM for the system.

Command Syntax

```
show rsvp admin-groups
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output showing four administrative groups configured through NSM.

```
#show rsvp admin-groups
 Admin group detail:
  Value of 0 associated with admin group 'a'
  Value of 1 associated with admin group 'b'
  Value of 2 associated with admin group 'c'
  Value of 3 associated with admin group 'd'
#
```

Table 7-298 explains the show command output fields.

Table 7-298: show rsvp admin-groups output field

Field	Description
Admin group detail	Administrative groups details which implements the link coloring of resource classes.

© 2021 IP Infusion Inc. Proprietary

show rsvp control-adjacency

Use this command to display RSVP specific information for control adjacency.

Command Syntax

```
show rsvp control-adjacency
show rsvp control-adjacency CANAME
```

Parameters

CANAME	Use this parameter to display the name of a control-adjacency

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#"show rsvp control-adjacency" without parameters:
Control Adj    Admin status   Oper Status    Peer-address   Gifindex       Control
Channel

#"show rsvp control-adjacency" with parameters:
Admin Status"Enabled" : "Disabled"
Oper Status"Up" : "Down"
Peer-address
Gifindex
Control-Channel in usecc->name : "N/A"
Control-Channel Gifindex
Control-Channel Local-address
Control-Channel Peer-address
Control-Channel ID
Control-Channel Binding Ifindex
Refresh Reduction usage"Disabled" : "Enabled"
Message Acknowledgement"Enabled" : "Disabled"
Bundle Buffer size
Current Epoch Value
Primary IPv4 addressIPv4_address : "N/A"
Primary IPv6 addressIPv6_address : "N/A"
Configured refresh time
Configured keep multiplier
Acknowledgement Await Timeout
Hello Receipt"Enabled" : "Disabled"
Hello Interval
Hello Timeout
Non IANA Hello exchange"Enabled" : "Disabled"
```

Table 7-300 explains the show command output fields.

Table 7-299: show rsvp control-adjacency output field

Field	Description
Control Adj	Control Adjacency status and configuration.
Admin status	Indicates whether the user can administratively disable a peer while still preserving its configuration. Up = Yes, Down = No.
Oper Status	Displays the current status of the cross-connect segment – Up or Down.
Peer-address	Peer address in aa IPv4 and IPv6 format.
Gifindex	Number of gif index on which RSVP is active.
Control Channel	Control Channel status and configuration.
Refresh Reduction usage	Measure of processing over head requests of refresh messages.
Message Acknowledgment	The router that initiates the acknowledgment messages for an RSVP session.
Bundle Buffer size	Number of bundle buffer size.
Current Epoch Value	Value of the database epoch and number of entries in the epoch.
Primary IPv4 address	Primary IPv4 address of the neighbor interface.
Primary IPv6 address	Primary IPv6 address of the neighbor interface.
Configured Refresh Time	Time refresher which takes to generate periodic RSVP messages.
Configured Keep Multiplier	Number of RSVP messages that can be lost before an RSVP state is declared stale.
Acknowledgment Await Timeout	The router that initiates the acknowledgment messages for an RSVP session waits for the timeout.
Hello Receipt	To exchange Hello messages among neighbors.
Hello Interval	Frequency at which RSVP hellos are sent on this interface (in seconds).
Hello Timeout	RSVP Hello State Timer feature detects when a neighbor is down and triggers faster state timeout.
Non IANA Hello exchange	Hello exchange state in the interface.

© 2021 IP Infusion Inc. Proprietary

show rsvp data-link

Use this command to display RSVP specific information for data links.

Command Syntax

```
show rsvp data-link
show rsvp data-link DLNAME
```

Parameters

DLNAME	Data link name

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh rsvp data-link
```

show rsvp graceful-restart

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > output redirection token.

Command Syntax

```
show rsvp graceful-restart
show rsvp graceful-restart A.B.C.D
```

Parameters

A.B.C.D	IPv4 address of a specific neighbor (optional).

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS-SP version 5.0.

Example

```
#show rsvp graceful-restart
Graceful Restart: Enabled
Advertised Restart Time: 180000 msec
Advertised Recovery Time: 360000 msec
Sending Recovery Time: Yes
Remote addr: 172.16.10.2 Local addr: 172.16.10.1
Nbr State: Normal Type: Reroute
Nbr Hello State: Up
LSPs protecting: 0
Restart Time: 0 msec, Recovery Time: 0 msec
Rest of Restart Time: 0 msec, Rest of Recovery Time: 0 msec
```


© 2021 IP Infusion Inc. Proprietary

show rsvp dste-info

Use this command to display data about a DSTE configuration for an RSVP bypass session.

Command Syntax

```
show rsvp dste-info
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp dste-info
te0: { default, 7 }
te1: { data, 6 }
te2: { voice-low, 5 }
te3: { voice-high, 4 }
ct0: default
ct1: data
ct2: voice-low
ct3: voice-high
```

Table 7-300 explains the show command output fields.

Table 7-300: show rsvp dste-info output field

Field	Description
ct0	TE Class and Class type for class 0.
ct1	TE Class and Class type for class 1.
ct2	TE Class and Class type for class 2.
ct3	TE Class and Class type for class 3.

show rsvp interface

Use this command to display data about RSVP-specific information for interfaces, or about a specific interface.

Command Syntax

```
show rsvp interface
show rsvp interface IFNAME
```

Parameter

IFNAME	The name of the interface to display data.

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp interface eth0
Status                          : Enabled
Interface Index                 : 2
Refresh Reduction usage         : Enabled
Message Acknowledgement         : Disabled
Bundle Buffer size              : 65535
Current Epoch Value             : 208043005
Primary IPv4 address            : 10.10.23.1
Primary IPv6 address            : N/A
Interface Type                  : Ethernet
Administrative Group            : a
                                : d
Configured refresh time         : 5
Configured keep multiplier      : 3
Acknowledgement Await Timeout   : 10
Hello Receipt                   : Disabled
Hello Interval                  : 2
Hello Timeout                   : 10
Non IANA Hello exchange         : Disabled
#
```

Table 7-301 explains the show command output fields.

Table 7-301: show rsvp interface output field

Field	Description
Status	Display the status of Resource Reservation Protocol (RSVP).
Interface Index	Number of interface index on which RSVP is active.
Refresh Reduction usage	Measure of processing over head requests of refresh messages.

© 2021 IP Infusion Inc. Proprietary

Table 7-301: show rsvp interface output field

Field	Description
Message Acknowledgement	The router that initiates the acknowledgment messages for an RSVP session.
Bundle Buffer size	Number of bundle buffer size.
Current Epoch Value	Value of the database epoch and number of entries in the epoch.
Primary IPv4 address	Primary IPv4 address of the neighbor interface.
Primary IPv6 address	Primary IPv6 address of the neighbor interface.
Interface Type	Type of interface.
Administrative Group	The administrators who belong to the same administrative group.
Configured Refresh Time	Time refresher which takes to generate periodic RSVP messages.
Configured Keep Multiplier	Number of RSVP messages that can be lost before an RSVP state is declared stale.
Acknowledgment Await Timeout	The router that initiates the acknowledgment messages for an RSVP session waits for the timeout.
Hello Receipt	To exchange Hello messages among neighbors.
Hello Interval	Frequency at which RSVP hellos are sent on this interface (in seconds).
Hello Timeout	RSVP Hello State Timer feature detects when a neighbor is down and triggers faster state timeout.
Non IANA Hello exchange	Hello exchange state in the interface.

© 2021 IP Infusion Inc. Proprietary

show rsvp neighbor

Use this command to display a list of IPv4 RSVP neighbors or just a single IPv4 RSVP neighbor.

Command Syntax

```
show rsvp neighbor
show rsvp neighbor A.B.C.D
```

Parameters

A.B.C.D	Use this parameter to display the IP address of the IPv4 RSVP neighbor.

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp neighbor
IP Address          UpStrm LSP DnStrm LSP RefreshReduc Srefresh In  Type
10.10.20.4          0          1          Enabled      5s           Implicit
10.10.23.2          0          1          Enabled      8s           Implicit
#
```

Table 7-302 explains the show command output fields.

Table 7-302: show rsvp neighbor output field

Field	Description
IP Address	Address for the interface.
UpStrm LSP	Specify the upstream label for the bidirectional label-switched path (LSP).
DnStrm LSP	Specify the dnstream label for the bidirectional label-switched path (LSP).
Refresh Reduc	Refresh reduction improves the scalability, latency, and reliability of Resource Reservation Protocol (RSVP) signaling to enhance network performance and message delivery.
Srefresh In	Remaining seconds for srefresh timer expiry.
Type	Type of neighbor interface.

© 2021 IP Infusion Inc. Proprietary

show rsvp local-addresses

Use this command to display data about any configured RSVP local address, including either IPv4 or IPv6 addresses.

Command Syntax

```
show rsvp local-addresses
show rsvp local-addresses ipv4
show rsvp local-addresses ipv6
```

Parameters

ipv4	Use this parameter to display IPv4 local addresses.
ipv6	Use this parameter to display IPv6 local addresses.

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp local-addresses
IPv4 Addresses:
 Address                        Interface
 4.4.4.40                       lo
 10.1.2.40                      eth0
 14.14.14.8                     eth4
 34.0.0.40                      eth2
 80.0.0.40                      eth2
 127.0.0.1                      lo
IPv6 Addresses:
 Address                        Interface
 ::1                            lo
 fe80::202:b3ff:fed5:8dbb       eth4
 fe80::202:b3ff:fed5:9842       eth2
 fe80::20e:cff:fe83:3727        eth0
#
```

Table 7-303 explains the show command output fields.

Table 7-303: show rsvp local-addresses output field

Field	Description
IPv4 Addresses	IPv4 address for the interface.
IPv6 Addresses	IPv6 address for the interface.

Table 7-303: show rsvp local-addresses output field

Field	Description
Address	Address for the interface.
Interface	Name of the interface.

© 2021 IP Infusion Inc. Proprietary

show rsvp nexthop-cache

Use this command to display the current nexthops being cached by RSVP.

Command Syntax

```
show rsvp nexthop-cache
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp nexthop-cache
Prefix              Nexthop          Outgoing Intf  Valid For   Num Sessions
10.10.20.80/32      0.0.0.0          eth1           12 seconds  1
10.10.23.60/32      0.0.0.0          eth0           17 seconds  1
#
```

Table 7-304 explains the show command output fields.

Table 7-304: show rsvp nexthop-cache output field

Field	Description
Prefix	It is an ordered list and entries are evaluated in order of increasing sequence number.
Nexthop	IP address of the next hop.
Outgoing Intf	Short name of the physical interface through which traffic goes to the protected link.
Valid For	Frequency at which RSVP hellos are sent next hop on this interface (in seconds).
Num Sessions	Number of session in the interface.

show rsvp path

Use this command to display the configured rsvp paths and their configured hops. Specify the pathname to show hops related to a specific path. If no pathname is specified all the rsvp paths are displayed.

Command Syntax

```
show rsvp path
show rsvp path PATHNAME
```

Parameter

PATHNAME	The name of a specific path.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Following are sample outputs from this command, with and without a PATHNAME (PRI) specified.

```
#show rsvp path
Path name: PRI, id: 1
 10.10.11.51 strict
 10.10.12.50 strict
 10.10.13.51 strict

Path name: SEC, id: 2
 10.10.10.51 strict

Path name: loop, id: 3
 10.10.11.51 strict
 10.10.12.50 strict
 10.10.13.51 strict
 10.10.14.50 strict
#

#show rsvp path PRI
Path name: PRI, id: 1
 10.10.11.51 strict
 10.10.12.50 strict
 10.10.13.51 strict
#
```

Table 7-305 explains the show command output fields.

© 2021 IP Infusion Inc. Proprietary

Table 7-305: show rsvp path output field

Field	Description
Path name	Name of the path.
id	Address of the rsvp path.

show rsvp session

Use this command to display session-related information for configured LSPs.

Command Syntax

```
show rsvp session
show rsvp session up
show rsvp session up detail
show rsvp session down
show rsvp session down detail
```

Parameters

`up`	Use this parameter to display sessions that are currently operational.
`down`	Use this parameter to display sessions that are currently not operational.
`detail`	Use this parameter to display detailed session-related information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Following is a sample output from the command using the detail parameter.

```
#show rsvp session detail
Ingress (Primary)
10.10.21.3
  From: 1.1.1.1, LSPstate: Up, LSPname: t1
  Setup priority: 5, Hold priority: 5
  CSPF usage: Disabled
  LSP Protection: None
  Label in: -,  Label out: 16,
  Tspec rate: 10m, Fspec rate: 10m
  Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 1.1.1.1
  Downstream: 10.10.23.2, eth0
  Path refresh: 5 seconds (due in 6772 seconds)
  Resv lifetime: 26 seconds (due in 25 seconds)
  Retry count: 0, intrvl: 30 seconds
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups: none
  Configured Path: p1 (in use)
  Configured Explicit Route Detail :
   10.10.23.2/32 strict
  Session Explicit Route Detail :
   10.10.23.2/32 strict
  Record route: <self> 10.10.23.2 10.10.21.3
  Style: Shared Explicit Filter
```


© 2021 IP Infusion Inc. Proprietary

```
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  LSP Type:  ELSP_SIGNAL
  CLASS    DSCP_value     EXP_value
#
```

Table 7-306 explains the show command output fields.

Table 7-306: show rsvp session output field

Field	Description
Ingress (Primary)	Information about ingress RSVP sessions. Each session has one line of output.
From	Source (ingress switch) of the session.
LSP state	State of the LSP that is being handled by this RSVP session. It can be either Up, Dn (down), or Admin Dn. Admin Dn indicates that the LSP is being taken down gracefully.
LSPname	Name of the LSP.
Setup priority	Value of the setup priority.
Hold priority	Determines the degree to which an LSP holds onto its session reservation after the LSP has been set up successfully.
CSPF usage	CSPF usage state in the rsvp session.
LSP Protection	Protects the traffic failures.
Label in	Incoming label for this LSP.
Label out	Outgoing label for this LSP.
Tspec rate	Sender's traffic specification, which describes the sender's traffic parameters.
Fspec rate	Fspec peak rate values.
Tunnel id	Tunnel address (destination port) for the session.
LSP id	Address of the LSP in the interface.
Ext-Tunnel Id	Session address for the ext-tunnel.
Down stream	Specify the dnstream label for the bidirectional label-switched path (LSP).
Path refresh	Path messages are sent periodically to refresh path states. The refresh interval is controlled by a variable called the refresh time.
Resv lifetime	Number of seconds remaining in the lifetime of the reservation.
Retry count	Number of times sanity polling periodically checks for an error condition in the FPC.
intrvl	Interval sets the time for the messages in order to control the session.
LSP Type	Type of ELSP signal.

show rsvp session count

Use this command to display session-related information for configured LSPs.

Command Syntax

```
show rsvp session count
show rsvp session count egress
show rsvp session count ingress
show rsvp session count transit
```

Parameters

`egress`	Use this parameter to display the number of configured egress sessions.
`ingress`	Use this parameter to display the number of configured ingress sessions.
`transit`	Use this parameter to display the number of configured transmit sessions.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp session count
Total configured: 1520, Up 1520, Down 0
#
```

Table 7-307 explains the show command output fields.

Table 7-307: show rsvp session count output field

Field	Description
Total configured	Number of configured rsvp session in the interface.

© 2021 IP Infusion Inc. Proprietary

show rsvp session egress

Use this command to display session-related information for an egress router.

Command Syntax

```
show rsvp session egress
show rsvp session egress A.B.C.D
show rsvp session egress X:X::X:X
show rsvp session egress detail
show rsvp session egress down
show rsvp session egress down detail
show rsvp session egress up
show rsvp session egress up detail
```

Parameters

A.B.C.D	Use this parameter to display an IPv4 address of an egress router
X:X::X:X	Use this parameter to display an IPv6 address of an egress router
down	Use this parameter to display sessions that are currently not operational
up	Use this parameter to display sessions that are currently operational
detail	Use this parameter to display detailed session-related information

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show rsvp session egress without parameters or with "up" or "down":
%s RSVP:
To              From            State                Pri Rt  Style Labelin
Labelout LSPName                          Uptime  Est.time   DSType
...
Total %d displayed

#show rsvp session egress with parameters:
"Bypass", "Primary", "Detour", "Secondary"
 Make-Before-Break Sibling for session with LSP-ID:prefix4: prefix6
  From: u.prefix4: u.prefix6
LSPstate: %s, LSPname:
      "Up/"Using Backup"/"Using Secondary"
      "Dn",
  Revert hold timer is ON due to expire in %d seconds
  Revert Timer Finished, Forced Switch to Secondary LSP In Effect
  CSPF usage: "Disabled" : "Enabled"
  , CSPF Retry Count: %d, CSPF Retry Interval: %d seconds"
  IGP-Shortcut: Enabled, LSP metric:
```

```
  IGP-Shortcut: Disabled, LSP metric:
  LSP Protection:
  Bypass trunk:
  Label in:
  Label out:
  Tspec rate:
  Fspec rate:
  Policer: Configured
      and installed in hardware
      but not installed in hardware
      Not Configured
  Tunnel Id: %d, LSP Id: %d
Ext-Tunnel Id:
  Downstream:
  Upstream:
  Path refresh: %d seconds (RR enabled), (due in %d seconds)
  Path lifetime: %d seconds (due in %d seconds)
  Resv refresh: %d seconds (due in %d seconds)
  Resv lifetime: %d seconds (due in %d seconds)
  Retry count: %d, intrvl: %d seconds", # remaining, next retry in: %d
seconds",
  RRO re-use as ERO:  "Enabled" : "Disabled"
  Label Recording: "Enabled" : "Disabled"
  FRR Admin Groups/Admin Groups:
     ***admin group info***
  Exclude path detail:
   Exclude "Link" : "Node
   Configured Path: "none" : "in use" : "not in use"
   %s Explicit Route Detail  "Configured" : "Received"
       "strict" : "loose"
  Record route: " <self>") "  ...incomplete"
  Style: %s\n", rsvp_style_to_str (style));
  Traffic type:  "guaranteed" : "controlled-load" : "none"
  Minimum Path MTU:
  Traffic type: N/A
  Minimum Path MTU: N/A
  LSP Type:  "ELSP_SIGNAL" : "ELSP_CONFIG"
  CLASS    DSCP_value     EXP_value
  The class to exp bits mapping is invalid.
  LSP Type:  L-LSP
  LLSP DSCP: %d%d%d%d%d%d   CLASS: %4s",
  DSTE CLass Type Number: Invalid, Class Type name(configured):
  DSTE Class Type Number: %d, Class Type name:
  Last Recorded Error Code: %s (%d)
  Last Recorded Error Value: %s (%d)
  Node where Last Recorded Error originated:
  Trunk Type: "gmpls" : "mpls"
  Tesid:
Merge Point Adderss [%d] =
```

Table 7-308 explains the show command output fields.

© 2021 IP Infusion Inc. Proprietary

Table 7-308: show rsvp session egress output field

Field	Description
LSP state	State of the LSP that is being handled by this RSVP session. It can be either Up, Dn (down), or Admin Dn. Admin Dn indicates that the LSP is being taken down gracefully.
LSP name	Name of the LSP.
CSPF usage	CSPF usage state in the rsvp session.
CSPF Retry Count	Number of times CSPF tried to find the path.
CSPF Retry Interval	The interval at which CSPF retry to find the path.
IGP-Shortcut	Status of IGP shortcut for the RSVP trunk.
LSP metric	Relative/Absolute metric value of the LSP.
LSP Protection	LSP Protection configured for the RSVP trunk.
Bypass trunk	Name for the configured Bypass trunk.
Tspec rate	Sender's traffic specification, which describes the sender's traffic parameters.
Fspec rate	Fspec peak rate values.
Policer	QoS Policy configured for the RSVP trunk.
Tunnel Id	Tunnel identifier (destination port) for the RSVP session.
LSP Id	Address of the LSP in the interface.
Ext-Tunnel Id	Ext Tunnel identifier (destination port) for the RSVP session.
Down stream	Specify the dn stream label for the bidirectional label-switched path (LSP).
Upstream	Address of the previous hop for the egress session.
Path refresh	Path messages are sent periodically to refresh path states. The refresh interval is controlled by a variable called the refresh time.
Path lifetime	Number of seconds remaining in the lifetime of the reservation.
Resv refresh	Remaining time in seconds for the next Resv refresh.
Resv lifetime	Number of seconds remaining in the lifetime of the reservation.
Retry count	Number of times sanity polling periodically checks for an error condition in the FPC.
intrvl	Interval sets the time for the messages in order to control the session.
next retry in	Remaining time in seconds for the next retry.
RRO re-use as ERO	Enabling to re-use Record route as Explicit route for rsvp session.
Label Recording	Enabling to record the labels exchanged by all the peers.
FRR Admin Groups/Admin Groups	Resource affinities associated with the rsvp session.

Table 7-308: show rsvp session egress output field

Field	Description
Exclude path detail	Detailed List of the link addresses to be excluded for RSVP Bypass session.
Exclude Link	Address of the Link to be excluded for RSVP Bypass session.
Configured Path	Configured path name associated with the rsvp session.
Record route	Established rsvp path with each hop information.
Style	Reservation style associated with the rsvp session.
Traffic type	Traffic type associated with the rsvp session.
Minimum Path MTU	Path maximum transmission unit (MTU) discovery in the interface.
LSP Type	Type of ELSP signal.
CLASS	Name of the class which is associated with rsvp session.
DSCP_value	DSCP value of diff-serv class which is associated with rsvp session.
EXP_value	EXP value of diff-serv class which is associated with rsvp sess
DSTE Class Type Number	Diff-serv class type number associated with rsvp session.
Class Type name	Diff-serv class type name associated with rsvp session.
Last Recorded Error Code	The last recorded error code for the RSVP session.
Last Recorded Error Value	The last recorded error for the RSVP session.
Node where Last Recorded Error originated	Error originated node in the rsvp session.
Trunk Type	Trunk type in the rsvp session.
Tesid	Traffic Engineering Service Instance Identifier
Merge Point Adderss	Address of the node where the Bypass LSP joins with the protected LSP.

© 2021 IP Infusion Inc. Proprietary

show rsvp session ingress

Use this command to display session-related information for an ingress router.

Command Syntax

```
show rsvp session ingress
show rsvp session ingress A.B.C.D
show rsvp session ingress X:X::X:X
show rsvp session ingress detail
show rsvp session ingress down
show rsvp session ingress down detail
show rsvp session ingress up
show rsvp session ingress up detail
```

Parameters

A.B.C.D	Use this parameter to display an IPv4 address of an ingress router
X:X::X:X	Use this parameter to display an IPv6 address of an ingress router.
down	Use this parameter to display sessions that are currently not operational
up	Use this parameter to display sessions that are currently operational
detail	Use this parameter to display detailed session-related information

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show rsvp session ingress without parameters or with "up" or "down":
%s RSVP:
To              From            State               Pri Rt  Style Labelin
Labelout LSPName                          Uptime  Est.time   DSType
...
Total %d displayed

#show rsvp session ingress with parameters:
"Bypass", "Primary", "Detour", "Secondary"
 Make-Before-Break Sibling for session with LSP-ID:prefix4: prefix6
  From: u.prefix4: u.prefix6
LSPstate: %s, LSPname:
      "Up/"Using Backup"/"Using Secondary"
      "Dn",
  Revert hold timer is ON due to expire in %d seconds
  Revert Timer Finished, Forced Switch to Secondary LSP In Effect
  CSPF usage: "Disabled" : "Enabled"
  , CSPF Retry Count: %d, CSPF Retry Interval: %d seconds"
```

```
  IGP-Shortcut: Enabled, LSP metric:
  IGP-Shortcut: Disabled, LSP metric:
  LSP Protection:
  Bypass trunk:
  Label in:
  Label out:
  Tspec rate:
  Fspec rate:
  Policer: Configured
      and installed in hardware
      but not installed in hardware
      Not Configured
  Tunnel Id: %d, LSP Id: %d
Ext-Tunnel Id:
  Downstream:
  Upstream:
  Path refresh: %d seconds (RR enabled), (due in %d seconds)
  Path lifetime: %d seconds (due in %d seconds)
  Resv refresh: %d seconds (due in %d seconds)
  Resv lifetime: %d seconds (due in %d seconds)
  Retry count: %d, intrvl: %d seconds", # remaining, next retry in: %d
seconds",
  RRO re-use as ERO:  "Enabled" : "Disabled"
  Label Recording: "Enabled" : "Disabled"
  FRR Admin Groups/Admin Groups:
     ***admin group info***
  Exclude path detail:
   Exclude "Link" : "Node
   Configured Path: "none" : "in use" : "not in use"
   %s Explicit Route Detail  "Configured" : "Received"
       "strict" : "loose"
  Record route: " <self>") "  ...incomplete"
  Style: %s\n", rsvp_style_to_str (style));
  Traffic type:  "guaranteed" : "controlled-load" : "none"
  Minimum Path MTU:
  Traffic type: N/A
  Minimum Path MTU: N/A
  LSP Type:  "ELSP_SIGNAL" : "ELSP_CONFIG"
  CLASS    DSCP_value     EXP_value
  The class to exp bits mapping is invalid.
  LSP Type:  L-LSP
  LLSP DSCP: %d%d%d%d%d%d   CLASS: %4s",
  DSTE CLass Type Number: Invalid, Class Type name(configured):
  DSTE Class Type Number: %d, Class Type name:
  Last Recorded Error Code: %s (%d)
  Last Recorded Error Value: %s (%d)
  Node where Last Recorded Error originated:
  Trunk Type: "gmpls" : "mpls"
  Tesid:
Merge Point Adderss [%d] =
```

Table 7-309 explains the show command output fields.

© 2021 IP Infusion Inc. Proprietary

Table 7-309: show rsvp session ingress output field

Field	Description
LSP state	State of the LSP that is being handled by this RSVP session. It can be either Up, Dn (down), or Admin Dn. Admin Dn indicates that the LSP is being taken down gracefully.
LSP name	Name of the LSP.
CSPF usage	CSPF usage state in the rsvp session.
CSPF Retry Count	Number of times CSPF tried to find the path.
CSPF Retry Interval	The interval at which CSPF retry to find the path.
IGP-Shortcut	Status of IGP shortcut for the RSVP trunk.
LSP metric	Relative/Absolute metric value of the LSP.
LSP Protection	LSP Protection configured for the RSVP trunk.
Bypass trunk	Name for the configured Bypass trunk.
Tspec rate	Sender's traffic specification, which describes the sender's traffic parameters.
Fspec rate	Fspec peak rate values.
Policer	QoS Policy configured for the RSVP trunk.
Tunnel Id	Tunnel identifier (destination port) for the RSVP session.
LSP Id	Address of the LSP in the interface.
Ext-Tunnel Id	Ext Tunnel identifier (destination port) for the RSVP session.
Down stream	Specify the dn stream label for the bidirectional label-switched path (LSP).
Upstream	Address of the previous hop for the egress session.
Path refresh	Path messages are sent periodically to refresh path states. The refresh interval is controlled by a variable called the refresh time.
Path lifetime	Number of seconds remaining in the lifetime of the reservation.
Resv refresh	Remaining time in seconds for the next Resv refresh.
Resv lifetime	Number of seconds remaining in the lifetime of the reservation.
Retry count	Number of times sanity polling periodically checks for an error condition in the FPC.
intrvl	Interval sets the time for the messages in order to control the session.
next retry in	Remaining time in seconds for the next retry.
RRO re-use as ERO	Enabling to re-use Record route as Explicit route for rsvp session.
Label Recording	Enabling to record the labels exchanged by all the peers.
FRR Admin Groups/Admin Groups	Resource affinities associated with the rsvp session.

Table 7-309: show rsvp session ingress output field

Field	Description
Exclude path detail	Detailed List of the link addresses to be excluded for RSVP Bypass session.
Exclude Link	Address of the Link to be excluded for RSVP Bypass session.
Configured Path	Configured path name associated with the rsvp session.
Record route	Established rsvp path with each hop information.
Style	Reservation style associated with the rsvp session.
Traffic type	Traffic type associated with the rsvp session.
Minimum Path MTU	Path maximum transmission unit (MTU) discovery in the interface.
LSP Type	Type of ELSP signal.
CLASS	Name of the class which is associated with rsvp session.
DSCP_value	DSCP value of diff-serv class which is associated with rsvp session.
EXP_value	EXP value of diff-serv class which is associated with rsvp sess
DSTE Class Type Number	Diff-serv class type number associated with rsvp session.
Class Type name	Diff-serv class type name associated with rsvp session.
Last Recorded Error Code	The last recorded error code for the RSVP session.
Last Recorded Error Value	The last recorded error for the RSVP session.
Node where Last Recorded Error originated	Error originated node in the rsvp session.
Trunk Type	Trunk type in the rsvp session.
Tesid	Traffic Engineering Service Instance Identifier.
Merge Point Adderss	Address of the node where the Bypass LSP joins with the protected LSP.

© 2021 IP Infusion Inc. Proprietary

show rsvp session LSP-NAME

Use this command to display information only for sessions with a specified name.

Command Syntax

```
show rsvp session LSP-NAME
show rsvp session LSP-NAME primary
show rsvp session LSP-NAME secondary
```

Parameters

`primary`	Use this parameter to display any primary LSP sessions
`secondary`	Use this parameter to display any secondary LSP sessions

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Usage

Following is a sample output from the command displaying session information about the LSP named `t1`.

```
#show rsvp session t1
Ingress (Primary)
192.168.0.90
  From: 192.168.0.63, LSPstate: Up, LSPname: t1
  Setup priority: 7, Hold priority: 0
  CSPF usage: Disabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  Label in: -,  Label out: 17,
  Tspec rate: 0
  Tunnel Id: 1, LSP Id: 1, Ext-Tunnel Id: 192.168.0.63
  Downstream: 10.10.23.60, eth0
  Path refresh: 30 seconds (due in 34 seconds)
  Resv lifetime 157 seconds (due in 155 seconds)
  Retry Count: 0, Retry Interval: 30 seconds
  RRO re-use as ERO: Enabled
  Labels Recording: Disabled
  Admin Groups: include-any -->  0(a)
  Configured Path: p1 (in use)
  Configured Explicit Route Detail :
   10.10.23.60/32 loose
  Session Explicit Route Detail :
   10.10.23.60/32 loose
   10.10.21.90/32 loose
  Record route: <self> 10.10.23.60 10.10.21.90
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  Last Recorded Error Code: None
  Last Recorded Error Value: None
```

#

Table 7-310 explains the show command output fields.

Table 7-310: show rsvp session LSP-NAME output field

Field	Description
Ingress (Primary)	Information about ingress RSVP sessions. Each session has one line of output.
From	Source (ingress switch) of the session.
LSP state	State of the LSP that is being handled by this RSVP session. It can be either Up, Dn (down), or Admin Dn. Admin Dn indicates that the LSP is being taken down gracefully.
LSPname	Name of the LSP.
Setup priority	Value of the setup priority.
Hold priority	Determines the degree to which an LSP holds onto its session reservation after the LSP has been set up successfully.
CSPF usage	CSPF usage state in the rsvp session.
LSP Protection	Protects the traffic failures.
Label in	Incoming label for this LSP.
Label out	Outgoing label for this LSP.
Tspec rate	Sender's traffic specification, which describes the sender's traffic parameters.
Fspec rate	Fspec peak rate values.
Tunnel id	Tunnel address (destination port) for the session.
LSP id	Address of the LSP in the interface.
Ext-Tunnel Id	Session address for the ext-tunnel.
Down stream	Specify the dnstream label for the bidirectional label-switched path (LSP).
Path refresh	Path messages are sent periodically to refresh path states. The refresh interval is controlled by a variable called the refresh time.
Resv lifetime	Number of seconds remaining in the lifetime of the reservation.
Retry count	Number of times sanity polling periodically checks for an error condition in the FPC.
intrvl	Interval sets the time for the messages in order to control the session.
RRO re-use as ERO	Enabling to re-use Record route as Explicit route for rsvp session.
Label Recording	Enabling to record the labels exchanged by all the peers.
Admin Groups	Resource affinities associated with the rsvp session.
Configured Path	Configured path name associated with the rsvp session.

© 2021 IP Infusion Inc. Proprietary

Table 7-310: show rsvp session LSP-NAME output field

Field	Description
Configured Explicit Route Detail	Configured explicit route with each hop information.
Session Explicit Route Detail	Established explicit route with each hop information.
Record route	Established rsvp path with each hop information.
Style	Reservation style associated with the rsvp session.
Traffic type	Traffic type associated with the rsvp session.
Minimum Path MTU	Path maximum transmission unit (MTU) discovery in the interface.
Last Recorded Error Code	Recorded error code for the last time service ran.
Last Recorded Error Value	No Recorded error value for the last time service ran.

show rsvp session transit

Use this command to display session-related information for the transit or intermediate router.

Command Syntax

```
show rsvp session transit
show rsvp session transit detail
show rsvp session transit up
show rsvp session transit down
show rsvp session transit up detail
show rsvp session transit down detail
```

Parameters

`up`	Use this parameter to display sessions that are operational
`down`	Use this parameter to display sessions that are not operational
`detail`	Use this parameter to display detailed session-related information

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Following are sample outputs from the command displaying detailed session information for the transit router.

```
#show rsvp session transit detail
Transit (Primary)
10.10.21.3
  From: 1.1.1.1, LSPstate: Up, LSPname: t1
  Setup priority: 5, Hold priority: 5
  LSP Protection: None
  Label in: 16,  Label out: 3,
  Tspec rate: 10m, Fspec rate: 10m
  Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 1.1.1.1
  Downstream: 10.10.21.3, eth1   Upstream: 10.10.23.1, eth3
  Path refresh: 5 seconds (due in 6155 seconds)
  Path lifetime: 26 seconds (due in 25 seconds)
  Resv refresh: 5 seconds (due in 2533 seconds)
  Resv lifetime: 26 seconds (due in 25 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups:   Received Explicit Route Detail :
   10.10.23.2/32 strict
  Record route: 10.10.23.1 <self> 10.10.21.3
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  LSP Type:  ELSP_SIGNAL
```


© 2021 IP Infusion Inc. Proprietary

```
  CLASS    DSCP_value     EXP_value
  af43      100110           7
  DSTE Class Type Number: 0, Class Type name: default
#
```

Table 7-311 explains the show command output fields.

Table 7-311: show rsvp session transit output field

Field	Description
Transit (Primary)	Transit RSVP sessions information in the interface.
From	Source (ingress switch) of the session.
LSP state	State of the LSP that is being handled by this RSVP session. It can be either Up, Dn (down), or Admin Dn. Admin Dn indicates that the LSP is being taken down gracefully.
LSP name	Name of the LSP.
Setup priority	Value of the setup priority.
Hold priority	Determines the degree to which an LSP holds onto its session reservation after the LSP has been set up successfully.
LSP Protection	Protects the traffic failures.
Label in	Incoming label for this LSP.
Label out	Outgoing label for this LSP.
Tspec rate	Sender's traffic specification, which describes the sender's traffic parameters.
Fspec rate	Fspec peak rate values.
Tunnel id	Tunnel address (destination port) for the session.
LSP id	Address of the LSP in the interface.
Ext-Tunnel Id	Session address for the ext-tunnel.
Down stream	Specify the dnstream label for the bidirectional label-switched path (LSP).
Path refresh	Path messages are sent periodically to refresh path states. The refresh interval is controlled by a variable called the refresh time.
Resv lifetime	Number of seconds remaining in the lifetime of the reservation.
RRO re-use as ERO	Enabling to re-use Record route as Explicit route for rsvp session.
Label Recording	Enabling to record the labels exchanged by all the peers.
Admin Groups	Resource affinities associated with the rsvp session.
Configured Explicit Route Detail	Configured path name associated with the rsvp session.

Table 7-311: show rsvp session transit output field

Field	Description
Record route	Recorded route for the session, taken from the record route object. Normally this value will be the same as that of explct route. Differences indicate that path rerouting has occurred, typically during fast reroute.
Style	Reservation style associated with the rsvp session.
Traffic type	Traffic type associated with the rsvp session.
Minimum Path MTU	Path maximum transmission unit (MTU) discovery in the interface.
LSP Type	Type of LSP for Diffserv services(E-LSP or L-LSP).
CLASS	Name of the class which is associated with rsvp session.
DSCP_value	DSCP value of diff-serv class which is associated with rsvp session.
EXP_value	EXP value of diff-serv class which is associated with rsvp session.
DSTE Class Type Number	Diff-serv class type number associated with rsvp session.
Class Type name	Diff-serv class type name associated with rsvp session.

© 2021 IP Infusion Inc. Proprietary

show rsvp summary-refresh

Use this command to display RSVP summary refresh data.

Command Syntax

```
show rsvp summary-refresh
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp summary-refresh:
Neighbor Addr       Tunnel ID  LSP ID     Ingress             Egress
```

Table 7-312 explains the show command output fields.

Table 7-312: show rsvp trunk output field

Field	Description
Neighbor Addr	Neighbor address on the primary address of the interface.
Tunnel ID	Tunnel identifier (destination port) for the RSVP session.
LSP ID	Address of the LSP in the interface.
Ingress	Information about ingress RSVP sessions.
Egress	Information about egress RSVP sessions.

show rsvp trunk

Use this command to display information for a specific trunk or for all trunks.

Command Syntax

```
show rsvp trunk
show rsvp trunk NAME
show rsvp trunk detail
```

Parameters

NAME	Enter the name of a trunk
detail	Use this parameter to display detailed information for all trunks

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp trunk
Trunk Name      Trunk ID  Type       # Sess       Egress Address(es)
T1              101       P2P             1       4.4.4.4
T2              102       P2P             2       5.5.5.5
Total trunks configured: 3.
#
```

Following is a sample output from the command using the detail parameter.

```
#show rsvp trunk detail
Trunk name: T1, tunnel-id: 101
 Type: P2P
 Ext-tunnel-id: 1.1.1.1/32
 Egress: 4.4.4.4/32
 # of LSPs in trunk: 1
 Mapped-routes: none

Trunk name: T2, tunnel-id: 102
 Type: P2P
 Ext-tunnel-id: 1.1.1.1/32
 Egress: 5.5.5.5/32
 # of LSPs in trunk: 2
 Mapped-routes: none
```

Table 7-313 explains the show command output fields.

© 2021 IP Infusion Inc. Proprietary

Table 7-313: show rsvp trunk output field

Field	Description
Trunk Name	Name of the trunk.
Trunk ID	Session address for the trunk.
Type	Trunk type in the rsvp session.
Sess	Number of sessions associated with rsvp trunk.
Egress	Information about egress RSVP sessions.
Total trunks configured	Number of configured trunk in the rsvp session.
Ext-tunnel-id	Extended Tunnel identifier (destination port) for the RSVP session.
Mapped-routes	Map the route of the interface.

show rsvp version

Use this command to display the version of the RSVP daemon. Current RSVP version is 1.

Command Syntax

```
show rsvp version
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp version
Resource ReSerVation Protocol, version 1. rfc2205
   RSVP protocol      = Enabled
   R(refresh timer)   = 30 seconds
   K(keep multiplier) = 3
   Preemption         = Normal
#
```

Table 7-314 explains the show command output fields.

Table 7-314: show rsvp version output field

Field	Description
Resource Reservation Protocol	RSVP software version.
RSVP protocol	Status of RSVP.
R (refresh timer)	Configured time interval used to generate periodic RSVP messages.
K (keep multiplier)	Number of RSVP messages that can be lost before an RSVP state is declared stale.
Preemption	Currently configured preemption capability.

© 2021 IP Infusion Inc. Proprietary

SECTION 16 Glossary

Glossary

Conventions

This document uses the conventions described below.

Sort Order

The terms are arranged in ASCII order with the case of the characters ignored. This is the same as if the terms were sorted by this Linux command:

sort -f

This means that spaces, symbols, and digits come before alphabetic characters. Digits are sorted as strings, not numeric values (“10” comes before “2”).

The exact ASCII collating sequence is as shown below, with a space character in the first position:

```
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
```

There are some exceptions to this rule when it makes more sense than strict ASCII order:

- (S,G) is under S
- G.8032 and G.8032 are under Numbers

Acronyms

The full phrase is shown before the acronym. For example:

- network address translation (NAT)
- Local Area Network (LAN)

An exception is when the acronym is used exclusively to refer to the term, in which case the acronym is shown before the full form:

- I-SID (Service Instance Identifier)
- NETCONF (Network Configuration Protocol)

When an acronym is part of a phrase and is defined separately, its full form is not shown:

- BGP confederation
- FEC-to-NHLFE (FTN) map
- GARP VLAN Registration Protocol (GVRP)
- MAC address

Case

As shown in the examples above, all lowercase is used for terms except when the predominant usage is initial uppercase or all uppercase.

© 2021 IP Infusion Inc. Proprietary

© 2021 IP Infusion Inc. Proprietary

Terms

Numbers

1588v2. IEEE specification for Precision Time Protocol (PTP).

802. A family of IEEE Local Area Network (LAN) standards. The services and protocols specified by the 802 standards map to Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model:

- 802.1: Overview architecture of LANs and interneworking
- 802.2: The logical link control (LLC) sublayer of Layer 2 (L2)
- 802.3: Layer 1 (L1) and the Media Access Control (MAC) sublayer of Layer 2 (L2), Also called Ethernet.

802.1AB. IEEE specification for Link Layer Discovery Protocol (LLDP).

802.1ad. Amendment to IEEE 802.1Q for Provider Bridging (PB).

802.1ag. Amendment to IEEE 802.1Q for Connectivity Fault Management (CFM).

802.1ah. IEEE specification that adds Provider Backbone Bridging (PBB) to 802.1ad Provider Bridging (PB):

802.1ak. Amendment to IEEE 802.1Q for Multiple Registration Protocol (MRP).

802.1aq. Amendment to IEEE 802.1D for Shortest Path Bridging (SPB).

802.1AX. IEEE specification for link aggregation and Multi-Chassis Link Aggregation (MC-LAG).

802.1D. IEEE specification which allows multiple LANs to be connected together through what the standard calls a “MAC bridge” which filters data sent between LAN segments, allowing networks to be partitioned for administrative purposes and reducing network congestion. The more common term for a MAC bridge is switch. The 802.1D standard includes Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

802.1p. IEEE 802.1Q defines priority signaling for traffic that can be used by Quality of Service (QoS) mechanisms to differentiate traffic. Packets are tagged as belonging to a queue, which determines the priority of the packet. Although this technique is often called “802.1p”, there is no standard by that name. Instead, the technique is incorporated into 802.1Q standard.

802.1Q. IEEE Virtual Local Area Network (VLAN) and Multiple Spanning Tree Protocol (MSTP) specifications. This standard refers to VLANs as “virtual bridged networks”. The 802.1D standard covers “VLAN-unaware” switches, while 802.1Q extends 802.1D for “VLAN-aware” switches.

802.1Qau. Amendment to IEEE 802.1Q for Quantized Congestion Notification (QCN).

802.1Qay. Amendment to IEEE 802.1Q for Provider Backbone Bridge-Traffic Engineering (PBB-TE).

802.1Qaz. Amendment to IEEE 802.1Q for Data Center Bridging Capability Exchange (DCBX) and Enhanced Transmission Selection (ETS).

802.1Qbb. Amendment to IEEE 802.1Q for Priority-based Flow Control (PFC).

802.1Qbg. Amendment to IEEE 802.1Q for Edge Virtual Bridging (EVB).

802.1v. Amendment to IEEE 802.1Q to classify incoming packets based on data link layer protocol identification.

802.1X. IEEE specification for port authentication.

802.3ah. IEEE specification for Ethernet to the First Mile (EFM).

802.3x. IEEE specification for flow control.

G.8032. ITU-T specification for Ethernet Linear Protection Switching (ELPS).

G.8032. ITU-T specification for Ethernet Ring Protection Switching (ERPS).

A

Access Control List (ACL). A set of rules used to filter traffic. Each rule specifies a set of conditions (such as source address, destination address, type of packet, or combination of these items) that a packet must meet to match the rule. When a device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether the packet is permitted or denied.

access layer. In the network design model, the layer that connects devices such as desktops, laptops, servers, and printers to the network and provides end users access to network resources. This layer accepts traffic into a network and can pass that traffic to the distribution layer. The access layer is usually built using Layer 2 (L2) switching such as Spanning Tree Protocol (STP). This layer connects logical broadcast domains and provides isolation to groups of users. Typically, Virtual Local Area Network (VLAN) instances are implemented as broadcast domains in the access layer. Also called the edge layer. See also customer edge (CE), provider edge (PE).

acknowledgment (ACK). Notification sent from one network device to another to acknowledge that some event (for example, receipt of a message) has occurred.

active route. Route chosen from all routes in a Routing Information Base (RIB) to reach a destination. Active routes are installed in the Forwarding Information Base (FIB).

address. A unique identifier for a device on a network, either as a sender or receiver. An address can be a physical address or a logical address.

See also address family, address resolution, Classless Interdomain Routing (CIDR), domain name, Domain Name Service (DNS), dynamic address, IP address, MAC address, name resolution, static address.

address family. A specific type of network addressing supported by a routing protocol. Examples are IPv4 unicast and IPv4 multicast.

address resolution. The process of translating the address of an entity on one system to the equivalent address of the same entity on another system. For instance, translating an IP address to its Domain Name Service (DNS) name. See also Address Resolution Protocol (ARP).

Address Resolution Protocol (ARP). A Transmission Control Protocol/Internet Protocol (TCP/IP) mechanism that maps a MAC address to an IP address in the ARP cache data structure. Defined in RFC 826. See also Neighbor Discovery Protocol (NDP).

© 2021 IP Infusion Inc. Proprietary

adjacency. The relationship between neighboring devices for exchanging routing information. Adjacent devices share a common network segment.

A given device can have multiple adjacencies, but each adjacency consists of only two devices connected by one link. A protocol data unit (PDU) that goes between them does not have to pass through any other network devices. See also neighbor.

administrative distance. How reliable the source of the route is considered to be. A lower value is preferred over a higher value. An administrative distance of 255 indicates no confidence in the source; routes with this distance are not installed in the Routing Information Base (RIB). Also called route preference.

Advanced Encryption Standard (AES). A cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information. Defined in Federal Information Processing Standards (FIPS) PUB 197.

advertising. Process in which routing or service updates are sent at specified intervals so that other devices on the network can maintain lists of usable routes.

Agent Extensibility (AgentX). A protocol used to implement Simple Network Management Protocol (SNMP) that defines communications between an SNMP agent and an SNMP client. AgentX does not directly communicate with an SNMP client, but relies on the agent to handle the protocol details of SNMP. Defined by RFC 2741.

aggregate route. A single entry in a routing table that represents a combination of groups of routes that have common addresses. See also route summarization.

alarm indication signal (AIS). A signal transmitted instead of the normal signal to maintain transmission continuity and to indicate to the receiving device that a transmission interruption (fault) has occurred either at the equipment originating the AIS signal or upstream of that equipment.

American National Standards Institute (ANSI). A voluntary organization of corporate, government, and other members that develops international and U.S. standards relating to, among other things, communications and networking. ANSI is a member of the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO).

application-specific integrated circuit (ASIC). An integrated circuit that is designed for a specific application.

area. A logical division of devices that maintains detailed routing information about itself as well as routing information that allows it to reach other routing subdomains. An area divides a network into small, manageable pieces, reducing the amount of information each device must store and maintain about all other devices.

In Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF), an area is a set of contiguous networks and hosts within an autonomous system (AS) that have been administratively grouped together.

area border router (ABR). A router on the border of one or more Open Shortest Path First (OSPF) areas that connects those areas to the backbone network. An ABR is a member of both the OSPF backbone and its attached areas. Therefore, an ABR maintains routing tables for both the backbone topology and the topology of the other areas. See also Not-So-Stubby-Area (NSSA), stub area.

authentication. A process that verifies that data is not altered during transmission and ensures that users are communicating with the individual or organization that they believe they are communicating with.

authentication, authorization, and accounting (AAA). A framework for controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services:

- Authentication determines who the user is and whether to grant that user access to the network

- Authorization determines what the user can do
- Accounting tracks the user's activities and provides an audit trail that can be used for billing or resource tracking

See also Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+).

Authentication Header (AH). An Internet Protocol Security (IPsec) protocol that authenticates either all or part of the contents of a packet by adding a header with a a hash message authentication code (HMAC) calculated based on the values in the packet. AH provides authentication but not confidentiality. See also Encapsulating Security Payload (ESP).

Automatic Protection Switching (APS). A means to detect a signal failure or signal degrade on a working channel and switch traffic to a protection channel. There are two types of APS:

- Ethernet Linear Protection Switching (ELPS)
- Ethernet Ring Protection Switching (ERPS)

autonomous system (AS). A network controlled as a single administrative entity sharing a common routing strategy. An autonomous system is subdivided into areas. An AS runs an Interior Gateway Protocol (IGP) such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or Intermediate System to Intermediate System (IS-IS) within its boundaries. An AS uses an Exterior Gateway Protocol (EGP) to exchange routing information with other ASs.

autonomous system border router (ASBR). An area border router (ABR) located between an Open Shortest Path First (OSPF) autonomous system (AS) and a non-OSPF network. ASBRs run both OSPF and another routing protocol, such as Routing Information Protocol (RIP).

An ASBR is a link between the OSPF autonomous system and the outside network. An ASBR exchanges routing information with routers in other ASes. The ASBR redistributes routing information received from other ASs throughout its own AS. An ASBR must reside in a standard OSPF area.

availability. The amount of time that a system is available during time periods when it is expected to be available. Availability is often measured as a percentage of an elapsed year. For example, 99.95% availability equates to 4.38 hours of downtime in a year (0.0005 * 365 * 24=4.38) for a system that is expected to be available all the time.

B

B-MAC. A source and destination backbone MAC address (B-AA and a B-DA) in a Provider Backbone Bridging (PBB) header.

B-TAG. See backbone VLAN (B-VLAN).

backbone. The part of a network used as the primary path for transporting traffic between network segments.

backbone core bridge (BCB). A device that bridges frames based on backbone VLAN (B-VLAN) and backbone MAC address (B-MAC) information in a Provider Backbone Bridging (PBB) network core.

backbone edge bridge (BEB). A device that encapsulates customer frames for transmission across a Provider Backbone Bridging (PBB) network. There are two types:

- B-BEB (B type BEB): Contains a B-component for bridging in the provider space based on backbone MAC address (B-MAC) and backbone VLAN (B-VLAN) information.

© 2021 IP Infusion Inc. Proprietary

- I-BEB (I type BEB): Contains an I-component for bridging in the customer space based on customer MAC address (C-MAC) and service VLAN (S-VLAN) information.

backbone VLAN (B-VLAN). A field in a Provider Backbone Bridging (PBB) header that carries the backbone VLAN identifier information. The format is the same as a service VLAN (S-VLAN) tag. Also called B-VID tag, B-TAG.

backhaul. The part of a hierarchical network that connects small subnetworks at the edge of the network to the core or backbone network.

In wireless backhaul, the part of the network that transports traffic from a cellular base station to a core network that routes and switches voice and data traffic.

bandwidth. A measure of the data transfer rate of a communications transport medium.

base station. An earth-based transmitting/receiving station for cellular phones and other wireless transmission systems.

Bellman-Ford algorithm. Used in distance-vector routing protocols such as Routing Information Protocol (RIP) to determine the best path to all routes in the network. Contrast with Dijkstra algorithm.

best effort. Traffic class in which the network forwards as many packets as possible in as reasonable a time as possible. By default, packets not explicitly assigned to a specific traffic class are assigned to the best-effort class.

BGP confederation. A method to solve scaling problems created by the iBGP full-mesh requirement. BGP confederations effectively break up a large autonomous system (AS) into subautonomous systems (sub-ASs). Each sub-AS must be uniquely identified within the confederation AS by a sub-AS number.

Within a sub-AS, the same iBGP full mesh requirement exists. Connections to other confederations are made with eBGP, and peers outside the sub-AS are treated as external. To avoid routing loops, a sub-AS uses a confederation sequence, which operates like an AS path but uses only the privately assigned sub-AS numbers.

BGP neighbor. Another device on the network that is running Border Gateway Protocol (BGP). There are two types of BGP neighbors: internal neighbors in the same autonomous system (AS) and external neighbors in different autonomous systems.

BGP peer. A remote Border Gateway Protocol (BGP) speaker that is an established neighbor of the local BGP speaker. BGP peers do not have to be directly connected to each other to share a BGP session.

BGP speaker. A router configured to run the Border Gateway Protocol (BGP) routing protocol. A BGP speaker must be explicitly configured with a set of BGP peers with which it exchanges routing information.

Bidirectional Forwarding Detection (BFD). Protocol that reduces the reliance upon the relatively slow hello mechanism in routing protocols to detect failures where no hardware signaling is available. BFD works with Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) v2, and Intermediate System to Intermediate System (IS-IS) to enable them to receive failure notifications. Defined in RFCs 5880 and 5881.

bit error rate (BER). The ratio of error bits to the total number of bits transmitted. A BER is generally shown as a negative exponent (for example, 10-7, which means one out of 10,000,000 bits is in error).

Border Gateway Protocol (BGP). An Exterior Gateway Protocol (EGP) that maintains a table of IP networks, or prefixes, which designate network reachability among autonomous system (AS) instances. BGP uses path-vector routing that makes decisions based on path, network policies, and/or rule sets. BGP is the primary protocol for the global Internet. First defined by RFC 1163.

BGP Version 4 (BGP4) defined in RFC 4271 supports Classless Interdomain Routing (CIDR) and route summarization.

BGP performs these tasks:

- Collects information about reachable networks from neighboring autonomous systems
- Advertises its reachable networks to routers inside the AS and to neighboring autonomous systems
- Selects routes if there are multiple routes available.

Each BGP device can have both external and internal connections to other BGP devices:

- Internal BGP (iBGP) connections are within the same autonomous system
- External BGP (eBGP) connections are between different autonomous systems

The configuration and behavior is slightly different between eBGP and iBGP.

You can use iBGP for multihomed BGP networks (with more than one connection to the same external autonomous system).

To avoid routing loops, iBGP does not advertise routes learned from an internal BGP peer to other internal BGP peers. Instead, BGP requires that all internal peers be fully meshed so that any route advertised by one router is advertised to all peers within the autonomous system (AS). As a network grows, the full-mesh requirement becomes difficult to manage. To combat scaling problems, BGP uses route reflection and BGP confederations.

Multiprotocol BGP (MP-BGP) allows different types of addresses (address families) to be distributed in parallel. MP-BGP supports IPv4 and IPv6 addresses as well as unicast and multicast variants of each. Defined in RFC 4760. See also IPv6 Provider Edge (6PE).

See also community.

bridge. A device operating at Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model that forwards frames from one network segment to another based on the MAC address.

The term bridge also describes a device that connects collision domains. Collisions that appear on one side of a switch are not allowed to propagate to the other.

Originally, bridges only had two ports, with each one connected to a network segment. Later, bridges had multiple ports that could connect more than two network segments as well as directly connecting hosts. As bridges evolved, they were also able to filter frames, that is, forward only certain traffic from one network segment to another. This type of device is sometimes called an intelligent bridge, but the more modern term is switch. The term “bridge” is somewhat archaic but is still often used in standards documents.

bridge protocol data unit (BPDU). A protocol data unit (PDU) sent by switches running the Spanning Tree Protocol (STP) to learn about other switches in the network and maintain the spanning tree.

broadcast. The process of a single host simultaneously sending the same message to all nodes on a network. Compare to multicast, where a only a subset of the receivers are addressed. See also unicast.

bursty. The tendency of the bandwidth needed in a network to vary greatly from one moment to the next.

C

C-MAC. A source and destination customer MAC address (C-SA and a C-DA) in a Provider Backbone Bridging (PBB) header.

C-TAG. See customer VLAN (C-VLAN).

© 2021 IP Infusion Inc. Proprietary

Carrier Ethernet. Extensions to Ethernet that enable network operators to provide Ethernet services to customers and to use Ethernet technology in their networks. See also Metro Ethernet Forum (MEF).

certificate. Electronic document that identifies a person or entity. Through the use of keys and certificates, the entities exchanging data can authenticate each other.

channel. A connecting path that carries information from a sending device to a receiving device. A channel can refer to a physical medium (such as a coaxial cable or fiber optic cable).

circuit. A communications channel or path between two devices capable of carrying electrical current.

circuit switching. A network where a dedicated circuit must be opened between devices before they can communicate and, while the circuit is open, no other devices may use that circuit or parts of it. A circuit can remain open without any information transmission, and still be unusable by other devices; it must be closed before it is available to other users. Contrast with packet switching.

Class of Service (CoS). A way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, video, voice, file transfer) together and treating each type as a class with its own level of service priority. However, no guarantees are made that a given priority will meet any specified minimum level. See also Quality of Service (QoS).

classful IP addressing. An older addressing scheme for configuring the ratio of networks to hosts using fixed length prefixes. See Classless Interdomain Routing (CIDR).

Classless Interdomain Routing (CIDR). A notation for specifying an IP addresses and its network prefix which appends a slash character to the address and a decimal number indicating the leading bits in the network prefix. For example:

- In the IPv4 notation “192.168.0.0/16”:
  - “192.168” (the first 16 bits) defines the network address.
  - .0.0 up to .255.255 refer to the host addresses on that network. This leaves 16 bits to contain host addresses, enough for 65536 host addresses.
- In the IPv6 notation “2001:db8::/32”:
  - “2001:db8” (the first 32 bits) defines the network address.
  - :0:0:0:0:0:0 to:ffff:ffff:ffff:ffff:ffff:ffff refer to host addresses on that network. This leaves 96 bits to contains host addresses, enough for 7,922,816,251,426,433 host addresses.

The lower the number after the slash, the more hosts contained in that block.

CIDR uses variable length subnet masking (VLSM) based on arbitrary length prefixes. In VLSM, the number of network and host bits assigned to a subnet can vary based on the number of hosts the subnet needs to support.

CIDR replaced traditional classful IP addressing, in which address allocation was based on octet (8-bit) boundary segments of the IP address. In CIDR, the boundary between the network and host portions of an IP address can be on any bit boundary. The old classful A, B, and C network designations correspond to CIDR prefixes of /8, /16, or /24. 192.168.0.0/16 corresponds to an old class B network. With CIDR, finer grained division of networks are possible, down to individual IP addresses, such as 192.168.100.2/32.

CIDR routes can be carried by Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Routing Information Protocol (RIP).

Before CIDR notation, IPv4 networks were represented using dotted decimal notation for both the address and a subnet mask.

Also called route summarization or supernetting.

client/server architecture. A computing architecture that distributes processing between clients and servers on the network. A client program makes a service request from a server which fulfils the request.

collapsed core. Collapsing the core layer and the distribution layer into one layer (one device) in the network design model. A collapsed core design reduces cost, while maintaining most of the benefits of the network design model for small networks that do not grow significantly larger over time.

collision domain. A network segment where data frames can collide with one another when being sent on a shared medium such as Ethernet. Hosts in a collision domain arbitrate among themselves using an access control mechanism.

command-line interface (CLI). Environment for entering commands to configure and monitor routing and switching software and hardware.

committed information rate (CIR). The average rate at which packets are admitted to the network. Each packet is counted as it enters the network. Packets that do not exceed the CIR are marked green, which corresponds to low loss priority. Packets that exceed the CIR but are below the peak information rate (PIR) are marked yellow, which corresponds to medium loss priority.

common and internal spanning tree (CIST). A single topology connecting all Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP) switches into one active topology. In other words, an entire spanning tree fabric.

common spanning tree (CST). The topology connecting all Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP) *switches* and multiple spanning-tree (MST) region *instances*. An MST region appears as a single switch to spanning tree configurations outside the region.

community. In Border Gateway Protocol (BGP), a logical group of prefixes or destinations that share a common attribute; used to simplify a routing policy. Community members can be on different networks and in different autonomous systems.

In Simple Network Management Protocol (SNMP), an authentication scheme that authorizes SNMP clients based on the source IP address of incoming SNMP packets, defines which Management Information Base (MIB) objects are available, and specifies the operations (read-only or read-write) allowed on those objects.

congestion. The state in which the network load exceeds the available resources such as link capacity or memory buffers.

connection-oriented. A packet switching technology where a virtual circuit between sending and receiving devices makes it seem like the devices are connected by a switched circuit with a fixed bandwidth without regard to their physical addresses. In a connection-oriented service, packets always reach their destination in the same order as they were sent. Transmission Control Protocol (TCP) is a connection-oriented transport service. See also connectionless.

Connection-oriented protocols can be used to send information that requires a constant delay and bandwidth such as voice and video.

connectionless. A packet switching technology where the source and destination addresses are included in each packet so that a direct connection or an established session between sender and receiver is not required for communications. In a connectionless service, each packet is handled independently of all others, and packets might not reach their destination in the same order in which they were sent. User Datagram Protocol (UDP) is a connectionless transport service. See also connection-oriented.

© 2021 IP Infusion Inc. Proprietary

Connectivity Fault Management (CFM). An Operation, Administration, and Maintenance (OAM) protocol that can manage Ethernet services and detect, verify, and isolate connectivity failures in VLANs. CFM enables service providers to configure:

- Maintenance association End Point (MEP) on a per-port, per-VLAN, or per-domain basis
- Maintenance domain Intermediate Point (MIP) on a per-port and per-level basis

CFM can operate over a LAN segment, customer VLAN (C-VLAN), service VLAN (S-VLAN), backbone VLAN (B-VLAN), or backbone identified by an I-SID (Service Instance Identifier). Defined by IEEE 802.1ag and 802.1ah.

Constrained Shortest Path First (CSPF). An extension of shortest path first (SPF). The path computed using CSPF is the shortest path that fulfills a set of constraints. After running the shortest path algorithm, the paths are pruned, removing those links that violate a given set of constraints.

See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Content Addressable Memory (CAM). An integrated circuit in a device that stores a table used to make frame forwarding and classification decisions. CAM can perform a massively parallel search of entries in the table much faster than a serial search than in conventional Random Access Memory (RAM).

There are two types of CAM:

- Binary CAM: A binary lookup that returns either a 1 or 0. A MAC address in an Ethernet frame comes into a switch, the switch looks in its MAC address table and either finds that MAC address or does not (1 or 0).
- Ternary CAM (TCAM): A binary lookup that returns either a 1 or 0 but also has a “do not care” bit. TCAM can have multiple matches and can determine a best match. This is necessary because Classless Interdomain Routing (CIDR) lookups need a longest prefix match. For example, 192.168.1.7/32 matches both 192.168.1.0/24 and 192.168.1.0/25. The closest match to 192.168.1.7/32 is 192.168.1.0/25 which would be chosen.

Continuity Check Message (CCM). A multicast Connectivity Fault Management (CFM) protocol data unit (PDU) transmitted periodically by a Maintenance association End Point (MEP) in ensure continuity over the Maintenance Association (MA) to which the transmitting MEP belongs.

control plane. The part of switch or router architecture that makes decisions about where traffic is sent. Control plane processing is the “signalling” of the network. Anything that is needed to get routing and switching working on a device is considered part of the control plane. The control plane serves the data plane.

The control plane functions include the manual system configuration and management operations performed by a network administrator. The control plane functions also include dynamic routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or Border Gateway Protocol (BGP) that exchange topology information with other routers and construct a Routing Information Base (RIB).

The control plane functions are not performed on each arriving individual packet, so they do not have a strict speed constraint and are not time-critical.

Control plane packets are sent to or are locally originated by the device itself.

convergence. The synchronization process that a network must go through immediately after a topology change. Convergence time is the time required to update all the devices on the network with the routing information changes. See also routing table.

core layer. In the network design model, the layer that provides a transit function to access the internal network and external networks. The core layer moves packets between distribution layer devices. The core layer also links to the devices at the enterprise edge to support Internet, virtual private networks (VPN), extranet, and WAN access.

The core layer uses Layer 3 (L3) routing protocols that scale well and converge quickly such as Open Shortest Path First (OSPF).

The core serves as the backbone for the network and is critical for connecting distribution layer devices, so it is important for the core to be fast with low-latency, reliable, and scalable.

Also called backbone or trunk.

count-to-infinity. A distance-vector routing problem where if A tells B that it has a path somewhere, there is no way for B to know if the path has B as a part of it.

The count-to-infinity problem is caused by a link failure that partitions the network into two or more segments. When the network is partitioned, devices in one part of the segment cannot reach devices in the other part of the segment. The distance-vector algorithm adjusts the distance value slowly upwards toward infinity.

The count-to-infinity problem can be solved through split horizon methods.

cryptography. Rendering information unintelligible and restoring encrypted information to an intelligible form.

customer edge (CE). A device that provides an interface between a Local Area Network (LAN) and an enterprise or service provider core network. Outbound packets from the LAN are forwarded from the CE to a provider edge (PE) device, and inbound packets are forwarded from the PE to the CE.

customer VLAN (C-VLAN). In a Provider Bridging (PB) frame, a field that identifies the customer VLAN. See also service VLAN (S-VLAN). Also called C-TAG.

D

daemon. A background program that runs unattended and is usually invisible to users and that provides important system services. Pronounced “dee-mon” or “day-mon”.

Data Center Bridging (DCB). A collection of extensions for Ethernet that allows LANs and Storage Area Networks (SANs) to use a single unified fabric in a data center. DCB can carry Fibre Channel, TCP/IP, and inter-process communication traffic over a single, converged Ethernet network. DCB features include:

- Priority-based Flow Control (PFC)
- Enhanced Transmission Selection (ETS)
- Quantized Congestion Notification (QCN)
- Data Center Bridging Capability Exchange (DCBX)

Data Center Bridging Capability Exchange (DCBX). Defined in IEEE 802.1Qaz, a protocol that uses Link Layer Discovery Protocol (LLDP) to convey configuration of Data Center Bridging (DCB) features between neighbors.

data communications equipment (DCE). The interface between data terminal equipment (DTE) and a network.

Data Encryption Standard (DES). A method of data encryption using a private (secret) key. There are 72 quadrillion or more possible encryption keys that can be used. For each given message, the key is chosen at random from among these. Both the sender and the receiver must know and use the same private key.

In triple DES (3DES), a symmetric-key block cipher applies the DES cipher algorithm three times to each data block.

data link layer. See Layer 2 (L2).

data plane. The part of switch or router architecture that forwards frames and packets arriving on an interface. Routers and switches use what the control plane has built to process incoming frames and packets. The data plane

© 2021 IP Infusion Inc. Proprietary

forwards traffic to the next hop along the path to the destination according to the control plane logic. Data plane frames or packets go *through* the device.

Also called forwarding plane.

data terminal equipment (DTE). Any device such as a host, router, or switch connected to a network. A DTE connects to a network through data communications equipment (DCE).

default gateway. A router that connects hosts on a network segment to the Internet.

default route. A route used to forward Internet Protocol (IP) packets when a more specific route is not present in the Routing Information Base (RIB). Often represented as 0.0.0.0/0, the default route is sometimes called the “route of last resort”.

Differentiated Services (DiffServ). A mechanism to classify and manage network traffic and provide Quality of Service (QoS) guarantees for service providers. DiffServ extends the Resource Reservation Protocol—Traffic Engineering (RSVP-TE). DiffServ enables traffic to be prioritized by class, so that certain kinds of traffic, for example voice traffic, can take precedence over other types of traffic.

DiffServ redefines bits in the type of service (ToS) field of an IP packet header. DiffServ uses the Differentiated Services Code Point (DSCP) field for the QoS priority and supports 64 levels of classification.

Defined by RFC 2474; Multi-Protocol Label Switching (MPLS) support is defined in RFCs 3270 and 4124.

Differentiated Services Code Point (DSCP). A six-bit field in an IP header that enables service providers to allocate resources on a per-packet basis to meet customer requirements. See also Differentiated Services (DiffServ).

Diffie–Hellman. A method of securely exchanging cryptographic keys that allows two parties with no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Digital Signature Algorithm (DSA). An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Dijkstra algorithm. An algorithm used by Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) to make routing decisions based on link state. Also called shortest path first (SPF). Contrast with Bellman-Ford algorithm.

distance-vector routing. A family of routing algorithms that calculate the best route to use to send data based on information from adjacent (directly connected) routers on the network.

“Distance-vector” means that routes are advertised with two characteristics:

- Distance: How far it is to the destination based on a metric such as the number of hops, cost, bandwidth, or delay.
- Vector: The direction (exit interface) of the next hop router to reach the destination.

Each router sends its neighbors a list of networks it can reach and the distance to that network. For each network path, the receiving router picks the neighbor advertising the lowest metric, then adds this entry into its Routing Information Base (RIB). These best paths are advertised to each adjacent router.

Routing information is broadcast periodically rather than only when a change occurs, which makes the method compute- and bandwidth-intensive. For this reason, a distance-vector algorithm is best used in relatively small networks with few interrouter connections.

The Bellman-Ford algorithm is often used to determine the best path, which is used by the Routing Information Protocol (RIP).

Distance-vector routing can be prone to routing loops which are avoided through split horizon techniques.

Contrast with link-state routing and shortest-path routing.

distribution layer. In the network design model, the layer that aggregates the data received from the access layer and sends it to the core layer or to other segments of the local network. Routers or multilayer switches in the distribution layer performs many functions including:

- Routing between subnetworks and Virtual Local Area Network (VLAN) instances in the access layer
- Managing access control, routing, filtering, and QoS policies
- Managing firewalls and network address translation (NAT)
- Managing queues and prioritizing traffic
- Summarizing routes before advertising them to the core
- Isolating the core from access layer failures or disruptions

The distribution layer uses Layer 3 (L3) routing to connect to the core layer and Layer 2 (L2) switching to connect to the access layer.

Also called the aggregation layer or concentration layer.

domain. A representation of all or a subset of a network used for addressing and administrative purposes. Also refers to a collection of routers that use a common Interior Gateway Protocol (IGP). See also area and autonomous system (AS).

domain name. A meaningful and easy-to-remember name for an IP address. A domain name is a sequence of names (labels) separated by periods such as “example.com”.

Domain Name Service (DNS). A service that translates a domain name into a numeric IP address needed to locate devices. The DNS database is hierarchical. When a client such as a Web browser gives a request that specifies a host name, the DNS resolver on the client first contacts a DNS server to determine the server's IP address. If the DNS server does not contain the needed mapping, it forwards the request to a different DNS server at the next higher level in the hierarchy. After potentially several forwarding and delegation exchanges within the DNS hierarchy, the IP address for the given host eventually arrives at the client. Defined in RFCs 1034 and 1035.

dotted decimal. A method of representing an IPv4 address as four decimal numbers separated by dots, or periods; for example, 194.65.87.3. See also IP address.

double colon. A notation used to represent a consecutive block of zeroes in the middle of an IPv6 address. For example, given this address:

FE80:0000:0000:0000:0202:B3FF:FE1E:8329

With double colon notation, the address shown above becomes:

FE80::0202:B3FF:FE1E:8329

You can only use the double colon notation once in an address.

double tagged. See Provider Bridging (PB).

dynamic address. An address assigned to a device on a network with no regard to matching a specific address to that device. When a client device (such as a laptop) is given a dynamic address, it simply receives one from a pool of available addresses. It might or might not be allocated the same IP address as on previous connections. See also Dynamic Host Configuration Protocol (DHCP).

© 2021 IP Infusion Inc. Proprietary

Dynamic Host Configuration Protocol (DHCP). A protocol where a client can obtain an IP address and other information such as default gateway, subnet mask, and Domain Name Service (DNS) servers, for the client to use to connect to a network. Defined in RFCs 2131 and 3315. See also Transmission Control Protocol/Internet Protocol (TCP/IP).

A DHCP server “leases” an IP address for a predetermined period of time, and reclaims the address for reassignment at the expiration of that period. DHCP greatly simplifies the administration of large networks, and networks in which nodes such as laptops, tablets, and smart phones frequently join and leave.

dynamic routing. A technique used by routing protocols where devices send and receive messages about the network topology to and from other devices and update a local Routing Information Base (RIB) used to locate the best available path to a destination.

There are different forms of dynamic routing: distance-vector routing, link-state routing, and path-vector routing. Several protocols use dynamic routing such as Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

Also called adaptive routing. Contrast with static routing.

E

east/west. The flow of traffic traversing a data center or cloud horizontally between servers. Contrast with north/south.

Edge Virtual Bridging (EVB). A mechanism that enables a virtual switch to send all traffic to an adjacent physical switch. This moves the forwarding decisions and network operations from the host CPU to the switch. EVB leverages the advanced management capabilities in access or aggregation layer switches. Defined by IEEE 802.1Qbg.

egress. Outbound or outgoing, referring to a protocol data unit (PDU) exiting a device. See also ingress.

encapsulation. The technique used by layered protocols in which a layer adds its own header information to the protocol data unit (PDU) from the layer above. As an example, in the Open Systems Interconnection (OSI) Reference Model, a PDU can contain a header for Layer 1 (L1), followed by a header for Layer 2 (L2), followed by a header for the Layer 3 (L3), followed by a header for the transport layer (Transmission Control Protocol (TCP), followed by data for the higher layers.

encryption. The process of encoding information in an attempt to make it secure from unauthorized access, particularly during transmission. The reverse of this process is known as decryption. Two main encryption schemes are in common use:

- Private (symmetrical) key: Using a private encryption key known to both the sender and the receiver of the information.
- Public (asymmetrical) key: Using a public key to encrypt and a private key to decrypt.

See also Data Encryption Standard (DES).

end-of-row switch. A chassis-based switch in a rack or cabinet at either end of the server row in a data center that connects to hundreds of servers in that row. Each cabinet in the row has cabling connecting 48 (or more) servers to the end-of-row switch. An end-of-row switch typically has redundant supervisor engines, power supplies, and overall better high availability characteristics than a Top-of-Rack (ToR) switch.

An end-of-row switch extends Layer 1 (L1) cabling topology from the switch to each rack, resulting in a smaller Layer 2 (L2) footprint and fewer Spanning Tree Protocol (STP) nodes in the topology.

Enhanced Transmission Selection (ETS). A protocol for assigning bandwidth to frame priorities. Defined in IEEE 802.1Qaz.

equal-cost multipath (ECMP). A forwarding mechanism for routing traffic along multiple paths of equal cost that ensures load balancing. The link-state routing protocols that use a cost-based metric such as Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) explicitly allow ECMP routing.

Encapsulating Security Payload (ESP). An Internet Protocol Security (IPsec) protocol that ensures confidentiality by encrypting IP packets. An encryption algorithm combines the data in a packet with a key to transform the packet into an encrypted form. At the destination, the packet is decrypted it using the same algorithm. ESP also ensures the integrity of a packet using a hash message authentication code (HMAC). ESP also supports an authentication scheme like that used in Authentication Header (AH), or can be used in conjunction with AH.

Ethernet. A specification for a LAN technology at Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model based on packetized transmissions between physical ports over a variety of electrical and optical media. Ethernet can transport several upper-layer protocols, the most popular of which is Transmission Control Protocol/Internet Protocol (TCP/IP). Ethernet standards are maintained by the IEEE 802.3 committee.

Ethernet uses a bus topology and CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to resolve contention when two devices try to access the network at exactly the same time. Transmission speeds range from 10 Mbps, to Fast Ethernet at 100 Mbps, to Gigabit Ethernet at 1000 Mbps.

Ethernet Linear Protection Switching (ELPS). A type of Automatic Protection Switching (APS) that specifies these techniques:

- Linear 1+1 (One-plus-One) operates with either uni-directional or bi-directional switching; normal traffic is copied and fed to both working and protection transport entities
- Linear 1:1 (One-to-One) operates with bi-directional switching; normal traffic is transported either on the working transport entity or on the protection transport entity, using a selector bridge at the source

Defined by ITU-T G.8032.

Ethernet Local Management Interface (E-LMI). An Operation, Administration, and Maintenance (OAM) protocol for communications between two User-to-Network Interface (UNI) instances. E-LMI provides both UNI and Ethernet Virtual Connection (EVC) status information to customer edge devices. This information enables automatic configuration of customer edge operation based on the configuration. Defined by Metro Ethernet Forum (MEF) 16.

Ethernet Ring Protection Switching (ERPS). A type of Automatic Protection Switching (APS) that protects traffic in a ring topology by ensuring that no loops are within the ring. Loops are prevented by blocking traffic on either a predetermined link or a failed link. ERPS integrates Operation, Administration, and Maintenance (OAM) functions with a simple APS protocol. An Ethernet ring uses normal learning, forwarding, filtering, and flooding mechanisms and a forwarding database (FDB). Defined by ITU-T G.8032.

Ethernet to the First Mile (EFM). A set of extensions to the 802.3 MAC and MAC sub layer. EFM describes technologies and the physical layer specifications for subscriber access, including remote failure detection, remote loop back, and link monitoring. Defined by IEEE 802.3ah.

Ethernet Virtual Connection (EVC). An association of two or more instances of a User-to-Network Interface (UNI). There are three types of EVC:

- In a point-to-point EVC, exactly two UNIs are associated with one another.
- In a multipoint EVC, two or more UNIs are associated with one another.

© 2021 IP Infusion Inc. Proprietary

- In a rooted-multipoint EVC, one or more of the UNIs must be designated as root and each of the other UNIs must be designated as a leaf. If root, the UNI can send service frames to all other points in the EVC; if leaf, the UNI can send and receive service frames to and from root only.

Explicit Route Object (ERO). An extension to Resource Reservation Protocol (RSVP) that allows a path message to traverse an explicit sequence of routers that is independent of conventional shortest-path IP routing.

Exterior Gateway Protocol (EGP). An interdomain protocol such as Border Gateway Protocol (BGP) used to exchange network reachability information between autonomous system (AS) instances. Contrast with Interior Gateway Protocol (IGP).

F

FEC-to-NHLFE (FTN) map. In Multi-Protocol Label Switching (MPLS), a mapping from the forwarding equivalence class (FEC) of incoming packets to the corresponding Next Hop Label Forwarding Entry (NHLFE).

filtering. The process of determining whether to forward a frame or packet through a port. The simplest form of filtering is to not forward frames out the same port on which they were received. A network administrator can configure filtering manually or a device can be "self-learning" and record the source addresses of devices on each segment of a network in a filtering database.

Filtering behavior is sometimes referred to as "drop, flood, or forward":

- If the switch determines that the destination MAC is on the same port, it does not forward the frame, dropping it.
- If the switch determines that the destination MAC is on a different port, it forwards the frame on that port.
- If the switch does not know where to send the frame (or if it is multicast or broadcast), the frame is flooded out all ports (except the port it was received on).

filtering database. A data structure in a switch that maps addresses to ports, addresses to VLANs, and/or ports to VLANs. A switch learns the location of hosts by recording the source MAC address-port number association for each frame received at an incoming port. All future transmissions destined to a MAC address in the filtering database are only directed to the port associated with that MAC address unless the transmission originated on that port.

A switch can also be configured and act as several independent switches by creating VLAN associations to switch ports.

flapping. Condition of network instability when a route is announced and then withdrawn repeatedly, usually as the result of an intermittently failing link. Also called route flapping.

flooding. Forwarding a frame onto all ports except the port upon which it arrived. In Open Shortest Path First (OSPF), distributing and synchronizing the link-state database (LSDB) between routers.

flow control. Any mechanism that prevents a source from sending faster than the destination is capable of receiving.

Forward Error Correction (FEC). A system of error control that allows the receiver to correct some errors without having to request a re-transmission of data.

forwarding. Finding the output port to which a frame needs to go, and relaying the frame to that port.

forwarding equivalence class (FEC). A set of packets with similar characteristics that are forwarded in the same manner, on the same path, with the same forwarding treatment, and using the same Multi-Protocol Label Switching

(MPLS) label. FECs are defined by the Label Distribution Protocol (LDP). FECs are also represented in other label distribution protocols.

Forwarding Information Base (FIB). A data structure used to find the interface to which to forward a packet. The FIB contains the minimum amount of information required to make a forwarding decision for a particular packet, such as destination prefix and nexthop. The FIB is an abbreviated form of the information in the Routing Information Base (RIB).

Also called forwarding table.

frame. A protocol data unit (PDU) at Layer 2 (L2) with addressing and protocol control information. A frame contains a header field and a trailer field that "frame" the user data. (Some control frames contain no data.)

See also packet.

G

GARP Multicast Registration Protocol (GMRP). A Generic Attribute Registration Protocol (GARP) application that allows switches to exchange multicast group information with other GMRP switches, prune unnecessary broadcast traffic, and dynamically create and manage multicast groups. See also Multiple MAC Registration Protocol (MMRP).

GARP VLAN Registration Protocol (GVRP). A Generic Attribute Registration Protocol (GARP) application that provides VLAN registration services. A switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs. Defined by 802.1Q. See also Multiple VLAN Registration Protocol (MVRP).

gateway. A device that understands and converts between two different networking models. Since Transmission Control Protocol/Internet Protocol (TCP/IP) has become the dominant model, gateways are not used much at this time.

See also default gateway.

Generic Attribute Registration Protocol (GARP). A generic framework for devices to register attributes, such as VLAN identifiers and multicast group membership. See also Multiple Registration Protocol (MRP).

generic routing encapsulation (GRE). A tunneling protocol that encapsulates Layer 3 (L3) packets inside IP packets. GRE provides a virtual point-to-point link over an IP network. GRE is completely insecure, but provides a fast and simple way to access a remote network.

graceful restart. A process that allows a router whose control plane is restarting to continue forwarding traffic while recovering its state from neighboring routers. Without graceful restart, a control plane restart disrupts services provided by the router. Also called nonstop forwarding.

gratuitous ARP. Broadcast request for a router's own IP address to check whether that address is being used by another node. Used to detect IP address duplication.

H

hash message authentication code (HMAC). A method of calculating a message authentication code (MAC) using a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it can be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or SHA-2, can be used to calculate an HMAC.

© 2021 IP Infusion Inc. Proprietary

header. The portion of a protocol data unit (PDU) that contains control information for the message such as destination address, source address, input sequence number, the type of message, and priority level.

hello packet. A multicast packet that is used by protocols for neighbor discovery and recovery. Hello packets also indicate that a client is still operating and network-ready.

high availability. The ability of a system or component to limit or avoid network disruption when a component fails. High availability provides both hardware and software methods to minimize downtime and improve the performance of a network.

hold down. A state that a route is placed into so that devices will neither advertise the route nor accept advertisements about the route for a specific length of time (the hold down period). A hold down is used to flush bad information about a route from all devices in a network. A route is placed into hold down when a link in that route fails.

hop. A single link between two computer systems that a protocol data unit (PDU) must cross on its way to its destination. See also hop count.

hop count. The number of links that must be crossed to get from a source to a destination. A protocol data unit (PDU) might pass over many hops to reach its destination. If it must pass between five computers, it is said to have taken four hops to reach its destination. Hop count is often used as a metric for evaluating a route in distance-vector routing. Routing Information Protocol (RIP) uses hop count as its sole metric.

host. A computer connected to a network that is assigned a Layer 3 (L3) address and that provides an access point to that network. Similar to a node, except that host usually implies a computer system, whereas node generally applies to any networked device such as a router or switch.

hypervisor. A thin operating system designed solely to provide virtualization. A hypervisor drives physical hardware, executes virtual machine (VM) instances, and dynamically shares the underlying hardware with the associated virtual hardware. A hypervisor does not serve as a general-purpose operating system, but instead provides the platform on which VMs can run.

I

I-SID (Service Instance Identifier). A field in an I-TAG that defines the service instance to which the Provider Backbone Bridging (PBB) frame is mapped.

I-TAG. Field in the Provider Backbone Bridging (PBB) header that carries the I-SID (Service Instance Identifier) associated with the frame.

Incoming Label Map (ILM). In Multi-Protocol Label Switching (MPLS), a mapping from incoming labels to corresponding Next Hop Label Forwarding Entry (NHLFE).

ingress. Inbound or incoming, referring to a protocol data unit (PDU) entering a device. See also egress.

Institute of Electrical and Electronics Engineers (IEEE). A coordinating body for computing and communications standards. The IEEE mainly covers Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model. (Pronounced “eye-triple-ee”.) See http://www.ieee.org.

interface. The point at which a connection is made between two devices. An interface describes the logical and physical connections and usually means the same thing as the term port.

Interior Gateway Protocol (IGP). An intradomain protocol used to exchange network reachability and routing information among devices within an autonomous system (AS), such as Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), or Routing Information Protocol (RIP). Contrast with Exterior Gateway Protocol (EGP).

Intermediate System to Intermediate System (IS-IS). An Interior Gateway Protocol (IGP) that floods link state information throughout a network of routers. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information. A Routing Information Base (RIB) is calculated from the database by constructing a shortest path tree (SPT).

Like Open Shortest Path First (OSPF), IS-IS uses the Dijkstra algorithm to find the best path through a network. Packets are then forwarded, based on the computed ideal path, through the network to the destination.

Defined by International Organization for Standardization (ISO) 10589.

internal spanning tree (IST). A special type of multiple spanning-tree instance (MSTI) that runs in an multiple spanning-tree (MST) region. An IST connects all the switches in the MST region and appears as a subtree in the common and internal spanning tree (CIST) that encompasses the entire switched domain.

An IST is identified by the number zero (0) and exists on all ports; you cannot delete the IST. By default, all VLANs are assigned to the IST. The IST is the only spanning tree instance that sends and receives bridge protocol data unit (BPDU) messages.

Any other spanning tree instance within an MST region is called a multiple spanning-tree instance (MSTI).

International Organization for Standardization (ISO). An international standards body that establishes global standards for communications and information exchange. Voting members are designated standards bodies of participating nations; American National Standards Institute (ANSI) is the U.S. member of the ISO. The Open Systems Interconnection (OSI) Reference Model is one of the ISO's most widely accepted recommendations.

Sometimes mistakenly referred to as the "International Standards Organization". Because "International Organization for Standardization" has different acronyms in different languages (IOS in English, OIN in French for *Organisation internationale de normalisation*), the founders gave it the short form ISO. ISO is derived from the Greek *isos*, meaning "equal".

For more, see http://www.iso.org/iso/home.html.

International Telecommunication Union (ITU). An international organization that develops standards for telecommunications. Formerly known as the CCITT. See http://www.itu.int.

Internet. The world's largest computer network, serving universities, commercial interests, government agencies, and private individuals. The Internet uses Transmission Control Protocol/Internet Protocol (TCP/IP) protocols, and Internet computers and devices run many different operating systems.

No government agency, single person, or corporate entity controls the Internet. All decisions on methods and standards are made by standards groups based on input from users.

See also Internet Engineering Task Force (IETF); Request for Comments (RFC).

Internet Control Message Protocol (ICMP). An Internet Protocol (IP) that provides management and control functions. Routers send ICMP messages to respond to undeliverable datagrams by placing an ICMP message in an IP datagram and then sending the datagram back to the original source. ICMP is also used by the ping (packet internet groper) command and enables a host to discover addresses of operating routers on the subnet. Defined in RFC 792.

IPv6 makes greater use of ICMP (ICMPv6 defined in RFC 4443) than IPv4, including neighbor solicitation, neighbor advertisement, router solicitation, router advertisement, and redirect.

© 2021 IP Infusion Inc. Proprietary

Internet Engineering Task Force (IETF). An international community of network designers, operators, vendors, and researchers that develops Request for Comments (RFC) documents that define protocols and specifications for the Internet. The IETF mainly covers Layer 2 (L2) and Layer 3 (L3) of the Open Systems Interconnection (OSI) Reference Model. See http://www.ietf.org.

Internet Group Management Protocol (IGMP). An IPv4 protocol that allows hosts to add or remove themselves from a multicast group. Defined by RFC 3376.

IGMP enables receivers to register that they want to receive a particular multicast transmission, but does not route multicast traffic from the source to receivers. That task is left to a multicast routing protocol, such as Protocol Independent Multicast (PIM).

See also Multicast Listener Discovery (MLD), multicast group, (S,G).

Internet Key Exchange (IKE or IKEv2). An Internet Protocol Security (IPsec) protocol used to set up a security association (SA) by negotiating keys in secret. IKE builds upon Internet Security Association and Key Management Protocol (ISAKMP) using X.509 certificates for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. In addition, a security policy for every peer which will connect must be manually maintained.

The IKE protocol runs in two phases. The first phase establishes a ISAKMP SA which is used in the second phase to negotiate and set up the IPsec SAs.

Internet Protocol (IP). A Layer 3 (L3) protocol that provides connectionless delivery of data across heterogeneous physical networks. IP provides features for addressing, type-of-service, fragmentation and reassembly, and security. Defined by RFCs 791 and 1349.

Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IP is best effort and provides no guarantees of reliability, so if packets are lost in transit, accidentally duplicated, arrive in the wrong order, or arrive corrupted, no effort is made to address the problem on the IP level—that is left to protocols a layer above, such as Transmission Control Protocol (TCP).

Internet Protocol Security (IPsec). A protocol suite for securing IP communications by authenticating and encrypting packets during a communication session. Authentication Header (AH) and Encapsulating Security Payload (ESP) are the main wire-level protocols used by IPsec. Before either AH or ESP can be used, however, the two devices must share a public key through Internet Key Exchange (IKE or IKEv2).

RFC 2401 specifies the base architecture for IPsec compliant systems. RFCs 2402, 2406, and 2407 provide more details about IPsec.

Internet Security Association and Key Management Protocol (ISAKMP). A framework for authentication and key exchange with actual authenticated keying material provided either by manual configuration with pre-shared keys or Internet Key Exchange (IKE or IKEv2). See also Internet Protocol Security (IPsec).

IP address. A unique number that identifies a device on an Internet Protocol (IP) network. IP addresses have two formats:

- An IPv4 address is 32 bits and is usually written in dotted decimal notation as four decimal numbers separated by periods. For example, 192.168.50.4 is an IPv4 address.
- An IPv6 address is 128 bits and is written in a hexadecimal notation of eight 16-bit parts separated by colons. For example, FE80:0000:0000:0000:0202:B3FF:FE1E:8329 is an IPv6 address. In the double colon address format, consecutive colons (“::”) represent successive 16-bit blocks that contain zeros: FE80::0202:B3FF:FE1E:8329. While a much larger address space is a feature, IPv6 also has other features such as multicast support, jumbograms (packets up to 4 GB in size), and stateless host auto-configuration.

Table 10-315 compares the IPv4 and IPv6 address formats.

Table 10-315: IPv6 and IPv4 Address Formats

Feature	IPv6	IPv4
Address space	128-bits = 3.4 x 1038 (340 unidecillion)	32-bits = 4.3 x 109 (4.2 billion)
Field separator	colon (:)	period (.)
Notation	hexadecimal	decimal
Example	db8:0:0:1	0.23.2.3

Each IP address contains a network part, an optional subnetwork part, and a host part. The network and subnetwork parts together are used for routing, while the host part is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork parts from the IP address. Classless Interdomain Routing (CIDR) provides a way to represent IP addresses and subnet masks.

IP addresses are difficult to remember, so people tend to refer to computers by their domain names instead.

IPv6 Provider Edge (6PE). A protocol that enables IPv6 domains to communicate with each other over an Multi-Protocol Label Switching (MPLS) IPv4 core network. V6PE routers are “dual stack” and run both IPv4 and IPv6. Multiprotocol Border Gateway Protocol (BGP) (MP-BGP) in the IPv4 network is used to exchange IPv6 reachability information along with a label for each IPv6 prefix announced. Defined in RFC 4798.

Also called V6PE.

K

keepalive message. A message sent between devices when no data traffic has been detected for a given period of time. This communication verifies that the virtual and physical connection between the devices is still active.

kernel. The part of an operating system that performs basic functions such as allocating hardware resources.

KVM (Kernel-based Virtual Machine). A virtualization infrastructure for the Linux kernel that turns it into a hypervisor. KVM requires a processor with hardware virtualization technology extensions. By itself, KVM does not perform any emulation. Instead, KVM exposes an interface with which a user space host can then set up guest virtual machine (VM) instances.On Linux, QEMU (Quick EMUlator) is one such user space host.

L

Label Distribution Protocol (LDP). A protocol for distributing labels in non-traffic-engineered applications. LDP allows routers to create label-switched path (LSP) instances through a network by mapping network layer routing information directly to data-link layer switched paths.

A label is a short fixed-length, locally-significant identifier that identifies a forwarding equivalence class (FEC).

LDP works with other routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) to create LSPs.

See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

© 2021 IP Infusion Inc. Proprietary

label edge router (LER). A router that operates at the edge of an Multi-Protocol Label Switching (MPLS) network and acts as the entry and exit points for the network.

When forwarding IP packets into an MPLS domain, an LER makes the initial path selection, add the appropriate labels to the packet, and forwards the labelled packets into the MPLS domain. Likewise, upon receiving a labelled packet which is destined to exit the MPLS domain, the LER strips off the label and forwards the resulting IP packet using normal IP forwarding rules. (Under penultimate hop popping (PHP), the popping function might be performed by an label switch router (LSR) directly connected to the LER.)

Also called an edge LSR.

label switch router (LSR). A Multi-Protocol Label Switching (MPLS) router located in the middle of a MPLS network. When an LSR receives a packet, it uses the label included in the packet header to determine the next hop on the label-switched path (LSP) and find a corresponding label for the packet from a lookup table. The old label is then removed from the header and replaced with the new label before the packet is forwarded.

Also called transit router.

label-switched path (LSP). A sequence of routers that cooperatively perform Multi-Protocol Label Switching (MPLS) operations for a packet stream. An LSP is a unidirectional, point-to-point, half-duplex connection carrying information downstream from the ingress (first) router to the egress (last) router. The ingress and egress routers cannot be the same device.

latency. Delay in the transmission through a network from source to destination. See also line rate, wire speed.

Layer 1 (L1). The physical layer in the Open Systems Interconnection (OSI) Reference Model that conveys the bit stream through electrical impulse, light waves, or radio signals through the network. L1 represents the basic network hardware and specifies the type of medium used for transmission and the network topology.

Layer 2 (L2). The data link layer in the Open Systems Interconnection (OSI) Reference Model that provides reliable transit of data across a physical link between two directly connected devices. L2 refers to physical addressing, network topology, line discipline, error notification, sequenced delivery of frames, and flow control.

L2 transfers data between network entities by splitting data into frames to send on Layer 1 (L1) and receiving acknowledgment frames. The data link layer performs error checking and retransmits frames not received correctly. In general, the data link layer controls the flow of information across the link, providing an error-free virtual channel to Layer 3 (L3).

The data-link layer has two sublayers:

- logical link control (LLC)
- Media Access Control (MAC)

Also called link layer.

Layer 3 (L3). The network layer in the Open Systems Interconnection (OSI) Reference Model that routes packets of data from source to destination across a network. L3 provides network-wide communication, including global addressing, lifetime control, fragmentation, and reassembly. Internet Protocol (IP) is an example.

Layer 4 (L4). The transport layer in the Open Systems Interconnection (OSI) Reference Model that provides logical communication between processes running on different hosts. L4 manages the end-to-end delivery of payload from a source to a destination within and between networks while maintaining the quality of service. Transmission Control Protocol (TCP) is an example.

Lightweight Directory Access Protocol (LDAP). A protocol used to locate organizations, individuals, and other resources in a network. Defined in RFC 4511. See also authentication, authorization, and accounting (AAA), Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+).

line rate. Total number of physically transferred bits per second, including useful data and protocol overhead, over a communication link. For example, if the line rate of a link is 10 Gbps, the link transmits 10 gigabits of data every second over its physical interface. Contrast with throughput. See also latency, wire speed.

link. Communication path between two neighbor nodes.

link aggregation. A method for using multiple parallel links between a pair of devices as if they were a single higher-performance channel. The aggregated interface is viewed as a single link to each device. Spanning Tree Protocol (STP) also views it as one interface. Link aggregation can also be used to increase availability so that when there is a failure in one physical link, the remaining links stay up, and there is no disruption. Defined by IEEE 802.1AX.

Also called link aggregation group (LAG), LAG bundle, and EtherChannel. See also Link Aggregation Control Protocol (LACP), Multi-Chassis Link Aggregation (MC-LAG).

Link Aggregation Control Protocol (LACP). Mechanism for exchanging port and system information to create and maintain link aggregation groups.

link cost. An arbitrary number configured on an Open Shortest Path First (OSPF) interface which is used in shortest path first calculations.

Link Layer Discovery Protocol (LLDP). A mechanism for the devices on a network to advertise their identity, capabilities, and neighbors to each other. Defined by IEEE 802.1AB.

link state. Information about a link and link cost to neighboring routers.

link-state advertisement (LSA). An Open Shortest Path First (OSPF) protocol data unit (PDU) to share information on the operating state of a link, link cost, and other OSPF neighbor information. LSAs are used by the receiving routers to update their Routing Information Base (RIB)s.

link-state database (LSDB). The data structure on a router that contains all routing knowledge in a link-state network. An LSDB stores all link-state advertisement (LSA) instances produced by a link-state routing protocol such as Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS). Each router runs shortest path first (SPF) algorithm against this database to locate the best network path to each destination in the network.

link-state routing. A routing technique used by Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) where each router shares information with other routers by flooding information about itself to every reachable router in the area. Link-state protocols use characteristics of the route such as speed and cost to determine the best path. Link-state information is transmitted only when something has changed in the network.

Every router constructs a map of the connectivity of the network, determining the interconnections between all routers. As a router receives an advertisement, it stores this information in a link-state database (LSDB). Each router then independently calculates the best next hop from it to every possible destination in the network using the shortest path first (SPF) algorithm to build a shortest path tree (SPT) with itself as the center of that tree. The shortest path to each reachable destination within the network is found by traversing the tree. The collection of best next hops forms the router's Routing Information Base (RIB).

Link-state algorithms create a consistent view of the network and are therefore not prone to routing loops, but they achieve this at the cost of more computing cycles and more traffic compared to distance-vector routing.

See also Dijkstra algorithm.

Linktrace Message (LTM). A Connectivity Fault Management (CFM) protocol data unit (PDU) initiated by a Maintenance association End Point (MEP) to trace a path to a target MAC address, forwarded from Maintenance domain Intermediate Point (MIP) to MIP, up to the point at which the LTM reaches its target MEP.

© 2021 IP Infusion Inc. Proprietary

Linux. A Unix-like computer operating system assembled under the model of free and open source software development and distribution. The defining component of Linux is the kernel, the central part of the operating system that manages system services. Many people use the name “Linux” to refer to the complete operating system package which is called a Linux distribution which is made up of a collection of software based around the Linux kernel.

Linux has since been ported to more computer hardware platforms than any other operating system and is available for a wide variety of systems from small embedded systems up to supercomputers. In particular, networking devices such as switches and routers almost universally run some Linux distribution.

As an open operating system, Linux is developed collaboratively, meaning no one organization is solely responsible for its development or ongoing support. Companies participating in the Linux community share research and development costs with their partners and competitors.

Local Area Network (LAN). A group of computers and devices connected by a communications channel, capable of sharing resources among several users. LANs are based on a small physical area such as a building, floor, or department. LANs can connect to a wide area network (WAN). Ethernet is the most popular LAN technology.

logical link control (LLC). The higher sublayer of Layer 2 (L2) in the Open Systems Interconnection (OSI) Reference Model. The LLC sublayer provides the interface for Layer 3 (L3) and handles error control, flow control, framing, and MAC-sublayer addressing. The most prevalent LLC protocol is IEEE 802.2, which includes both connectionless and connection-oriented variants. See also Media Access Control (MAC).

loopback. A troubleshooting test in which a signal is transmitted from a source to a destination and then back to the source again so that the signal can be measured and evaluated.

M

MAC address. A permanent, unique serial number that uniquely identifies a network device among all other network devices in the world. MAC addresses are 12-digit numbers, 48 bits in length. MAC addresses are usually written as six groups of two hexadecimal digits, separated by hyphens (“-”) or colons (“:”):

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

Each pair of hexadecimal digits represents one byte of the 6-byte (48-bit) address.

An example of a MAC address is 68:A3:C4:3B:8D:24:

- The first three parts (68:A3:C4) identify the manufacturer (Liteon Technologies)
- The second three parts (3B:8D:24) is the serial number assigned by the manufacturer

At Layer 2 (L2), other devices use MAC addresses to locate specific ports in a network, and to create and update a Routing Information Base (RIB). A MAC address maps to an IP address through the Address Resolution Protocol (ARP).

Also called physical address, Ethernet address, or hardware address.

MAC-in-MAC. See Provider Backbone Bridging (PBB).

Maintenance Association (MA). In Connectivity Fault Management (CFM), a set of Maintenance association End Point (MEP) instances, each configured with the same MAID (Maintenance Association Identifier) and Maintenance Domain (MD) Level, established to verify the integrity of a single service instance.

Maintenance association End Point (MEP). A Connectivity Fault Management (CFM) entity at the edge of a Maintenance Domain (MD) that confines CFM messages within the domain via the MD level. MEPs periodically

transmit and receive Continuity Check Message (CCM) instances from other MEPs within the domain. MEPs are either “Up” (toward the switch) or “Down” (toward the wire).

Maintenance Domain (MD). In Connectivity Fault Management (CFM), the network or the part of the network for which faults in connectivity can be managed.

Maintenance domain Intermediate Point (MIP). A Connectivity Fault Management (CFM) entity that catalogs and forwards information received from Maintenance association End Point (MEP) instances. MIPs are passive points that respond only to CFM Linktrace Message (LTM) and loopback messages.

Management Information Base (MIB). A specification of objects used by Simple Network Management Protocol (SNMP) to monitor or change network settings. MIBs provides a logical naming scheme for resources on a network. A MIB contains information about a device such as settings, usage statistics, performance data, or physical properties (such as temperature or fan speed). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches. Standard MIBs are defined by the IETF.

Maximum Transmission Unit (MTU). The maximum number of bytes in a packet or frame. For Ethernet, the default MTU is 1500 bytes (data payload), but each media has different sizes. The Ethernet MTU is defined in RFC 894.

Media Access Control (MAC). The lower sublayer of Layer 2 (L2) in the Open Systems Interconnection (OSI) Reference Model. The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several network nodes to communicate within a multiple-access network that uses a shared medium such as Ethernet. The MAC sublayer is the interface between the logical link control (LLC) sublayer and Layer 1 (L1).

mesh. A physical or logical network topology in which devices have many redundant interconnections. A full mesh is when all devices in a network have a connection to all other devices, a partial mesh is when some devices have a connection to all other devices.

Metro Ethernet Forum (MEF). A defining body for Carrier Ethernet with many participating organizations including service providers, and network hardware and software manufacturers. The MEF’s mission is to accelerate the worldwide adoption of carrier-class Ethernet networks and services. For more, see http://metroethernetforum.org/.

Multi-Chassis Link Aggregation (MC-LAG). A technique that extends the link aggregation concept. At either one or both ends of a link aggregation group, a single aggregation system is replaced by a *portal* that is a collection of one to three portal systems. Defined by IEEE 802.1AX.

Also called MLAG and Distributed Resilient Network Interconnect (DRNI).

Multi-Protocol Label Switching (MPLS). A method for forwarding packets through a network. MPLS operates between the traditional definitions of Layer 2 (L2) and Layer 3 (L3).

In a traditional IP network, each router performs an IP lookup to determine a next hop based on its routing table, and forwards the packet to that next hop. Every router in the path repeats this process, making its own independent routing decisions, until the final destination is reached.

In an MPLS network, the first device does a routing lookup, but instead of finding a next hop, it finds the final destination router and finds a pre-determined path from the source to the destination. The router applies a “label” based on this information. Other routers in the path use the label to route the traffic without needing to perform any additional IP lookups.

At each incoming (ingress) point of the network, packets are assigned a label by a label edge router (LER). Packets are forwarded along an label-switched path (LSP) where each label switch router (LSR) makes forwarding decisions based on the label information. At each hop, an LSR swaps the existing label for a new label that tells the next hop how to forward the packet. At the outgoing (egress) point, an LER removes the label, and forwards the packet to its destination via IP routing.

© 2021 IP Infusion Inc. Proprietary

MPLS enables these applications: Virtual Private Network (VPN), traffic engineering (TE), and Quality of Service (QoS).

See also Label Distribution Protocol (LDP), Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Multi-Protocol Label Switching - Transport Profile (MPLS-TP). A subset of Multi-Protocol Label Switching (MPLS) with extensions that address transport network requirements. The extensions provide the same QoS, protection and restoration, and Operation, Administration, and Maintenance (OAM) as in SONET/SDH. In MPLS-TP, some of the MPLS functions are turned off, such as penultimate hop popping (PHP), label-switched path (LSP) merge, and equal-cost multipath (ECMP).

The use of a control plane protocol is optional in MPLS-TP. The control plane can set up an LSP automatically across a packet-switched network domain. However, some network operators might prefer to configure the LSPs statically without using an IP or routing protocol.

multicast. The process of a single host sending messages to a selected group of receivers. See also broadcast, unicast.

multicast group. A collection of hosts receiving packets from a host that is transmitting multicast packets. Only hosts that need to hear a particular multicast declare that requirement. A multicast group restricts traffic to just those paths between the sources and destinations associated with the multicast address. Membership is dynamic; when a host joins a group, it starts receiving the datastream, and when a host leaves a group, it stops receiving the datastream. When there are no more members, the group simply ceases to exist.

See also GARP Multicast Registration Protocol (GMRP), Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), Multiple MAC Registration Protocol (MMRP), (S,G).

Multicast Listener Discovery (MLD). An IPv6 protocol that allows hosts to add or remove themselves from a multicast group. Defined by RFC 3810.

See also Internet Group Management Protocol (IGMP), multicast group, (S,G).

Multiple MAC Registration Protocol (MMRP). A protocol that manages multicast group MAC addresses. In addition, MMRP improves the convergence time of GARP Multicast Registration Protocol (GMRP). Defined by 802.1ak.

Multiple Registration Protocol (MRP). A generic registration framework with protocols, procedures, and managed objects for switches to register attributes with other switches in a LAN. Defined by 802.1ak. MRP replaces Generic Attribute Registration Protocol (GARP)

Multiple Spanning Tree Protocol (MSTP). An enhancement to the Rapid Spanning Tree Protocol (RSTP) where a separate spanning tree for can be configured for a VLAN group. Each VLAN group belongs to a multiple spanning-tree instance (MSTI). Several MSTIs can run in an multiple spanning-tree (MST) region, with each region interconnected in a common and internal spanning tree (CIST).

MSTP is backward compatible with both RSTP and Spanning Tree Protocol (STP).

Originally defined in IEEE 802.1s and later merged into 802.1Q.

multiple spanning-tree (MST) region. A collection of interconnected switches that have the same Multiple Spanning Tree Protocol (MSTP) configuration which includes region name, revision number, and VLAN-to-instance map. Each MST region can contain multiple instances of spanning trees. The network administrator must properly configure participating switches throughout the region. All regions are bound together using a common and internal spanning tree (CIST), which creates a loop-free topology across regions. An MST region appears as a single switch to spanning tree configurations outside the region.

multiple spanning-tree instance (MSTI). A group of VLANs in a spanning-tree instance managed by Multiple Spanning Tree Protocol (MSTP) within an multiple spanning-tree (MST) region. Within each MST region, MSTP maintains multiple spanning-tree instances. Each instance has a spanning-tree topology independent of other spanning-tree instances. An MSTI provides a fully connected active topology for frames belonging to a VLAN. You can assign a VLAN to only one spanning-tree instance at a time.

An internal spanning tree (IST) is a special type of MTSI.

Multiple VLAN Registration Protocol (MVRP). A protocol that manages registration of VLANs, tracking which routers are members of which VLANs and which router interfaces are in which VLAN. MVRP removes routers and interfaces from the VLAN information when they become unavailable. MVRP improves the convergence time of GARP VLAN Registration Protocol (GVRP). Defined by 802.1ak.

N

name resolution. The process of translating an IP address to a name that is easily remembered by a person. In a TCP/IP environment, a name such as www.example.com is translated into its IP equivalent by the Domain Name Service (DNS).

neighbor. An adjacent system reachable by traversing a single subnetwork; an immediately adjacent device. Also called peer. See also adjacency.

Neighbor Discovery Protocol (NDP). An IPv6 protocol that nodes on the same link use to discover each other's presence, determine each other's Link Layer addresses, find routers, and maintain reachability information about the paths to active neighbors. NDP is defined in RFC 2461 and is equivalent to the Address Resolution Protocol (ARP) used with IPv4.

NETCONF (Network Configuration Protocol). A mechanism to install, manipulate, and delete the configuration of network devices. The operations, notifications, and the database contents supported by a particular NETCONF server are extensible, and defined with a modeling language called YANG. The database is used to store YANG data structures which represent the configuration of the device containing the NETCONF server. This configuration can be saved in non-volatile storage so the configuration can be restored upon reboot. Defined in RFC 6241.

network. A group of computers and related devices connected by a communications channel capable of sharing resources among several users. A network consists of transmission media, devices such as routers or switches, and protocols that make message sequences meaningful.

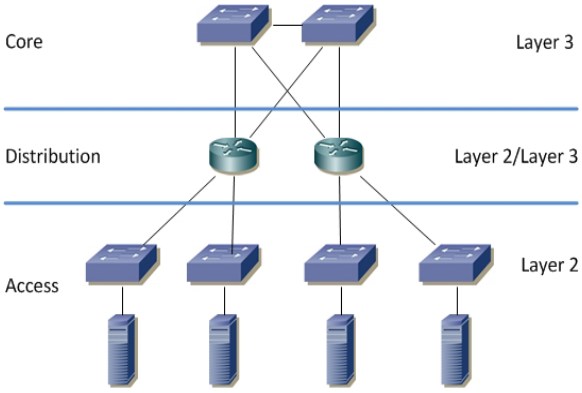
A network can range from a peer-to-peer network connecting a small number of users in an office or department, to a Local Area Network (LAN) connecting many users, to a wide area network (WAN) connecting users on several networks spread over a wide geographic area.

network address translation (NAT). A method to use one set of IP addresses for an internal inetwork and a second set of addresses for the public Internet. This allows an organization to shield internal addresses from the public Internet. NAT is configured on the router at the border of an internal network and the Internet. NAT translates the internal local addresses to globally unique IP addresses before sending packets to the Internet and vice versa. Defined by RFC 1631.

network administrator. The person responsible for the day-to-day operation and management of a network.

network design model. A hierarchical model originally defined by Cisco that divides a network into three functional areas, or layers. This model optimizes network hardware and software to perform specific roles.

© 2021 IP Infusion Inc. Proprietary



The roles that each layer performs are:

- The access layer provides local user access to the network
- The distribution layer connects network services to the access layer, and implements policies regarding security, traffic loading, and routing
- The core layer provides high-speed transport for the distribution layer

See also collapsed core.

Network Element (NE). Any device in a network such as a host, router, switch, or firewall that performs a service or function for the network.

Network Functions Virtualization (NFV). The ability to decouple network services from dedicated hardware devices to be hosted on a virtual machine (VM). Once the network services are under the control of a hypervisor, the services can be performed on standard x86 servers.

network layer. See Layer 3 (L3).

network segment. A portion of a computer network that is separated from the rest of the network by a device such as a router or switch. Each segment can contain one or more hosts.

Network Services Module (NSM). The base module in OcNOS that communicates with every OcNOS routing and switching process. The protocol components use APIs exposed by the NSM client, which act as conduits to transfer data between the protocol modules and NSM.

Network Time Protocol (NTP). A protocol used to synchronize the system clocks of hosts on a network to Universal Coordinated Time (UTC). A device can update its clock automatically by configuring itself as an NTP client. Using NTP enables the device to record accurate times of events. Defined by RFC 5905.

Neutron. The networking component of OpenStack that provides “networking as a service” between virtual NICs managed by other OpenStack services.

Neutron provides a “plug-in” mechanism that lets network operators enable different technologies. It also lets tenants create multiple private networks and control their IP addressing. Organizations have control over security and compliance policies, Quality of Service (QoS), monitoring and troubleshooting, as well as the ability to deploy network services, such as a firewall, intrusion detection, and Virtual Private Network (VPN) instances.

next hop. The next device to which a protocol data unit (PDU) is sent on its way to its destination.

Next Hop Label Forwarding Entry (NHLFE). An Multi-Protocol Label Switching (MPLS) entry containing next hop information (interface and next hop address) and label manipulation instructions; it can also include label encoding, L2 encapsulation information, and other information to process packets in the associated stream.

node. An addressable device such as a host, router, or switch, attached to a network, that transmits and receives data.

north/south. The flow of traffic traversing between users and a data center (spanning-tree). Contrast with east/west.

northbound. An interface that allows a network component to communicate with a higher-level component. A northbound interface hides complex details of operations. Northbound flow can be thought of as going upward. In architectural diagrams, northbound interfaces are drawn at the top of the component. See also southbound.

Not-So-Stubby-Area (NSSA). An extension of a Open Shortest Path First (OSPF) stub area. OSPF uses an NSSA as a transit to send external routes to other areas or to domains that are not part of the OSPF autonomous system. OSPF does not flood external routes from other areas into an NSSA, but does translate and flood route information from the NSSA into other areas such as the backbone. Defined by RFC 1587.

O

Open Network Foundation (ONF). A non-profit organization responsible for the development and standardization of a software architecture that supports Software-Defined Networking (SDN). ONF is also responsible for the commercialization and promotion of SDN as a concept and its underlying technologies. For more, see: https://www.opennetworking.org/.

Open Shortest Path First (OSPF). An Interior Gateway Protocol (IGP) based on link-state routing. OSPF is widely deployed in large networks because of its efficient use of network bandwidth and its rapid convergence after changes in topology. Defined in RFCs 2328 and RFC 5340.

OSPF advertises the states of local network links within an autonomous system (AS) and makes routing decisions based on the shortest path first (SPF) algorithm. Each OSPF router maintains an identical database describing the autonomous system's topology. From this database, a Routing Information Base (RIB) is calculated by constructing a shortest path tree (SPT).

OSPF features include least-cost routing, multipath routing, and load balancing. OSPF includes explicit support for Classless Interdomain Routing (CIDR) and the tagging of externally derived routing information.

OSPF version 2 supports IPv4 and OSPF version 3 supports IPv6.

OSPF divides an autonomous system into contiguous groups of networks called areas.

- In a standard area, intra-area routes, inter-area routes, and external routes (learned from other routing protocols such as RIP and BGP) are distributed. Inter-area routes and external routes are distributed as summary addresses.
- A backbone area is essentially a standard area which has been designated as the central point to which all other areas connect. A backbone area combines a set of independent areas into an AS and acts as a hub for inter-area transit traffic and routing information distribution. Each non-backbone area is directly connected to the backbone area.
- OSPF uses stub area instances and Not-So-Stubby-Area (NSSA) instances to limit distribution of inter-area routes and external routes.

See also area border router (ABR), autonomous system border router (ASBR).

© 2021 IP Infusion Inc. Proprietary

Open Systems Interconnection (OSI) Reference Model. A conceptual model defined by the International Organization for Standardization (ISO) that organizes the computer-to-computer communications process into seven layers. Each layer provides services to the layer above and receives services from the layer below. Such a set of layers is called a protocol stack.

Layers seven through five manage end-to-end communications between the message source and destination, while layers one through four manage network access:

- Layer 4 (L4) ensures the end-to-end delivery from a source to a destination
- Layer 3 (L3) routes packets of data from source to destination across a network
- Layer 2 (L2) reliably transports data across the physical link between two directly connected nodes
- Layer 1 (L1) conveys the bit stream at the electrical and mechanical level

The OSI Reference Model is often compared to the more descriptive (versus prescriptive) Transmission Control Protocol/Internet Protocol (TCP/IP) model.

Open vSwitch (OVS). A software switch used in virtualized server environments that forwards traffic between different virtual machine (VM) instances on the same physical host and between VMs and the physical network. OVS enables network automation through programmatic extension, while still supporting standard management interfaces and protocols. For more, see http://openvswitch.org/.

OpenFlow. An open standard for forwarding plane operations that enables researchers to run experimental protocols. OpenFlow is developed, specified, and sponsored by the Open Network Foundation (ONF). OpenFlow provides a protocol that enables a controller to dynamically program internal flow-tables in devices. Network vendors have added OpenFlow features to routers and switches.

OpenStack. A cloud operating system that controls pools of compute, storage, and networking resources in a data center which users manage through a Web-based dashboard, command-line tools, or a RESTful API. See also Neutron.

Operation, Administration, and Maintenance (OAM). A set of Ethernet specifications that provide connectivity monitoring, fault detection and notification, fault verification, fault isolation, loopback, and remote defect identification. The primary specifications are 802.3ah link-fault management (LFM) and 802.1ag Connectivity Fault Management (CFM).

P

packet. A protocol data unit (PDU) at Layer 3 (L3) of the Open Systems Interconnection (OSI) Reference Model. A packet contains source and destination addresses, user data, and control information such as the length of the packet, the header checksum, and flags indicating whether the packet has been fragmented. The user data in a packet is often referred to as the payload. The actual format of a packet depends on the protocol that creates the packet.

A packet sent through a connectionless protocol such as User Datagram Protocol (UDP) is sometimes called a datagram.

See also frame, packet switching.

packet switching. A data-transmission method that transmits information over one of several routes. Information is sent to the destination through the best route, determined by a routing algorithm.

A packet switched network breaks information to be transmitted into discrete packets. Related packets might not all follow the same path to their destination. Packet sequence numbers are used to reassemble the original message at the destination.

A packet-switched network is connectionless because each packet contains its destination address and does not require a dedicated path to reach that destination. Multiple users may transmit packets over the same connection at the same time, independent of one another.

The Internet is an example of a packet-switched network.

Contrast with circuit switching.

paravirtualized. A software component that is aware that it is running in a virtual machine (VM). For example, a paravirtualized virtual device driver runs in a VM that communicates with the underlying host OS. Typically, a paravirtualized driver is optimized to share queues, buffers, or other data items with the underlying host OS to improve throughput and reduce latency.

path computation element (PCE). An entity (component, application, or server) that can compute a network path or route based on a network graph and constraints (see RFC 4655).

path-vector routing. A routing technique that advertises a network as a destination address and a complete path to reach that destination. Each entry in the Routing Information Base (RIB) contains the destination network, the next router, and the path to reach the destination.

A path vector protocol guarantees loop-free paths by recording each hop the routing advertisement traverses through the network. A node can easily detect a loop by looking for its own node identifier in the path.

This technique is sometimes used in Bellman-Ford algorithm to avoid count-to-infinity problems.

Border Gateway Protocol (BGP) is an example of a prefix-based path-vector protocol where the Routing Information Base (RIB) maintains the autonomous systems to traverse to reach a destination.

peer. Immediately adjacent device with which a protocol relationship has been established. Also called neighbor.

penultimate hop popping (PHP). A technique where the outermost label of an Multi-Protocol Label Switching (MPLS) packet is removed by a label switch router (LSR) before the packet is passed to an adjacent label edge router (LER).

physical layer. See Layer 1 (L1).

ping (packet internet groper). A command used to test network connectivity by transmitting an Internet Control Message Protocol (ICMP) diagnostic packet to a specific node on the network, forcing the node to acknowledge that the packet reached the correct destination. If the node responds, the link is operating; if not, something is wrong.

The word ping is often used as a verb, as in “ping that workstation to see if it is alive.”

policing. Applying rate limits on bandwidth and burst size for traffic for a particular interface.

policy-based routing (PBR). Classifying packets to determine their forwarding path within a device. PBR is used to redirect traffic for analysis. Also called filter-based forwarding (FBF).

port. The point at which a communications circuit terminates on a network. A port can be logical, physical or both. Examples include:

- The physical interface between a device and a communications circuit, usually identified by a number or name.
- The logical interface between a TCP/IP applications and a communications facility which use well-known port numbers such as FTP: 20, HTTP: 80, and NFS: 2049.
- The logical interface between a process and a communications facility that allows more than one logical port to be associated with one physical port. For example, Ethernet uses multiple MAC addresses to distinguish between separate logical channels connecting two ports on the same physical transport network interface.

© 2021 IP Infusion Inc. Proprietary

Also called interface.

port authentication. A mechanism for port-based user authentication and network access control for LAN devices. Defined by IEEE 802.1X.

Precision Time Protocol (PTP). A protocol that synchronizes clocks throughout a computer network. On a LAN, PTP achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. The time synchronization is achieved through packets that are transmitted and received in a session between a master clock and a slave clock. Defined by IEEE 1588v2.

Priority-based Flow Control (PFC). A flow control mechanism that can be set independently for each frame priority on full-duplex links. Defined by IEEE 802.1Qbb.

private VLAN (PVLAN). A switch with ports that cannot communicate with each other, but can access other networks. A PVLAN has at least one private port and a trunk port. All traffic received on a private port is forwarded out the trunk port. All traffic received on a trunk port is handled as normal switch traffic. No traffic communication occurs between the private ports.

protocol. A set of rules that end points in a network connection must follow when they communicate. A protocol includes data representation, data item ordering, message formats, message and response sequencing rules, block data transmission conventions, and timing requirements.

The Open Systems Interconnection (OSI) Reference Model and Transmission Control Protocol/Internet Protocol (TCP/IP) are both used as a model for many protocols. There are one or more protocols at each layer in the models that both ends of the connection must recognize and observe.

protocol data unit (PDU). A unit of data transmitted as a composite by a protocol.

In the Open Systems Interconnection (OSI) Reference Model, the actual name used for a PDU depends on the layer:

- Layer 4 (L4): segment
- Layer 3 (L3): packet
- Layer 2 (L2): frame
- Layer 1 (L1): stream, symbol stream, or bit stream

See also bridge protocol data unit (BPDU). Sometimes called datagram.

Protocol Independent Multicast (PIM). A method to determine the best paths for distributing a multicast transmission. PIM uses unicast routing tables (such as those used by Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP)) and static routes to perform multicasting. Each host must be registered using IGMP to receive the transmission.

PIM has these variations:

- PIM dense mode (PIM-DM: RFC 3973) uses a push model. PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors prune back the unwanted traffic. This process repeats periodically.
- PIM sparse mode (PIM-SM: RFC 4601) uses a pull model. PIM-SM uses a shortest path tree (SPT) where sources forward multicast packets to a designated router which unicasts the packets to an assigned rendezvous point router, which then forwards the packets to members of multicast groups.
- PIM source-specific multicast (PIM-SSM: RFC 3569) uses PIM-SM functionality to create a SPT between the client and the source without using a rendezvous point.
- Bidirectional PIM (Bidir-PIM: RFC 5015) uses PIM-SM functionality to route traffic only along a bidirectional SPT that is rooted at the rendezvous point for a group.

protocol stack. The layers of software used in network communications.

Provider Backbone Bridge-Traffic Engineering (PBB-TE) . An extension to Provider Backbone Bridging (PBB) that removes features such as flooding, dynamically created forwarding tables, and spanning tree protocols. PBB-TE also covers Connectivity Fault Management (CFM) and Ethernet Linear Protection Switching (ELPS).

In PBB-TE, a network administrator configures the forwarding tables in the backbone switches with static routes to ensure that frames take predetermined paths within the network. Frames with destination MAC addresses not in a forwarding table are dropped. Broadcast frames are not supported and are also dropped by backbone switches.

Defined in IEEE 802.1Qay.

Provider Backbone Bridging (PBB). A technique to create Ethernet backbones for service access networks. Defined in IEEE 802.1ah, PBB extends Provider Bridging (PB) defined in 802.1ad in these ways:

- The 802.1ah header adds an I-SID (Service Instance Identifier) which is a label that maps to a customer VLAN identifier. An I-SID virtualizes VLANs across a network. VLANs are mapped into I-SIDs by configuring only the edge of the network at a backbone edge bridge (BEB). This makes the maximum number of service instances 16 million.
- The 802.1ah header encapsulates backbone source and destination MAC addresses (B-MAC) along with the customer source and destination MAC addresses (C-MAC). The B-MAC contains MAC addresses of the service provider's PBB edge switches. The 802.1ah format is sometimes called “MAC-in-MAC” because of this MAC address encapsulation. The encapsulation of customer MAC addresses in backbone MAC addresses means that the backbone does not need to learn customer MAC addresses. Customer MAC addresses are learned at BEB ports only.

Provider Bridging (PB). A technique that enables a service provider to use the architecture and protocols of 802.Q to offer the equivalent of separate LANs, bridged LANs, or VLANs to multiple customers. Provider bridging requires no active cooperation between customers and requires minimal cooperation between an individual customer and the service provider.

When VLANs were originally defined in 802.1Q, the number of unique VLAN identifiers was limited to 4096. In large provider networks, each subscriber needs a separate address, so this limit could prevent a provider from having more than 4096 subscribers.

To overcome this limit, 802.1ad inserts an additional VLAN tag into a single 802.1Q Ethernet frame. Frames passing through the provider network are doubly tagged with:

- customer VLAN (C-VLAN) tag which identifies the customer network VLAN
- service VLAN (S-VLAN) tag which identifies the service provider network VLAN

With two VLAN identifiers in combination for each provider-customer pair, it is possible to define up to 16,777,216 VLANs.

The frame format for 802.1ad is also called Q-in-Q, double tagged, stacked VLANs, or VLAN stacking.

provider edge (PE). A device at the edge of an enterprise or service provider core network. A PE offers an initial, first level of network traffic aggregation for many customer edge (CE) devices.

pseudowire (PW). An emulation of a point-to-point connection over a packet-switching network. A pseudowire is a way to transport legacy services such as TDM over a packet-switched network:

- Structure-aware TDM circuit emulation service over packet-switched network (CESoPSN)
- Structure-agnostic TDM over packet (SAToP)

A pseudowire that both originates and terminates on the edge of a single packet-switched network (autonomous system or carrier network) is called a single-segment pseudowire (SS-PW). A pseudowire that extends through multiple autonomous systems or carrier networks is called a multi-segment pseudowire (MS-PW).

© 2021 IP Infusion Inc. Proprietary

Q

Q-in-Q. See Provider Bridging (PB).

QEMU (Quick EMUlator). A hosted hypervisor that performs hardware virtualization. QEMU emulates CPUs through dynamic binary translation and provides a set of device models enabling it to run a variety of unmodified guest operating systems. QEMU also can be used together with KVM (Kernel-based Virtual Machine) to run virtual machines at near-native speed (requiring hardware virtualization extensions on x86 machines). QEMU can also be used purely for CPU emulation for user-level processes, allowing applications compiled for one architecture to be run on another.

Quality of Service (QoS). The ability to *guarantee* the delivery, control the bandwidth, set priorities for specific network traffic, and provide an appropriate level of security. QoS provides a level of predictability and control beyond the best effort delivery that a device provides by default.

See also Class of Service (CoS).

Quantized Congestion Notification (QCN). An end-to-end congestion management scheme for protocols capable of transmission rate limiting. Defined by IEEE 802.1Qau.

R

radio access network (RAN). The air interface and base station technology in a cellular network. In addition to the RAN, the entire cellular system includes the core network, which provides the backbone and services, as well as the cellphones.

Rapid Per-VLAN Spanning Tree Plus (RPVST+). A version of Cisco Per VLAN Spanning Tree Plus (PVST+) that uses the Rapid Spanning Tree Protocol (RSTP) state machine. PVST+ runs a spanning tree instance for each VLAN in the network. PVST+ is not scalable when there are many VLANs in a network. A compromise between RSTP and R-PVST+ is Multiple Spanning Tree Protocol (MSTP) which runs multiple instances of spanning tree that are independent of VLANs. MSTP maps a set of VLANs to each spanning tree instance.

Rapid Spanning Tree Protocol (RSTP). An enhancement to the Spanning Tree Protocol (STP) that re-configures quickly after a topology change. RSTP can verify if a port can change to a forwarding state safely without waiting for timers to start convergence. RSTP is not aware of VLANs and blocks ports at the physical level. Defined by IEEE 802.1D. See also Multiple Spanning Tree Protocol (MSTP).

Remote Authentication Dial In User Service (RADIUS). An authentication and accounting protocol to authenticate users and authorize their access to the requested system or service.

Defined in RFCs 2058, 2059, and 2865. See also authentication, authorization, and accounting (AAA), Lightweight Directory Access Protocol (LDAP), Terminal Access Controller Access Control System Plus (TACACS+).

remote monitoring (RMON). A Management Information Base (MIB) specification that defines functions for remotely monitoring networked devices. The RMON specification provides many problem detection and reporting capabilities. Defined by RFC 2819.

Request for Comments (RFC). Proposals and standards that define protocols for communications over the Internet. RFCs are developed and published by the Internet Engineering Task Force (IETF).

Resource Reservation Protocol (RSVP). A signalling protocol for reserving resources across a network. RSVP is rarely used by itself, but Resource Reservation Protocol—Traffic Engineering (RSVP-TE) is widely used.

Resource Reservation Protocol—Traffic Engineering (RSVP-TE). RSVP with traffic engineering extensions, as defined by RFC 5101, that allows RSVP to establish label-switched path (LSP) instances in Multi-Protocol Label Switching (MPLS) networks, using Constrained Shortest Path First (CSPF), taking into consideration constraints such as available bandwidth and explicit hops. The LSPs might not agree with the route suggested by the Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS).

reverse path forwarding (RPF). An algorithm that checks the unicast Routing Information Base (RIB) to determine whether there is a shortest path back to the source address of an incoming multicast packet. Unicast RPF helps determine the source of denial-of-service attacks and rejects packets from unexpected source addresses.

Rivest-Shamir-Adleman (RSA). A public key, or asymmetric, encryption scheme. The oretical background to RSA is that it is difficult to find the factors of a very large number that is the product of two prime numbers. RSA is considered very secure provided a sufficiently long key is used.

route. The path from source to destination through a network.

route flap damping. Method for minimizing instability caused by route flapping. The router stores a penalty value for each route. Each time the route flaps, the router increases this value. If the penalty for a route reaches a configured suppress value, the router does not include the route as a forwarding entry and does not advertise the route to peers.

route redistribution. One protocol learning routes from another protocol running on the same device. Also called redistribution or route leakage.

route reflection. A method of allowing iBGP routers to accept and propagate iBGP routes to their clients.

To avoid routing loops, Border Gateway Protocol (BGP) does not advertise routes learned from an internal BGP peer to other internal BGP peers. Instead, BGP requires that all internal peers be fully meshed so that any route advertised by one router is advertised to all peers within the autonomous system (AS). As a network grows, the full mesh requirement becomes difficult to manage. To handle scaling problems, BGP uses route reflection and BGP confederations.

Route reflection allows you to designate one or more routers as route reflectors. BGP relaxes the re-advertising restriction on route reflectors, allowing them to accept and propagate iBGP routes to their clients.

route summarization. Consolidating multiple routes into a single route advertisement, in contrast to flat routing where a Routing Information Base (RIB) contains a unique entry for each route.

Classless Interdomain Routing (CIDR) is used to implement route summarization. All IP addresses in the route advertisement must have identical high-order bits.

Also called route aggregation. See also subnet mask.

router. A Layer 3 (L3) device that makes decisions about the paths over which network traffic will flow. Routers use dynamic routing protocols to learn about the network and to find the best route to forward packets toward their final destination:

1. Find a matching destination address in the Routing Information Base (RIB)
2. Find the MAC address for the packet from the Address Resolution Protocol (ARP) cache
3. Write the new MAC address in the IP packet
4. Send the packet on the port associated with the MAC address

© 2021 IP Infusion Inc. Proprietary

routing. The process of finding a path to a destination to use to transmit a protocol data unit (PDU) over a network. Routing is usually controlled by a Routing Information Base (RIB) which defines where a PDU should go. Each router only needs to know where a PDU should be sent on its next hop, and does not know nor care what happens afterward; the next hop plus one is the responsibility of the next router, and so on through the network until a PDU reaches its destination.

Routing Information Base (RIB). A data structure in a device that lists the routes to destinations and metrics (distances) associated with those routes. A RIB contains information about the topology of the network immediately around it. Maintaining a RIB by discovering network topology is the primary purpose of dynamic routing protocols such as Border Gateway Protocol (BGP), Routing Information Protocol (RIP), and Open Shortest Path First (OSPF). Network administrators can also add fixed routes to the RIB for static routing.

Also called a routing table. Contrast with Forwarding Information Base (FIB).

Routing Information Protocol (RIP). An Interior Gateway Protocol (IGP) that implements a distributed variant of the Bellman-Ford algorithm to provide distance-vector routing capabilities. RIP uses the hop count of a destination to detect the best path to route packets, but limits the maximum number of hops to 15 to prevent routing loops. RIP implements split horizon techniques. Defined in RFC 1058.

RIP is easy to configure and has low processing requirements. However, the hop count limit restricts the size of the network that RIP can support. Also, RIP can be slow to converge.

RIPv2 defined in RFC 2453 also supports subnet information, allowing Classless Interdomain Routing (CIDR).

RIPng (next generation), an extension of RIPv2 defined in RFC 2080, supports IPv6.

routing protocol. A set of processes, algorithms, and messages that are used to exchange routing information and populate the local Routing Information Base (RIB) with the best path between a source and destination.

The term “routing protocol” usually implies dynamic routing, where a device reports changes and shares information with other devices in the network. Each router starts with knowledge of only the devices to which it is directly attached. The routing protocol shares this information first with its immediate neighbors, and then throughout the network. This way, routers learn the topology of the network.

A primary benefit of dynamic routing protocols over static routing is that routers exchange information when there is a topology change. This exchange allows routers to automatically learn about new devices and networks and also to find alternate paths when there is a link failure in the current network.

Table 10-316 summarizes the characteristics of the dynamic routing protocols supported by OcNOS:

Table 10-316: Dynamic routing protocols

	Border Gateway Protocol (BGP)	Routing Information Protocol (RIP)	Open Shortest Path First (OSPF)	Intermediate System to Intermediate System (IS-IS)
Algorithm	path-vector routing	distance-vector routing	link-state routing	link-state routing
Type	Exterior Gateway Protocol (EGP)	Interior Gateway Protocol (IGP)	Interior Gateway Protocol (IGP)	Interior Gateway Protocol (IGP)
Classless Interdomain Routing (CIDR)	Yes	RIP v1: No RIP v2: Yes	Yes	Yes
Scalable	Yes	No	Yes	Yes
Speed of convergence	Moderate	Slow	Fast	Fast

Table 10-316: Dynamic routing protocols

	Border Gateway Protocol (BGP)	Routing Information Protocol (RIP)	Open Shortest Path First (OSPF)	Intermediate System to Intermediate System (IS-IS)
Resource Use	High	Low	High	High
Configuration ease	Complex	Simple	Complex	Complex

routing table. See Routing Information Base (RIB).

S

S-TAG. See service VLAN (S-VLAN).

(S,G). A notation used in multicast that enumerates a shortest path tree (SPT) where:

- S is the IP address of the source
- G is the multicast group address that identifies the receivers

If the IP address of the source is 192.1.1.1, and the IP address of the multicast group is 224.1.1.1, the source group is written as (192.1.1.1, 224.1.1.1).

Secure Shell (SSH). A protocol that allows the opening of a secure, encrypted channel between two computers with secure authentication. SSH is most often used to provide a secure shell to log in to a remote machine, but also supports file transfers, TCP, and other functions.

segment routing. A form of source routing where nodes and links are represented as segments. The path that a particular protocol data unit (PDU) needs to traverse is represented by one or more segments.

server. A system entity that provides a service to other entities called clients.

service VLAN (S-VLAN). In a Provider Bridging (PB) frame, a tag that identifies the service provider network VLAN. See also customer VLAN (C-VLAN). Also called an S-TAG or S-VID tag.

Shortest Path Bridging (SPB). A control plane protocol that combines an Ethernet data path with an Intermediate System to Intermediate System (IS-IS) link state protocol running between switches. SPB does not depend on spanning tree protocols to provide a loop-free topology, but instead uses IS-IS link-state packets to discover and advertise the network topology and compute the shortest path tree (SPT) instances from all bridges in the SPB area. SPB only requires provisioning at the edge of the network. Defined by IEEE 802.1aq, with RFC 6329 describing the IS-IS extensions to support SPB.

There are two types of SPB depending on the type of Ethernet data path:

- Shortest Path Bridging - VID (SPBV) uses a Provider Bridging (PB) (802.1ad) data path
- Shortest Path Bridging - MAC (SPBM) uses a Provider Backbone Bridging (PBB) (802.1ah) data path

shortest path first (SPF). Algorithm used by Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) to make routing decisions based on the state of network links. Also called the Dijkstra algorithm.

© 2021 IP Infusion Inc. Proprietary

shortest path tree (SPT). A Routing Information Base (RIB) formed by using the shortest path first (SPF) algorithm.

shortest-path routing. A routing algorithm in which paths to all network destinations are calculated. The shortest path is then determined by a cost assigned to each link.

signalling. The ability to transfer information within a network or between different networks.

Simple Network Management Protocol (SNMP). A standardized framework for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- SNMP manager: The system used to control and monitor the activities of network devices.
- SNMP agent: The component within a managed device that maintains the data for the device and reports the data SNMP managers.
- Management Information Base (MIB): How SNMP exposes data as variables which describe the system configuration. These variables can be queried (and sometimes set) by SNMP managers.

SNMP uses User Datagram Protocol (UDP) to send and receive messages on the network.

Single Root I/O Virtualization (SR-IOV). A specification that allows a single Peripheral Component Interconnect Express (PCIe) physical device under a single root port to appear to be multiple separate physical devices to the hypervisor or the guest operating system.

SR-IOV uses physical functions (PFs) and virtual functions (VFs) to manage global functions for the SR-IOV devices:

- PFs are used to configure and manage the SR-IOV functionality
- VFs are lightweight and contain all the resources necessary for data movement but have a minimal set of configuration resources

SR-IOV enables network traffic to bypass the software switch layer of a virtualization stack. The I/O overhead in the software emulation layer is nearly the same as in nonvirtualized environments.

Software-Defined Networking (SDN). An approach to designing, building, and operating networks that decouples the control plane from the data plane. The control plane is centralized in the form of a controller system. Communication between the controller system and the network device uses a standard protocol such as OpenFlow or other agents. The controller system can consist of multiple, domain specific, clustered controllers. An SDN architecture usually includes APIs that developers use to control the underlying network. These APIs can be standards-based, or they can be vendor-specific.

source routing. A technique where the sender of a protocol data unit (PDU) can partially or completely specify the route that the PDU should take through the network. See also segment routing.

southbound. An interface that allows a network component to communicate with a lower-level component. A southbound interface breaks down the concepts into smaller technical details that are specifically geared toward the lower-layer component within the architecture. Southbound flow can be thought of as going downward. In architectural diagrams, southbound interfaces are drawn at the bottom of the component. See also northbound.

spanning tree algorithm. A technique that finds the best path between segments of a multilooped, mesh network. If multiple paths exist in the network, the spanning tree algorithm finds the most efficient path and limits the link between the two networks to this single active path. If this path fails because of a cable failure or other problem, the algorithm reconfigures the network to use another path.

From the point of view of an individual switch, a spanning tree has a root node and one path that connects all the other switches.

Spanning Tree Protocol (STP). A protocol that creates spanning trees within mesh networks of connected devices, disabling any links that are not a part of the tree and leaving a single active connection between any two unique network nodes. Defined by 802.1D.

STP devices exchange bridge protocol data unit (BPDU) messages. The spanning tree algorithm calculates the best path and prevents multiple paths between network segments. STP elects a root bridge, finds paths and determines the least cost path to the root bridge, then disables all other paths.

Network managers can set up redundant links as backups in case active links fails. Automatic backup takes place without the pitfalls of bridge loops or the need to manually enable or disable backup links.

See also Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).

split horizon. A technique where routes learned from an interface are not advertised on that same interface, preventing the router from seeing its own route updates.

In split horizon with poison reverse, routes learned from an interface are set as unreachable and advertised on that same interface which also prevents the router from seeing its own route updates.

stacked VLAN. See Provider Bridging (PB).

static address. An address permanently assigned to a device. Contrast with a dynamic address.

static routing. A method where a network administrator programs connecting paths between networks into a router. If a connection fails, the administrator must reprogram the router to use a new path. Static routes have precedence over routes chosen by dynamic routing protocols.

stub area. A type of Open Shortest Path First (OSPF) area where external routes are distributed as a single default route (address 0.0.0.0). Inter-area routes are distributed in a stub area as summary addresses.

In a *totally stubby area*, a single default route is distributed for all external *and* inter-area routes. Addresses from both other areas and external networks are distributed as the default route (address 0.0.0.0).

See also Not-So-Stubby-Area (NSSA).

subnet mask. A bit pattern that shows how an Internet address is divided into network, subnetwork, and host parts. The mask has ones in the bit positions to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion, and the subnet field should be contiguous with the network portion.

This is an example is this IPv4 address and subnet mask:

192.168.100.12 with subnet mask of 255.255.255.0

The first 24 bits of the address is the network address (192.168.100.0) and the last 8 bits are the hosts (12). The entire subnet spans the address range 192.168.100.0 to 192.168.100.255.

The addresses on a given subnet are always contiguous and can all be derived from the network address. Bit masks are always with respect to binary digits, so the number of IP addresses on a given subnet is always some power of two.

A mask gives the first address in the block (the network address) when ANDed with an address in the block.

Classless Interdomain Routing (CIDR) represents the equivalent of a subnet mask by adding a prefix length to an IP address that is the number of bits in the network portion. For example, the subnet mask above can be written as:

192.168.100.12/24

where 192.168.100.12 is the IP address and /24 is the number of bits in the subnet mask.

A subnet mask represents the same information as a prefix length, but predates the use of CIDR.

Also called address mask, network mask.

© 2021 IP Infusion Inc. Proprietary

subnetwork. A group of related IP addresses that all begin with the same network portion and end with a unique portion identifying the host within the subnet.

Also called subnet. See also subnet mask.

subsequent address family identifier (SAFI). Number that further identifies an address family.

supernetting. The process of taking several discrete network addresses and advertising them as one route. For example, if an organization is using 192.10.1.0/24 to 192.10.254.0/24, instead of advertising 254 separate networks, the organization can advertise only the single route 192.10.0.0/16.

switch. A Layer 2 (L2) device that forwards frames based on a destination MAC address. A switch finds a destination address in its filtering database and transmits the frame on the port associated with the destination address. The filtering database is populated through a self-learning process, where each incoming frame is used to update the entries in the filtering database.

A switch that is VLAN-aware can also forward frames based on VLAN identifiers. A network administrator can configure this mapping manually or a switch can dynamically learn mappings via GARP VLAN Registration Protocol (GVRP).

Basic switch behavior is defined in IEEE 802.1D and 802.1Q.

See also bridge. Contrast with router.

Synchronous Ethernet (SyncE). SONET/SDH/PDH-based synchronization that is used to synchronize and send frequency information to devices on an Ethernet network. Synchronous Ethernet provides only frequency synchronization, not time or phase synchronization.

T

telnet. A client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of purposes.

Terminal Access Controller Access Control System Plus (TACACS+). An authentication method that provides access control for networked devices using one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting (AAA) services. (Usually pronounced like tack-axe.)

See also Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS).

throughput. Average rate of successful delivery of data packets over a communication link. Throughput is measured in bits per second, data packets per second, or sometimes data packets per time slot. See also line rate, latency, wire speed.

time to live (TTL). A limit on how long a piece of information can exist before it should be discarded. TTL is a field in an IP header that is (usually) decremented by 1 for each hop through which the packet passes. If the field reaches zero, the packet is discarded, and a corresponding error message is sent to the source of the packet.

Top-of-Rack (ToR) switch. In a data center, an access layer switch that connects to servers installed in the same rack. A ToR switch is usually low profile (one or two rack units in height) with a low port count (typically 48 ports). All cabling for servers stays within the rack as relatively short cables from the servers to the switch. The switch connects

the rack to the data center network with one fiber uplink to a distribution layer switch. There is no need to run cabling between racks and each rack can be managed as a modular unit.

A ToR switch extends the Layer 2 (L2) topology from the aggregation switch to each individual rack resulting in a larger Layer 2 footprint.

See also end-of-row switch.

topology. The physical or logical layout of a network.

topology change notification (TCN). In Spanning Tree Protocol (STP), a bridge protocol data unit (BPDU) that a switch sends to signal a topology change.

traffic engineering (TE). The ability to control the path taken through a network based on a set of traffic parameters. Traffic engineering optimizes the performance of networks and their resources by balancing traffic load across links, routers, and switches in the network. See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Transmission Control Protocol (TCP). A Layer 4 (L4) protocol that works above Internet Protocol (IP) and provides reliable data delivery over connection-oriented links.

TCP splits the stream of data into packets with a sequence number, and sends the packets over an IP-based network. At the destination, TCP acknowledges packets that have been received (so that missing packets can be resent) and reassembles received packets in the correct order to provide an in-order data stream to the remote application. If TCP detects a missing, corrupted, or out of order packet, it requests it be resent from the source.

See also Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP).

Transmission Control Protocol/Internet Protocol (TCP/IP). A family of Internet protocols that describe how data should be formatted, addressed, transmitted, routed, and received to enable computers to communicate over a network.

The Open Systems Interconnection (OSI) Reference Model is a more prescriptive (versus descriptive) approach to network design. TCP/IP does not map cleanly to the OSI model because it was developed before the OSI model and was designed to solve a specific set of problems, not to be a general description for all network communications.

TCP/IP is a widely published open standard and is supported by many vendors and is available on many different computers running many different operating systems. TCP/IP is separated from the network hardware and will run over Ethernet and other connections.

TCP/ IP also refers to the specific functionality at layers 4 and 3:

- Transmission Control Protocol (TCP) at Layer 4 (L4) splits a message into packets that are transmitted over the Internet and reassembles the packets into the original message at the destination
- Internet Protocol (IP) at Layer 3 (L3) addresses and routes each packet so that it gets to its destination

transport layer. See Layer 4 (L4).

tunneling. A method of transporting data in one protocol by encapsulating it in another protocol. Tunneling is used for reasons of incompatibility, implementation simplification, or security. For example, a tunnel lets a remote VPN client have encrypted access to a private network.

type of service (ToS). A field in the IPv4 header used to differentiate packet flows. See also Differentiated Services (DiffServ).

type-length-value (TLV). A data structure used to encode optional information in a data communications protocol:

- Type: the kind of field that this part of the message represents

© 2021 IP Infusion Inc. Proprietary

- Length: the size of the value field, usually in bytes
- Value: a variable-sized set of bytes that contains the data of the message

U

unicast. The process of a single host sending messages to one destination.See also broadcast, multicast.

User Datagram Protocol (UDP). A connectionless transport layer protocol that exchanges datagrams without acknowledgments or guaranteed delivery and which requires other protocols to handle error processing and retransmission. Defined in RFC 768.

Multicast applications that deliver audio and video streams use UDP as their delivery mechanism because the acknowledgment and retransmission services offered by Transmission Control Protocol (TCP) are not needed and add too much overhead.

User-to-Network Interface (UNI). The physical interface/demarcation between a service provider and a subscriber, the service start or end point. There are two types of UNI:

- UNI-C: customer-side processes
- UNI-N: network-side processes

V

VirNOS. An IP Infusion product based on Network Functions Virtualization (NFV) that helps network operators deploy and manage networking services. Many core networking services, including switching, routing, load balancing and VPN can be performed by software either running directly on x86-64 servers or running as virtual machine (VM) instances instead of requiring expensive networking equipment. Therefore, organizations are migrating networking functions to standard, high-volume server environments and replacing dedicated network hardware with virtualization software that runs on commodity servers. Carriers, service providers, enterprises and network equipment manufacturers can run VirNOS as-is, on top of a standard server platform. IP Infusion customers can integrate VirNOS into their software offering and thereby add services and features quickly.

Virtual Ethernet Bridge (VEB). A virtual switch implemented in a virtualized server environment. A VEB mimics a traditional external Layer 2 (L2) switch for connecting to a virtual machine (VM). VEBs can communicate between VMs on a single physical server, or they can connect VMs to the external network. The most common implementations of VEBs are software-based vSwitches built into hypervisors.

Virtual Local Area Network (VLAN). A logical group of network devices that appear to be on the same LAN, regardless of their physical location. VLANs enable multiple bridged LANs to transparently share the same physical network link while maintaining isolation between networks. Traffic between VLANs is restricted to devices that forward unicast, multicast, or broadcast traffic only on the LAN segments that serve the VLAN to which the traffic belongs.

VLANs make it easy to administer logical groups of hosts that can communicate as if they were on the same LAN.

Membership in a particular VLAN can be by port, MAC address, protocol, or subnet.

VLANs are configured as unique Layer 2 (L2) broadcast domains. VLANs allow network administrators to resegment their networks without physically rearranging the devices or network connections. VLANs span one or more ports on multiple devices and several VLANs can co-exist on a single physical switch. By default, each VLAN maintains its own filtering database containing MAC addresses learned from frames received on ports belonging to the VLAN.

IEEE 802.1Q provides for tagging Ethernet frames with VLAN identifiers. 802.1Q only supports up to 4094 VLANs, which is a scaling constraint for service providers.

virtual machine (VM). An operating system or application environment installed on emulated hardware and not physically installed on dedicated hardware. The virtual machine's guest operating system does not have to be modified to run in a virtualized environment. A VM behaves like a traditional, physical server and runs a traditional operating system such as Windows or Linux.

A hypervisor emulates the computer's CPU, memory, hard disk, network and other hardware resources completely, enabling virtual machines to share the resources. The hypervisor can emulate multiple virtual hardware platforms that are isolated from each other. For example, virtual machines can run Linux and Windows operating systems and share the same underlying physical host. An operating sysem is unaware that it is running in a VM.

See also paravirtualized, virtualization.

virtual port. A port on a vSwitch (Virtual Switch) where virtual Ethernet adapters or physical uplinks can be attached. During their creation, virtual switches are typically configured with a specific number of virtual ports.

virtual private LAN service (VPLS). Multipoint-to-multipoint Layer 2 (L2) VPN service used to interconnect multiple Ethernet LANs across an Multi-Protocol Label Switching (MPLS) backbone.

VPLS evolved as a logical extension of Virtual Private Wire Service (VPWS) based on RFC 4447.

VPLS can be defined as several instances of a virtual switch instance (VSI) that are interconnected to form a single logical bridge domain.

Virtual Private Network (VPN). A network service which uses encryption and tunneling to provide a subscriber with a secure private network that runs over the public network infrastructure.

Virtual Private Wire Service (VPWS). Point-to-point Layer 2 (L2) VPN service used to interconnect multiple Ethernet LANs across an Multi-Protocol Label Switching (MPLS) backbone. Also called Virtual Leased Line (VLL) or Ethernet over MPLS (EoMPLS).

virtual router (VR). A OcNOS proprietary abstraction where multiple distinct logical routers exist within a single device. Each virtual router executes separate instances of the routing protocol and network management software. A virtual router provides support for multiple Routing Information Base (RIB) instances and multiple Forwarding Information Base (FIB) instances per physical router. Each VR might consist of an Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), or Routing Information Protocol (RIP) routing process, each with its own Routing Information Base (RIB) and Forwarding Information Base (FIB). Applications include segregating traffic dedicated to different customers, enterprise Virtual Private Network (VPN) users, or a specific traffic type such as streaming video.

Do not confuse a Virtual Router Redundancy Protocol (VRRP) virtual router with a OcNOS virtual router. They are two different things.

Virtual Router Redundancy Protocol (VRRP). A protocol that uses a *virtual router*, an abstract representation of multiple routers (master and backup routers) that act as a group. VRRP advertises a virtual router as the default gateway instead of one physical router. Two or more physical routers are configured, with only one doing the actual routing at any given time. If the current physical router that is routing on behalf of the virtual router fails, the other physical router automatically takes over. Defined by RFC 5798.

Do not confuse a VRRP virtual router with an OcNOS virtual router (VR). They are two different things.

Virtual Routing and Forwarding (VRF). A technology that allows multiple instances of a Routing Information Base (RIB) to co-exist within the same router at the same time. Multiple VRFs inside a virtual router (VR) logically subdivide the RIBs. Service providers can use VRF technology to create a separate Virtual Private Network (VPN) for each of their customers. Therefore, the technology is also called VPN routing and forwarding.

© 2021 IP Infusion Inc. Proprietary

virtual switch instance (VSI). A mechanism for VLANs to pass packets to other VLANs without sending the packets through a router. With a VSI, the switch recognizes packet destinations that are local to the sending VLAN and bridges (switches) those packets. Only packets destined for another VLAN are routed.

A VSI is similar to the bridging defined in IEEE 802.1Q; a frame is switched, based on the destination MAC and membership in a Layer 2 (L2) VPN. A VSI floods unknown, broadcast, or multicast frames to all ports associated with the VSI.

virtualization. A technology that abstracts the physical characteristics of a machine, creating a logical version of it, including creating logical versions of entities such as operating systems and network resources. See also hypervisor, virtual machine (VM).

vNIC (Virtual Network Interface Card). Software that behaves like a Ethernet hardware adapter. It has a MAC address, and it sends and receives Ethernet frames.

VPN routing and forwarding. See Virtual Routing and Forwarding (VRF).

vSwitch (Virtual Switch). Software that behaves like a physical Ethernet switch. A vSwitch connects virtual machine (VM) instances in a virtual network at layer 2:

- Connects vNIC (Virtual Network Interface Card) instances from multiple VMs to virtual ports
- Connects physical network interface cards to virtual ports
- Uplinks to the physical network

A vSwitch maintains a MAC address table and routes traffic to specific ports, rather than repeating traffic on all ports. A vSwitch can include other features found in physical Ethernet switches, such as VLANs.

See also Open vSwitch (OVS).

W

weighted fair queuing (WFQ). Queue scheduling discipline where each queue has a weight and is assigned a different percentage of output port bandwidth. WFQ supports variable-length packets so that flows with larger packets are not allocated more bandwidth than flows with smaller packets.

WFQ classifies traffic as high- or low-bandwidth with low-bandwidth traffic getting priority and high-bandwidth traffic sharing what is left over. If traffic bursts ahead of the rate at which the interface can transmit, new high-bandwidth traffic is discarded after a congestive-messages threshold has been reached.

WFQ provides preferential treatment for higher priority traffic while preventing total starvation of lower priority traffic under sustained overload conditions.

weighted random early detection (WRED). Congestion avoidance mechanism which prevents an output queue from ever filling to capacity. WRED provides separate thresholds and weights for different IP precedences, allowing you to provide different qualities of service in regard to packet dropping for different traffic types. Standard traffic may be dropped more frequently than premium traffic during periods of congestion.

weighted round-robin queuing (WRR). Queue scheduling discipline that supports flows with significantly different bandwidth requirements. Each queue can be assigned a weight that is relative to other queues. WRR ensures that lower-priority queues are not denied access to buffer space and output port bandwidth. At least one packet is removed from each queue during each service round.

white box switch. In computer hardware, a white box is a server without a well-known brand name made from commonly available parts. White box switches are like white box servers, offering low cost without the brand name or tight integration of silicon and network software features.

Traditional black box switches are built with vertically integrated hardware and software. Some vendors use custom application-specific integrated circuit (ASIC) components to boost performance and add features, which adds to the cost. A white box switch decouples the software from the switching hardware. By decoupling software and hardware, customers have more flexibility and can potentially change software without changing hardware.

A white box switch runs a network operating system on generic x86 hardware with “merchant silicon” chipsets from manufacturers such as Broadcom, Centec, Intel, Marvell, and Mellanox. White box switches rely on an operating system such as Linux to integrate the Layer 2 (L2)/Layer 3 (L3) networking functions.

White box switches do not have the same complex features as black box switches because most interact with Software-Defined Networking (SDN) controllers to make forwarding and control plane decisions from a centralized point for all switches in the network. The SDN controller uses OpenFlow (or another southbound API) to program the forwarding table of the white box switches.

Some vendors sell a complete white box solution with the operating system already installed, while others supply just the “bare-metal” switch and you buy the operating system direct from the software vendor.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a Local Area Network (LAN) and that may use or provide public communication facilities.

wire speed. The ability of a device to achieve throughput equal to the maximum throughput of a communication standard.

Y

YANG. A data modeling language that specifies the syntax and semantics for NETCONF (Network Configuration Protocol) operations, notification events, and database content. YANG tools can automate behavior within the NETCONF protocol for clients and servers.

YANG can model both configuration and state data of network elements. YANG structures the data definitions into tree structures and provides many modeling features, including an extensible type system, formal separation of state and configuration data and a variety of syntactic and semantic constraints. YANG data definitions provide a strong set of features for extensibility and reuse. Defined in RFC 6020.

Z

ZebHA. An IP Infusion product that ensures a pre-agreed level of operational performance by minimizing system downtime. A ZebHA system operates redundant nodes that can provide continued service when a node fails. High availability does not mean that components will never fail, but it ensures that the system is available when the user needs it even if components fail. ZebHA provides:

- Simplex-Active or Active-Standby (1+1) control plane redundancy
- Reliable handling of operational, application, system and component failures;
- Strict Service Level Agreements (SLA) requirements of network operator customers

ZebHA supports protocol modules in Layer 2 (L2) and Layer 3 (L3).

There are two types of protocol recovery after a redundancy switchover: stateful switchover (SSO) and graceful restart.

© 2021 IP Infusion Inc. Proprietary

ZebIC. An IP Infusion product that enables network equipment manufacturers to develop networking solutions based on leading silicon platforms. ZebIC allows manufacturers to deliver networking products built around this switching platform.

ZebIC enables developers to develop, integrate, and test a target platform while the actual hardware system is still under development. Pre-integrated with ZebOS-XP control plane platform, ZebIC:

- Separates hardware development from software development through the ZebOS abstraction layer.
- Isolates all of the hardware and operating system specific interactions into a small set of well-defined function calls for the control plane.

ZebM. An IP Infusion product that allows network equipment manufacturers to develop management functionality for their networking products. ZebM provides a software framework and APIs for building on-device management systems for network equipment. The ZebM framework contains these core components:

- CML (Central Management Layer), transaction-oriented middleware that connects configuration and operational data on all management interfaces within a network device. CML is used by any northbound management application to manage ZebOS-XP or any third-party control plane.
- SMI (Simple Management Interface), a series of southbound Interface modules to connect with OcNOS or any third party control plane protocol modules. SMI is the interface between the managed object and the CML.
- Model-driven northbound interface for automatic rendering of interfaces such as command-line interface (CLI) and NETCONF (Network Configuration Protocol).

ZebOS-XP. An IP Infusion product with Layer 2 (L2) and Layer 3 (L3) control plane software that allows network equipment manufacturers to rapidly add networking capabilities to communications products. ZebOS-XP is targeted at manufacturers who provide solutions in carrier transport, access, Carrier Ethernet, mobile backhaul, data center, and cloud networking, including solutions for enterprise private clouds, hybrid clouds, and public clouds

The ZebOS-XP networking protocol modules conform to leading Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), Metro Ethernet Forum (MEF), and other industry standards.

© 2021 IP Infusion Inc. Proprietary

SECTION 17 Master Command Index

Master Command Index

1489
nvo vxlan access-if 3967
A.B.C.D 4326
aaa accounting default 411
aaa authentication login 410
aaa authentication login console 412
aaa authentication login console fallback error 414
aaa authentication login default 413
aaa authentication login default fallback error 415
aaa group server 416
aaa local authentication attempts max-fail 417
aaa local authentication unlock-timeout 418
abort transaction 538
abr-type 2363
accept-lifetime 2712
accept-lifetime 3480
accept-mode 3384
access-list logging cache-size 329
access-list logging rate-limit 330
ack-wait-timeout 4436
add policy 926
address-family 2461
address-family ipv6 2714
address-family labeled-unicast 2610
adjacency-check 2715
admin-group 626
advertise-label-for-default-route 4230
advertise-labels 4229
advertisement-interval 3385
advertisement-mode 4231
affinity 4460
aggregate-address 2463
allocate-label 2611
application-priority advertise-local-config 3300
application-priority enable (interface) 3301
application-priority enable (switch) 3302
area authentication 2230
area default-cost 2231
area default-cost 2364
area filter-list 2236
area interface 2232
area interface authentication 2233
area interface network-type 2234
area interface passive 2235
area nssa 2237
area nssa 2365
area range 2239
area range 2367
area shortcut 2240
area stub 2241
area stub 2368
area virtual-link 2242
area virtual-link 2369
area virtual-link 3520
area-password 2716
arp access-group 331
arp access-list 332
arp access-list filter 333
arp access-list remark 335
arp access-list resequence 336
arp access-list response 337
ARP ACL Configuration 1182
arp-ageing-timeout 2832
arp-cache disable 3943
arp-nd flood-suppress 3944
arp-nd refresh timer 3945
arp-reachable-time 2833
authentication key-chain 2717
authentication mode 2718
authentication send-only 2719
authentication text 3386
auth-mac auth-fail-action 1492
auth-mac disable 1493
auth-mac dynamic-vlan-creation 1494
auth-mac enable 1495
auth-mac mac-aging 1496
auth-mac system-auth-ctrl 1497
auto-cost reference bandwidth 2245
auto-cost reference bandwidth 2371
automatic-router-id-selection enable 2150
auto-summary 2464
backup 1068
bandwidth 3703
bandwidth 4121
bandwidth 4461
bandwidth 627
bandwidth-measurement uni-available-bandwidth static 628
bandwidth-measurement uni-residual-bandwidth static 629
bandwidth-measurement uni-utilized-bandwidth static 630
bandwidth-percentage 3303
banner motd 429
bfd 3483
bfd all-interfaces 2372
bfd all-interfaces 3521
bfd all-interfaces 2246
bfd all-interfaces 2720
bfd auth type 3482
bfd echo 3484
bfd echo interval 3485
bfd echo ipv4 source 3486
bfd interval 3488

© 2021 IP Infusion Inc. Proprietary

bfd multihop-peer 3489
bfd multihop-peer A.B.C.D interval 3491
bfd multihop-peer X:X::X:X interval 3492
bfd notification 3493
bfd session 3494
bfd slow-timer 3495
bfd-firmware 3487
bgp aggregate-nexthop-check 2465
bgp always-compare-med 2466
bgp as-local-count 2467
bgp bestpath as-path ignore 2468
bgp bestpath as-path multipath-relax 2469
bgp bestpath compare-confed-aspath 2470
bgp bestpath compare-routerid 2471
bgp bestpath dont-compare-originator-id 2472
bgp bestpath med 2473
bgp bestpath tie-break-on-age 2475
bgp client-to-client reflection 2476
bgp cluster-id 2477
bgp confederation identifier 2478
bgp confederation peers 2479
bgp config-type 2480
bgp dampening 2481
bgp default local-preference 2483
bgp deterministic-med 2484
bgp enforce-first-as 2485
bgp extended-asn-cap 2486
bgp fast-external-failover 2487
bgp graceful-restart 2488
bgp g-shut 2490
bgp g-shut-capable 2491
bgp g-shut-local-preference 2492
bgp inbound-route-filter 2616
bgp log-neighbor-changes 2493
bgp nexthop-trigger delay 2495
bgp nexthop-trigger enable 2496
bgp rfc1771-path-select 2497
bgp rfc1771-strict 2498
bgp router-id 2499
bgp scan-time 2500
bgp unnumbered-mode 2607
bgp update-delay 2503
bridge acquire 1280
bridge address 1281
bridge ageing 1282
bridge cisco-interoperability 1311
bridge forward-time 1283
bridge hello-time 1284
bridge instance 1312
bridge instance priority 1313
bridge instance vlan 1314
bridge mac-priority-override 1285
bridge max-age 1286
bridge max-hops 1287
bridge multiple-spanning-tree 1316
bridge priority 1288
bridge protocol ieee 1317
bridge protocol mstp 1318
bridge protocol provider-mstp 3198
bridge protocol provider-rstp 3199
bridge protocol rpvst+ 1383
bridge protocol rstp 1319
bridge provider-rstp 1320
bridge rapid-pervlan-spanning-tree 1384
bridge rapid-spanning-tree 1321
bridge region 1322
bridge revision 1323
bridge shutdown 1289
bridge spanning-tree 1324
bridge spanning-tree errdisable-timeout 1325
bridge spanning-tree force-version 1326
bridge spanning-tree pathcost 1327
bridge spanning-tree portfast 1328
bridge te-msti 1329
bridge te-msti vlan 1330
bridge transmit-holdcount 1290
bridge vlan 1380
bridge vlan priority 1381
bridge-group 1291
bridge-group instance 1331
bridge-group instance path-cost 1332
bridge-group instance priority 1333
bridge-group path-cost 1292
bridge-group path-cost 1334
bridge-group priority 1293
bridge-group priority 1335
bridge-group spanning-tree 1336
bridge-group vlan 1382
capability cspf 2247
capability cspf 2721
capability lls 2248
capability opaque 2249
capability restart 2250
capability restart 2373
capability restart graceful 2794
capability traffic-engineering 2251
capability vrf-lite 2252
capability vrf-lite 2450
cc interval 3154
cc multicast 3155
channel-group mode 1394
circuit-failover 3387
class type qos 3706
class type queuing 3707
class-map type qos 3704
class-map type queuing 3705
class-type 4462
clear aaa local user lockout username 998

 © 2021 IP Infusion Inc. Proprietary

clear access-list log-cache 340
clear access-list 339
clear allowed-ethertype 1294
clear arp 2834
clear arp access-list 341
clear bgp (A.B.C.D|X:X::X:X) 2504
clear bgp * 2505
clear bgp * l2vpn vpls 2617
clear bgp <1-4294967295> 2507
clear bgp <1-4294967295> l2vpn vpls 2619
clear bgp A.B.C.D l2vpn vpls 2621
clear bgp dampening 2509
clear bgp external 2510
clear bgp flap-statistics 2512
clear bgp peer-group 2513
clear bgp statistics 2515
clear clns is-neighbors 2723
clear clns neighbors 2722
clear ddm transceiver alarm 568
clear ddm transceiver alarm all 569
clear ethernet cfm maintenance-point remote 3156
clear ethernet cfm traceroute-cache 3157
clear hardware-discard-counters 631
clear interface counters 632
clear interface cpu counters 633
clear interface fec 634
clear ip access-list 342
clear ip bgp * ipv4 labeled-unicast 2614
clear ip bgp * vpnv4 2618
clear ip bgp <1-4294967295> vpnv4 2620
clear ip bgp A.B.C.D 2516
clear ip bgp A.B.C.D ipv4 labeled-unicast 2612
clear ip bgp A.B.C.D vpnv4 2622
clear ip bgp A.B.C.D vrf 2518
clear ip bgp peer-group WORD ipv4 labeled-unicast 2613
clear ip bgp table-map 2519
clear ip dhcp relay option statistics 592
clear ip dhcp relay statistics 593
clear ip igmp 2938
clear ip isis route 2724
clear ip mroute 2922
clear ip mroute 2989
clear ip ospf 2253
clear ip pim sparse-mode 2991
clear ip prefix-list 635
clear ip route 2152
clear ip route kernel 2151
clear ip route vrf NAME 2153
clear ip sla statistics 742
clear ipv6 access-list 343
clear ipv6 neighbors 2835
clear ipv6 neighbors 636
clear ipv6 ospf process 2374
clear ipv6 prefix-list 637
clear isis adjacency 2725
clear isis counter 2726
clear isis interface counter 2727
clear isis process 2728
clear lacp 1396
clear ldp adjacency 4232
clear ldp session 4233
clear ldp statistics 4234
clear ldp statistics advertise-labels 4235
clear line 999
clear lldp counters 3226
clear logging logfile 885
clear mac access-list 344
clear mac address table dynamic vxlan 3946
clear mac address-table 1295
clear mcec statistics 1426
clear mpls counters ldp 4122
clear mpls counters rsvp 4123
clear mpls counters static 4124
clear mpls l2-circuit statistics 4125
clear ntp statistics 756
clear nvo vxlan counters 3947
clear nvo vxlan mac-stale-entries 3949
clear nvo vxlan tunnels 3948
clear nvo vxlan tunnels 4006
clear qos statistics 3708
clear radius-server 786
clear router-id 2154
clear rsvp p2mp-session 4463
clear rsvp session 4327
clear rsvp trunk 4328
clear sflow statistics 822
clear snmp hostconfig 837
clear spanning-tree detected protocols 1337
clear spanning-tree statistics 1338
clear ssh host-key 800
clear ssh hosts 801
clear tacacs-server counters 927
clear tfo counter 988
clear user 1000
clock set 431
clock timezone 430
cml logging 539
cml netconf translation 540
cmlsh transaction 541
cmlsh transaction limit 542
cnpv 3326
commit 543
compatible rfc1583 2254
configure terminal 432
configure terminal force 433
continue 2181
control-mode 4236
control-word 4128

© 2021 IP Infusion Inc. Proprietary

copy empty-config startup-config 518
copy file startup-config 536
copy ftp startup-config (interactive) 530
copy ftp startup-config 525
copy http startup-config (interactive) 535
copy http startup-config 529
copy running-config (interactive) 520
copy running-config 519
copy running-config startup-config 434
copy scp filepath 531
copy scp startup-config (interactive) 532
copy scp startup-config 526
copy sftp startup-config (interactive) 533
copy sftp startup-config 527
copy startup-config (interactive) 522
copy startup-config 521
copy system file (interactive) 524
copy system file 523
copy techsupport 860
copy tftp startup-config (interactive) 534
copy tftp startup-config 528
cos queue 4007
cp enable 3327
cpu-core-usage 492
cpu-queue 3709
cross-connect 1069
cross-connect 1552
cross-connect switchover type revertive 1070
crypto pki generate rsa common-name ipv4 435
cspf 4329
customer-spanning-tree customer-edge path-cost 1339
customer-spanning-tree customer-edge priority 1340
customer-spanning-tree forward-time 1341
customer-spanning-tree hello-time 1342
customer-spanning-tree max-age 1343
customer-spanning-tree priority 1344
customer-spanning-tree provider-edge path-cost 1345
customer-spanning-tree provider-edge priority 1346
customer-spanning-tree transmit-holdcount 1347
cvlan registration table 3200
cvlan svlan 3201
data-center-bridging 3304
data-traffic-vlan 3187
dcbx enable 3305
ddm monitor 570
ddm monitor all 571
ddm monitor interval 572
debounce-time 638
debug aaa 419
debug bfd 3496
debug bgp 2520
debug bgp bfd 3522
debug bgp mpls 2623
debug cml 545
debug cmm 494
debug ddm 573
debug dns client 614
debug dot1x 1498
debug ip arp 2836
debug ip dhcp snooping 552
debug ip igmp 2939
debug ip mrib 2923
debug ip ospf graceful-restart 2260
debug ip ospf lfa 2261
debug ip ospf redist 2262
debug ip ospf retransmission 2263
debug ip pim 2992
debug ip pim packet 2993
debug ip pim timer assert 2995
debug ip pim timer bsr 2996
debug ip pim timer hello 2997
debug ip pim timer joinprune 2999
debug ip pim timer register 3001
debug ipv6 nd 2837
debug ipv6 ospf 2375
debug ipv6 ospf bfd 2376
debug ipv6 ospf events 2377
debug ipv6 ospf ifsm 2378
debug ipv6 ospf lfa 2379
debug ipv6 ospf lsa 2380
debug ipv6 ospf nfsm 2381
debug ipv6 ospf nsm 2382
debug ipv6 ospf packet 2383
debug ipv6 ospf retransmission 2384
debug ipv6 ospf rib 2385
debug ipv6 ospf route 2386
debug isis 2729
debug isis bfd 3523
debug lacp 1397
debug ldp advertise-labels 4237
debug ldp all 4238
debug ldp dsm 4239
debug ldp events 4240
debug ldp fsm 4241
debug ldp hexdump 4242
debug ldp inter-area 4243
debug ldp nsm 4244
debug ldp packet 4245
debug ldp usm 4246
debug ldp vc usm 4247
debug lldp 3228
debug logging 887
debug mcec 1427
debug mstp 1348
debug nsm 436
debug ntp 757
debug ospf bfd 3524
debug ospf database-timer rate-limit 2257

 © 2021 IP Infusion Inc. Proprietary

debug ospf events 2258
debug ospf ifsm 2259
debug ospf lsa 2264
debug ospf nfsm 2265
debug ospf nsm 2266
debug ospf packet 2267
debug ospf rib 2268
debug ospf route 2269
debug ospf 2255
debug pim all 2994
debug radius 787
debug rib 2155
debug rsvp all 4330
debug rsvp cspf 4331
debug rsvp events 4332
debug rsvp fsm 4333
debug rsvp hexdump 4334
debug rsvp nsm 4335
debug rsvp packet 4336
debug sflow 823
debug snmp 838
debug snmp-server 839
debug ssh server 802
debug tacacs+ 928
debug telnet server 948
debug user-mgmt 1001
debug vm-events 4024
debug vrrp 3388
default 929
default-information originate 2270
default-information originate 2387
default-information originate 2731
default-metric 2272
default-metric 2389
defense-mode cnpv 3328
delay-measurement min-max-uni-link-delay 639
delay-measurement uni-delay-variation 640
delay-measurement uni-link-delay 641
deny 930
description 2157
description 3950
description 642
description 977
destination 4464
destination port 972
detour-identification 4426
dhcp-lease-max 4025
dhcp-lease-time 4026
dhcp-range 4027
disable 1071
disable 1553
disable 3389
disable 438
disable-ldp 4248
disable-rsvp 4337
disk-image 4028
distance (IPv4) 2732
distance (IPv6) 2733
distance 2273
distance 2390
distance bgp 2522
distribute-list 2274
distribute-list 2391
do 439
domain hello timeout 1429
domain priority 1430
domain-address 1428
domain-id 2452
domain-password 2734
domain-system-number 1431
dot1x initialize 1499
dot1x keytxenabled 1500
dot1x port-control 1501
dot1x protocol-version 1502
dot1x quiet-period 1503
dot1x reauthentication 1505
dot1x reauthMax 1504
dot1x system-auth-ctrl 1506
dot1x timeout re-authperiod 1507
dot1x timeout server-timeout 1508
dot1x timeout supp-timeout 1509
dot1x timeout tx-period 1510
dscp queue 4008
duplex 643
Dynamic LAG Minimum Bandwidth Configuration 1121
dynamic-hostname 2735
dynamic-learning disable 3951
egress cos map 3710
egress dscp map 3711
elsp-signal-map 4338
enable 3390
enable 440
enable db-summary-opt 2276
enable db-summary-opt 2393
enable password 441
enable-ldp 4249
enable-rsvp 4339
encapsulation 3952
end 442
end-time (absolute) 958
end-time after (relative) 959
enhanced-transmission-selection (interface) 3309
enhanced-transmission-selection (switch) 3308
enhanced-transmission-selection accept-peer-config 3306
enhanced-transmission-selection advertise-local-config 3307
ep1 <interface_name> ep2 <interface_name> 1072

errdisable cause 1268
errdisable link-flap-setting 1269
errdisable timeout 1270
ethernet cfm domain-type 3158
ethernet cfm mep 3159
ethertype 3310
evpn esi holdtime 3953
evpn multi-homed 3955
evpn vxlan multi-homing enable 3954
evpn-vlan-service 3956
exec-timeout 443
exit 444
exit-address-family 2523
exit-ether-ma-mep-mode 3160
exit-ether-ma-mode 3161
exit-p2mp-lsp 4465
explicit-null 4250
explicit-null 4340
export map 2624
ext-tunnel-id 4466
ext-tunnel-id A.B.C.D 4341
ext-tunnel-id X:X::X:X 4342
fast-reroute keep-all-paths 2277
fast-reroute keep-all-paths 2394
fast-reroute per-prefix 2736
fast-reroute terminate-hold-on interval 2737
fast-reroute tie-break 2278
fast-reroute tie-break 2395
fast-reroute tie-break 2738
feature dhcp 580
feature dynamic-rbac enable 931
feature guest-vm 4029
feature ntp 758
feature rsyslog 886
feature sflow 824
feature software-watchdog 861
feature ssh 803
feature tacacs+ 932
feature telnet 949
feature vlan classifier 1476
fec 644
fib retain 2158
filter 4467
filter 975
flowcontrol 645
fog 989
fog tfc 990
fog type 991
force-switch|manual-switch 3177
forwarding custom-profile 908
forwarding profile 910
frequency 743
frequency 960
frequency days (specific days) 961
from 4468
from A.B.C.D 4343
from X:X::X:X 4344
from X:X::X:X 4427
g8032 erp-instance 3178
g8032 physical-ring 3176
g8032 profile 3179
garp-gna enable 3957
gateway-ip 4030
global-merge-capability 4251
graceful-restart 4252
graceful-restart 4345
graceful-restart recovery-time 4346
graceful-restart restart-time 4347
group-id 4126
group-name 4127
hardware-profile filter (Qumran) 912
hardware-profile filter (XGS) 911
hardware-profile flowcontrol (Qumran) 913
hardware-profile micro-bfd 3497
hardware-profile portmode 647
hardware-profile statistics (Qumran) 914
hello-interval 4253
hello-interval 4348
hello-receipt 4349
hello-timeout 4350
help 445
High-Level Architecture 80
history 446
hold-priority 4469
hold-time 4254
hop-limit 4470
host area 2280
host-core-affinity 4031
hostname 447
icmp-echo 744
if-arbiter 648
igmp snooping 2974
igmp snooping fast-leave 2975
igmp snooping mrouter 2976
igmp snooping querier 2977
igmp snooping report-suppression 2978
igmp snooping static-group 2979
ignore-lsp-errors 2740
import map 2625
import-bgp-routes 4255
ingress cos map 3712
ingress dscp map 3713
ingress exp map 3714
inter-area-lsp 4256
interface 649
interface po 1398
interface sa 1399
intra-domain-link 1432

 © 2021 IP Infusion Inc. Proprietary

intra-domain-peer 1433
ip access-group 345
ip access-list default 349
ip access-list filter 350
ip access-list fragments 353
ip access-list icmp 354
ip access-list remark 359
ip access-list resequence 360
ip access-list standard 322
ip access-list standard filter 323
ip access-list tcp|udp 361
ip access-list 348
ip address A.B.C.D/M 650
ip address dhcp 581
ip address dhcp 651
ip arp 2838
ip arp vrf 2839
ip as-path access-list 2524
ip bfd static all-interfaces 3528
ip community-list <100-500> 2526
ip community-list <1-99> 2525
ip community-list expanded 2527
ip community-list standard 2528
ip community-list WORD 2529
ip dhcp client request 582
ip dhcp relay (configure mode) 594
ip dhcp relay (interface mode) 595
ip dhcp relay (L3VPN) 599
ip dhcp relay address 596
ip dhcp relay information option 597
ip dhcp relay information source-ip 598
ip dhcp snooping database 553
ip domain-list 615
ip domain-lookup 616
ip domain-name 617
ip extcommunity-list <100-500> 2531
ip extcommunity-list <1-99> 2530
ip extcommunity-list expanded 2532
ip extcommunity-list standard 2533
ip forwarding 652
ip host 618
ip igmp 2941
ip igmp access-group 2942
ip igmp immediate-leave 2943
ip igmp join-group 2944
ip igmp last-member-query-count 2945
ip igmp last-member-query-interval 2946
ip igmp limit 2947
ip igmp mroute-proxy 2948
ip igmp offlink 2949
ip igmp proxy unsolicited-report-interval 2951
ip igmp proxy-service 2950
ip igmp querier-timeout 2952
ip igmp query-interval 2953
ip igmp query-max-response-time 2954
ip igmp ra-option 2955
ip igmp robustness-variable 2956
ip igmp ssm-map enable 2957
ip igmp ssm-map static 2958
ip igmp startup-query-count 2960
ip igmp startup-query-interval 2961
ip igmp static-group 2959
ip igmp version 2962
ip mroute 2924
ip multicast route-limit 2925
ip multicast ttl-threshold 2926
ip multicast-routing 2927
ip name-server 619
ip ospf authentication 2281
ip ospf authentication-key 2282
ip ospf bfd 3525
ip ospf bfd 2284
ip ospf cost 2285
ip ospf database-filter 2286
ip ospf dead-interval 2287
ip ospf disable 2288
ip ospf fast-reroute per-prefix candidate disable 2289
ip ospf flood-reduction 2290
ip ospf hello-interval 2291
ip ospf message-digest-key 2293
ip ospf mtu 2295
ip ospf mtu-ignore 2296
ip ospf multi-area 2292
ip ospf network 2297
ip ospf priority 2298
ip ospf retransmit-interval 2299
ip ospf transmit-delay 2300
ip pim 3002
ip pim accept-register 3003
ip pim anycast-rp 3004
ip pim bsr-border 3005
ip pim bsr-candidate 3006
ip pim cisco-register-checksum 3007
ip pim dr-priority 3008
ip pim exclude-genid 3009
ip pim hello-holdtime 3010
ip pim hello-interval 3011
ip pim ignore-rp-set-priority 3012
ip pim jp-timer 3013
ip pim neighbor-filter 3014
ip pim passive 3015
ip pim propagation-delay 3016
ip pim register-rate-limit 3017
ip pim register-rp-reachability 3018
ip pim register-source 3019
ip pim register-suppression 3020
ip pim router-id 3021
ip pim rp-address 3022

© 2021 IP Infusion Inc. Proprietary

ip pim rp-candidate 3024
ip pim rp-register-kat 3025
ip pim spt-threshold 3026
ip pim ssm 3027
ip pim state-refresh origination-interval 3028
ip pim unicast-bsm 3029
ip prefix-list 653
ip proxy-arp 2851
ip proxy-arp 655
ip radius source-interface 1511
ip remote-address 656
ip route 2159
ip router isis 2741
ip sla 745
ip sla schedule 746
ip static bfd 3530
ip static fall-over-bfd 3529
ip unnumbered 657
ip urpf allow-default 2162
ip urpf enable 2161
ip vrf 2163
ip vrf 2626
ip vrf forwarding 658
iptables 4032
iptables restore 4033
iptables-template 4034
ipv6 access-group 366
ipv6 access-list default 370
ipv6 access-list filter 371
ipv6 access-list fragments 374
ipv6 access-list icmpv6 375
ipv6 access-list remark 379
ipv6 access-list resequence 380
ipv6 access-list sctp 381
Ipv6 access-list standard 324
ipv6 access-list standard filter 325
ipv6 access-list tcp|udp 384
ipv6 access-list 368
ipv6 address 659
ipv6 address autoconfig 564
ipv6 address dhcp 583
ipv6 address PREFIX_FROM_SERVER X:X::X:X/M 563
ipv6 bfd static all-interfaces 3531
ipv6 dhcp address-prefix-length 584
ipv6 dhcp client 587
ipv6 dhcp client request 585
ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER 562
ipv6 dhcp relay (configure mode) 600
ipv6 dhcp relay (interface mode) 601
ipv6 dhcp relay (L3VPN) 604
ipv6 dhcp relay address 602
ipv6 dhcp relay subscriber-id 603
ipv6 forwarding 660
ipv6 mroute 2928
ipv6 nd current-hoplimit 2840
ipv6 nd link-mtu 2841
ipv6 nd managed-config-flag 2842
ipv6 nd other-config-flag 2843
ipv6 nd prefix 2844
ipv6 nd ra-interval 2846
ipv6 nd ra-lifetime 2847
ipv6 nd reachable-time 2848
ipv6 nd retransmission-time 2849
ipv6 nd suppress-ra 2850
ipv6 neighbor 2852
ipv6 ospf bfd 2397
ipv6 ospf cost 2398
ipv6 ospf dead-interval 2399
ipv6 ospf display route single-line 2400
ipv6 ospf hello-interval 2401
ipv6 ospf link-lsa-suppression 2402
ipv6 ospf mtu-ignore 2403
ipv6 ospf neighbor 2404
ipv6 ospf network 2406
ipv6 ospf priority 2407
ipv6 ospf restart grace-period 2408
ipv6 ospf restart helper 2409
ipv6 ospf restart planned-only 2410
ipv6 ospf retransmit-interval 2411
ipv6 ospf transmit-delay 2412
ipv6 prefix-list 661
ipv6 router isis 2742
ipv6 router ospf 2413
ipv6 static bfd 3533
ipv6 static fall-over-bfd 3532
ipv6 te-metric 2415
ipv6 unnumbered 663
isis authentication key-chain 2743
isis authentication mode md5 2744
isis authentication send-only 2745
isis bfd 3526
isis bfd 2746
isis circuit-type 2747
isis csnp-interval 2748
isis fast-reroute per-prefix candidate disable 2749
isis hello padding 2752
isis hello-interval 2750
isis hello-multiplier 2751
isis lsp-interval 2753
isis mesh-group 2754
isis metric 2755
isis network 2756
isis password 2757
isis priority 2758
isis restart grace-period 2795
isis restart helper 2797
isis restart suppress-adjacency 2798

 © 2021 IP Infusion Inc. Proprietary

isis restart-hello-interval 2796
isis retransmit-interval 2759
isis tag 2763
isis te-metric 2764
isis wait-timer 2761
isis wide-metric 2762
ispf 2760
is-type 2765
keepalive-interval 4257
keepalive-timeout 4258
keep-multiplier 4351
key chain 2766
key chain 3499
key 2767
key 3498
key-string encrypted 2769
key-string encrypted 3501
key-string 2768
key-string 3500
l2-move allow-first-frame 3391
l2vpn-unnumbered-mode 2534
label-record 4471
label-retention-mode 4259
label-switching 4129
lacp destination-mac 1400
lacp force-up 1401
lacp port-priority 1402
lacp system-priority 1403
lacp timeout 1404
ldp advertisement-mode 4260
ldp hello-interval 4261
ldp hold-time 4262
ldp keepalive-interval 4263
ldp keepalive-timeout 4264
ldp label-retention-mode 4265
ldp multicast-hellos 4266
ldp-optimization 4267
level 3180
license get 1020
license refresh 1021
license release 1022
line console 448
line vty (all line mode) 449
line vty (line mode) 450
line vty 390
link-debounce-time 664
link-fault-pass-through enable 1073
link-type 992
lldp debug 1524
lldp debug 3260
lldp disable default-agent 3261
lldp ip 1525
lldp ip 3262
lldp run 1526
lldp run 3229
lldp tlv 1527
lldp tlv 3263
lldp tlv basic-mgmt 3230
lldp tlv ieee-8021-org-specific 3232
lldp tlv ieee-8023-org-specific 3233
lldp tlv med 3231
lldp tlv-select 1528
lldp tlv-select basic-mgmt 3234
lldp tlv-select ieee-8021-org-specific 3235
lldp tlv-select ieee-8023-org-specific 3236
lldp-agent 3227
load interval 665
load-balance rtag7 915
load-balance rtag7 hash 918
load-balance rtag7 macro-flow 919
load-balance rtag7 vxlan inner-l2 3958
load-balance rtag7 vxlan inner-l3 3959
locator led 495
log syslog 888
log-adjacency-changes 2416
log-adjacency-changes 2301
logging cli 451
logging console 889
logging level 890
logging logfile 892
logging monitor 893
logging remote facility 894
logging remote server 895
logging timestamp 897
logout 452
loopback 666
loop-detection 4268
loop-detection 4352
loop-detection-hop-count 4269
loop-detection-path-vec-count 4270
loss-measurement uni-link-loss 667
lsp-gen-interval 2770
lsp-mtu 2771
lsp-refresh-interval 2772
mac 3960
mac access-group 391
mac access-list default 394
mac access-list filter 395
mac access-list remark 397
mac access-list resequence 398
mac access-list 393
mac ageing display 1297
mac vrf 3961
mac-holdtime 3962
Management Interface 81
map qos-profile cos-to-queue 4009
map qos-profile queue-color-to-cos 4010
map vnid 3963

map-route A.B.C.D 4216
map-route A.B.C.D 4353
map-route A.B.C.D 4444
map-route X:X::X:X 4354
map-route X:X::X:X 4445
match access-group 3715
match as-path 2183
match community 2184
match cos 3716
match cos inner 3717
match dscp 3718
match extcommunity 2185
match interface 2186
match ip address 2187
match ip address prefix-list 2188
match ip next-hop 2189
match ip next-hop prefix-list 2190
match ip peer 2191
match ip peer 2535
match ip rtp 3720
match ipv6 address 2192
match ipv6 address prefix-list 2193
match ipv6 next-hop 2194
match ipv6 next-hop prefix-list 2195
match ipv6 peer 2196
match mac 3721
match metric 2197
match origin 2198
match precedence 3722
match protocol 3723
match qos-group 3724
match route-type 2199
match tag 2200
match traffic-type 3725
match vlan 3726
match vlan 4130
match vlan inner 3727
max-area-address 2773
max-concurrent-dd 2302
max-concurrent-dd 2417
maximum-area 2303
maximum-paths 2164
max-lsp-lifetime 2774
max-paths 2536
max-session 453
max-static-routes 2165
max-traffic-class-group 3312
mcec domain configuration 1434
memory 4035
mep crosscheck 3162
mep lowest-priority-defect 3163
message-ack 4437
metric-style 2775
mlag 1435
mode 1436
monitor queue-drops 669
monitor session 968
monitor session shut 969
monitor speed 668
monitor speed threshold 670
mpls ac-group 4132
mpls admin-groups 4133
mpls bandwidth-class 4134
mpls disable-all-interfaces 4135
mpls enable-all-interfaces 4136
mpls ftn-entry tunnel-id 4137
mpls ftn-entry 4139
mpls ilm-entry pop 4140
mpls ilm-entry swap 4141
mpls ilm-entry vpnpop 4143
mpls ingress-ttl 4144
mpls l2-circuit 4145
mpls l2-circuit-fib-entry 4148
mpls label mode 4149
mpls ldp-igp sync isis 4271
mpls ldp-igp sync ospf 4272
mpls ldp-igp sync-delay 4273
mpls local-packet-handling 4151
mpls lsp-model 4152
mpls lsp-stitching 4153
mpls map-route 4154
mpls min-label-value 4155
mpls propagate-ttl 4156
mpls traffic-eng 2777
mpls traffic-eng 4157
mpls traffic-eng router-id 2778
mpls traffic-eng srlg 4158
mpls-l2-circuit NAME 4146
mtu 671
multicast 672
multicast-hellos 4274
nat dnat 4036
nat snat 4037
nd-ageing-timeout 2853
nd-cache disable 3964
nd-reachable-time 2854
neighbor 2304
neighbor 4275
neighbor A.B.C.D 4355
neighbor activate 2537
neighbor advertisement-interval 2538
neighbor allowas-in 2539
neighbor allow-ebgp-vpn 2627
neighbor as-origination-interval 2541
neighbor as-override 2628
neighbor attribute-unchanged 2542
neighbor authentication-key 2543
neighbor capability dynamic 2544

© 2021 IP Infusion Inc. Proprietary

neighbor capability graceful-restart 2545
neighbor capability orf prefix-list 2546
neighbor capability route-refresh 2548
neighbor collide-established 2549
neighbor default-originate 2550
neighbor description 2551
neighbor disallow-infinite-holdtime 2552
neighbor distribute-list 2553
neighbor dont-capability-negotiate 2554
neighbor ebgp-multihop 2555
neighbor enforce-multihop 2556
neighbor fall-over bfd 2557
neighbor filter-list 2558
neighbor g-shut 2559
neighbor g-shut-timer 2560
neighbor limit 2561
neighbor local-as 2562
neighbor maximum-prefix 2563
neighbor next-hop-self 2564
neighbor optional-as 2565
neighbor override-capability 2566
neighbor passive 2567
neighbor peer-group 2568
neighbor port 2572
neighbor prefix-list 2573
neighbor remote-as 2575
neighbor remove-private-AS 2577
neighbor restart-time 2578
neighbor route-map 2579
neighbor route-reflector-client 2581
neighbor route-server-client 2582
neighbor send-community 2583
neighbor send-community 2629
neighbor shutdown 2584
neighbor soft-reconfiguration inbound 2585
neighbor soo 2630
neighbor strict-capability-match 2586
neighbor timers 2587
neighbor unsuppress-map 2589
neighbor update-source 2590
neighbor version 2591
neighbor weight 2592
neighbor WORD peer-group 2594
neighbor WORD peer-group range 2571
neighbor X:X::X:X 4356
net 2779
network 2305
network 2595
network synchronization 2597
no debug all 2855
no nvo vxlan 3965
no shut 973
no-cspf 4357
no-loop-detection 4358
non-virtual-channel 3181
no-php 4359
no-refresh-path-parsing 4360
no-refresh-resv-parsing 4361
ntp acl 759
ntp authenticate 760
ntp authentication-key 761
ntp discard 762
ntp enable 763
ntp logging 764
ntp master 765
ntp master stratum 766
ntp peer 767
ntp server 769
ntp source-interface 771
ntp sync-retry 772
ntp trusted-key 773
nvo vxlan 3966
nvo vxlan mac-ageing-time 3969
nvo vxlan max-cache-disable 3970
nvo vxlan tunnel qos-map-mode cos-dscp 4011
nvo vxlan vtep-ip-global 3971
operational-ip 3392
ospf abr-type 2307
ospf area-interface-config-mode 2308
ospf flood-reduction 2309
ospf restart grace-period 2310
ospf restart helper 2311
ospf router-id 2312
os-type 4038
os-variant 4039
outer-vlan VLAN_RANGE2 (inner-vlan VLAN_RANGE2 |) 1555
overflow database 2313
overflow database external 2314
override-diffserv 4217
override-diffserv 4446
pack-affinity 4472
passive-interface 2315
passive-interface 2418
passive-interface 2780
permit 933
php 4362
physical-ring 3182
PIM-SM Configuration 2888
ping (interactive) 456
ping 454
ping ethernet mac 3164
ping mpls 4159
police 3728
policy 934
policy-map 3731
Port Security using MC-LAG 1212
port-channel load-balance 1405

port-channel min-bandwidth - dynamic LAG min-bandwidth 1406
port-channel min-bandwidth - static LAG min-bandwidth 1408
port-channel min-links - dynamic LAG min-links 1407
port-channel min-links - static LAG min-links 1409
port-security 1544
prc-interval-exp 2781
preempt-mode 3393
primary ADMIN-GROUP-NAME 4363
primary affinity 4364
primary bandwidth 4365
primary class-to-exp-bit 4218
primary class-type 4456
primary cspf 4366
primary cspf-retry-limit 4367
primary cspf-retry-timer 4368
primary elsp-signaled 4219
primary elsp-signaled 4448
primary fast-reroute bandwidth 4428
primary fast-reroute hold-priority 4429
primary fast-reroute hop-limit 4430
primary fast-reroute node-protection 4431
primary fast-reroute protection 4432
primary fast-reroute setup-priority 4433
primary filter 4369
primary hold-priority 4370
primary hop-limit 4371
primary label-record 4372
primary llsp 4220
primary llsp 4449
primary local-protection 4373
primary map class 4447
primary no-affinity 4374
primary no-cspf 4375
primary no-record 4376
primary path 4377
primary policer 4378
primary record 4379
primary retry-limit 4380
primary retry-timer 4381
primary reuse-route-record 4382
primary setup-priority 4383
primary traffic 4384
primary-lsp 4473
priority (queuing) 3733
priority 3394
priority 3732
priority-flow-control accept-peer-config 3338
priority-flow-control advertise-local-config 3339
priority-flow-control cap 3341
priority-flow-control enable 3340
priority-flow-control enable priority 3342
priority-flow-control link-delay-allowance 3343
priority-flow-control mode 3344
private-vlan association 1450
private-vlan community 1451
private-vlan isolated 1452
private-vlan primary 1453
privilege level 458
profile name 3183
propagate-release 4276
pw-status-tlv 4277
qcn enable 3330
qos (enable | disable) 3734
qos map-profile 3735
qos profile 3736
qos profile cos-to-queue 4012
qos profile dscp-to-queue 4013
qos profile precedence-to-queue 3738
qos profile queue-color-to-cos 4014
qos profile queue-color-to-dscp 4015
qos profile queue-to-precedence 3739
qos remark 3740
qos statistics 3741
queue cos 4016
queue dscp 4017
queue-limit 3742
quit 459
radius-server dot1x deadtime 1512
radius-server dot1x host 1513
radius-server dot1x key 1515
radius-server dot1x retransmit 1516
radius-server dot1x timeout 1517
radius-server login host 788
radius-server login host acct-port 789
radius-server login host auth-port 790
radius-server login host key 791
radius-server login key 793
radius-server login timeout 794
random-detect 3743
raps-channel-vlan 3186
rd (route distinguisher) 2631
redistribute 2316
redistribute 2419
redistribute 2598
redistribute 2782
redistribute isis 2784
redistribute isis WORD 2785
refresh-path-parsing 4386
refresh-reduction 4438
refresh-resv-parsing 4387
refresh-time 4385
reload 460
reload vm-name 4040
remote destination 978
renew ip dhcp snooping binding database 554
request-labels-for 4278

© 2021 IP Infusion Inc. Proprietary

request-retry 4279
request-retry-timeout 4280
restart bgp graceful 2600
restart ipv6 ospf graceful 2421
restart isis graceful 2799
restart ldp graceful 4281
restart ospf graceful 2318
restart rsvp graceful 4388
restart-timer 2800
retry-limit 4474
retry-timer 4475
rewrite ingress 4162
ring-id 3184
ring-type 3185
role 935
route-map 2201
router bgp 2601
router ipv6 ospf 2423
router isis 2786
router ldp 4282
router ospf 2319
router ospf vrf 2451
router rsvp 4389
router vrrp 3395
route-record 4476
router-id 2166
router-id 2422
router-id 4283
route-target 2632
rpl role 3188
rsvp ack-wait-timeout 4439
rsvp hello-interval 4390
rsvp hello-receipt 4391
rsvp hello-timeout 4392
rsvp keep-multiplier 4393
rsvp message-ack 4440
rsvp refresh-reduction 4441
rsvp refresh-time 4394
rsvp-path 4395
rsvp-trunk 4396
rsvp-trunk 4477
rsvp-trunk-restart 4397
secondary ADMIN-GROUP-NAME 4398
secondary bandwidth 4399
secondary class-type 4457
secondary cspf 4400
secondary cspf-retry-limit 4401
secondary cspf-retry-timer 4402
secondary elsp-signaled 4222
secondary elsp-signaled 4451
secondary filter 4403
secondary hold-priority 4404
secondary hop-limit 4405
secondary label-record 4406
secondary llsp 4223
secondary llsp 4452
secondary local-protection 4407
secondary map class 4221
secondary map class 4450
secondary no-affinity 4408
secondary no-cspf 4409
secondary no-record 4410
secondary path 4411
secondary policer 4412
secondary record 4413
secondary retry-limit 4414
secondary retry-timer 4415
secondary reuse-route-record 4416
secondary setup-priority 4417
secondary srlg-disjoint 4163
secondary traffic 4418
secondary-disk-image 4041
secondary-lsp 4478
secondary-priority srlg-disjoint 4164
Secured MAC Addresses Learned Statically 1209
send-lifetime 2787
send-lifetime 3502
server 420
service advanced-vty 461
service dns-masq 4042
service ma-type 3165
service password-encryption 462
service terminal-length 463
service unsupported-transceiver 574
service-policy 3745
service-policy type qos 3746
service-policy type queuing 3747
service-template 4165
service-tpid 4166
set aggregator 2202
set as-path 2203
set atomic-aggregate 2204
set bridge cos 3748
set bridge dscp 3749
set comm-list 2205
set community 2206
set cos 3751
set dampening 2208
set dscp 3752
set extcommunity 2209
set interface null0 2211
set ip next-hop 2212
set ipv6 next-hop 2213
set level 2214
set lldp agt-circuit-id 3237
set lldp chassis locally-assigned 3239
set lldp chassis-id-tlv 1530
set lldp chassis-id-tlv 3238

© 2021 IP Infusion Inc. Proprietary

set lldp chassis-id-tlv 3264
set lldp disable 1531
set lldp disable 3240
set lldp disable 3265
set lldp enable 1532
set lldp enable 3241
set lldp enable 3266
set lldp locally-assigned 1533
set lldp locally-assigned 3242
set lldp locally-assigned 3267
set lldp management-address-tlv 1534
set lldp management-address-tlv 3243
set lldp management-address-tlv 3268
set lldp med-devtype 3244
set lldp msg-tx-hold 1535
set lldp msg-tx-hold 3245
set lldp msg-tx-hold 3269
set lldp port-id-tlv 3246
set lldp system-description 1536
set lldp system-description 3270
set lldp system-name 1537
set lldp system-name 3271
set lldp timer 1538
set lldp timer 3247
set lldp timer 3272
set lldp too-many-neighbors 1539
set lldp too-many-neighbors 3249
set lldp too-many-neighbors 3273
set lldp tx-fast-init 3250
set lldp tx-max-credit 3251
set local-preference 2215
set metric 2216
set metric-type 2217
set mpls class 3754
set origin 2218
set originator-id 2219
set precedence 3755
Set Priority 1609
set qos queue scheduler 3757
set qos-group 3756
set queue 3758
set tag 2220
set vpnv4 next-hop 2221
set weight 2222
setup-priority 4479
sflow agent-ip 825
sflow collector 826
sflow poll-interval 827
sflow sampling enable 828
sflow sampling-rate 829
shape 3759
shape rate 3760
show (xml|json) running-config 549
show aaa accounting 424
show aaa authentication 421
show aaa authentication login 422
show aaa groups 423
show access-list log-cache 400
show access-lists 399
show allowed-ethertype 1298
show application-priority bridge 3313
show application-priority interface 3314
show arp 2856
show arp access-lists 401
show bfd 3503
show bfd interface 3504
show bfd session 3506
show bfd session A.B.C.D 3510
show bfd session ipv6 3513
show bgp 2635
show bgp A.B.C.D 2636
show bgp A.B.C.D/M 2638
show bgp client 2639
show bgp community 2640
show bgp community-list 2642
show bgp dampening dampened-paths 2643
show bgp dampening flap-statistics 2644
show bgp dampening parameters 2647
show bgp filter-list 2649
show bgp inconsistent-as 2651
show bgp ipv6 2652
show bgp ipv6 peer-group 2655
show bgp l2vpn evpn 3972
show bgp l2vpn evpn summary 3976
show bgp l2vpn vpls 2656
show bgp neighbors 2659
show bgp neighbors advertised-routes 2663
show bgp neighbors received prefix-filter 2664
show bgp neighbors received-routes 2665
show bgp neighbors routes 2666
show bgp nexthop-tracking 2668
show bgp nexthop-tree-details 2670
show bgp paths 2671
show bgp prefix-list 2672
show bgp quote-regexp 2673
show bgp regexp 2674
show bgp route-map 2675
show bgp statistics 2676
show bgp summary 2678
show bgp X:X::X:X 2681
show bgp X:X::X:X/M longer prefixes 2682
show bootup-parameters 862
show bridge 1299
show class-map 3761
show cli 465
show cli history 466
show clns is-neighbors 2802
show clns neighbors 2804

© 2021 IP Infusion Inc. Proprietary

show clock 464
show controller details 575
show cores 863
show cpu-queue details 3762
show cross-connect 1074
show cross-connect 1556
show crypto csr 467
show cspf rsvp forwarding-timer 2320
show cspf rsvp forwarding-timer 2806
show cvlan registration table 3203
show data-center-bridging 3315
show debug radius 795
show debug ssh-server 804
show debug tacacs+ 936
show debug telnet-server 950
show debugging bfd 3516
show debugging bgp 2683
show debugging dot1x 1518
show debugging ip arp 2858
show debugging ip dhcp snooping 555
show debugging ip igmp 2963
show debugging ip mrib 2929
show debugging ip pim 3030
show debugging ipv6 nd 2859
show debugging ipv6 ospf 2424
show debugging isis 2807
show debugging lacp 1410
show debugging ldp 4290
show debugging lldp 3252
show debugging mstp 1350
show debugging nsm 468
show debugging ospf 2321
show debugging pim 3031
show debugging rib 2167
show debugging rsvp 4482
show debugging vrrp 3396
show dot1x 1519
show dtag vlan 1454
show enhanced-transmission-selection bridge 3317
show enhanced-transmission-selection interface 3319
show errdisable details 1271
show etherchannel 1411
show ethernet cfm errors 3166
show ethernet cfm ma status 3167
show ethernet cfm maintenance-points local mep 3168
show ethernet cfm maintenance-points local mip 3170
show ethernet cfm maintenance-points remote 3171
show evpn multi-homing all 3998
show evpn multihoming-status 3999
show filter 984
show flowcontrol 673
show forwarding profile limit 920
show g8032 erp-instance 3189
show g8032 physical-ring 3190
show g8032 profile 3191
show hardware-discard-counters 674
show hardware-information 496
show hardware-profile filters 922
show hosts 620
show hosts 723
show igmp snooping groups 2982
show igmp snooping interface 2980
show igmp snooping mrouter 2985
show igmp snooping statistics 2986
show installers 1023
show interface 676
show interface capabilities 678
show interface counters (indiscard-stats|outdiscard-stats) 687
show interface counters 680
show interface counters drop-stats 683
show interface counters error-stats 686
show interface counters protocol 690
show interface counters queue-drop-stats 691
show interface counters queue-stats 692
show interface counters rate 694
show interface counters speed 696
show interface counters summary 697
show interface errdisable status 1272
show interface fec 699
show interface switchport 1300
show interface transceiver details 577
show ip access-lists 402
show ip bgp 2684
show ip bgp cidr-only 2687
show ip bgp community-info 2689
show ip bgp peer-group 2690
show ip bgp peer-group vrf all 2691
show ip bgp rtfilter all 2692
show ip bgp scan 2693
show ip bgp vpnv4 2694
show ip dhcp relay 605
show ip dhcp relay address 607
show ip dhcp relay option statistics 608
show ip dhcp relay statistics 609
show ip dhcp snooping arp-inspection statistics bridge 556
show ip dhcp snooping binding bridge 559
show ip dhcp snooping bridge 557
show ip extcommunity-list 2698
show ip forwarding 701
show ip igmp groups 2964
show ip igmp interface 2966
show ip igmp proxy 2968
show ip igmp ssm-map 2970
show ip interface 702
show ip isis igp-shortcut-lsp 2808
show ip isis lfa-config 2816

show ip isis route 2809
show ip isis route fast-reroute 2815
show ip isis route igp-shortcut 2811
show ip mroute 2930
show ip mvif 2933
show ip ospf 2322
show ip ospf border-routers 2326
show ip ospf database brief 2327
show ip ospf database detail 2329
show ip ospf igp-shortcut-lsp 2336
show ip ospf igp-shortcut-route 2337
show ip ospf interface 2338
show ip ospf multi-area-adjacencies 2341
show ip ospf neighbor 2343
show ip ospf route 2347
show ip ospf virtual-links 2350
show ip ospf valid 2349
show ip pim bsr-router 3032
show ip pim interface 3034
show ip pim local-members 3036
show ip pim mroute 3037
show ip pim neighbor 3039
show ip pim nexthop 3042
show ip pim rp mapping 3044
show ip pim rp-hash 3043
show ip prefix-list 704
show ip protocols 2352
show ip protocols 2699
show ip protocols 2813
show ip route 705
show ip route A.B.C.D/M longer-prefixes 707
show ip route fast-reroute 2354
show ip route fast-reroute 2814
show ip rpf 2168
show ip sla statistics 747
show ip sla summary 749
show ip vrf 2701
show ip vrf 716
show ipv6 access-lists 403
show ipv6 dhcp interface 565
show ipv6 dhcp relay 610
show ipv6 dhcp relay address 611
show ipv6 dhcp vendor-opts 589
show ipv6 forwarding 717
show ipv6 interface brief 718
show ipv6 neighbors 2860
show ipv6 ospf 2425
show ipv6 ospf database 2426
show ipv6 ospf interface 2430
show ipv6 ospf neighbor 2432
show ipv6 ospf route 2435
show ipv6 ospf virtual-links 2440
show ipv6 ospfv3 topology 2438
show ipv6 prefix-list 722
show ipv6 route 720
show ipv6 route fast-reroute 2437
show ipv6 rpf 2170
show ipv6 vrf 2442
show isis counter 2817
show isis database 2818
show isis interface 2821
show isis spf-logs 2824
show isis topology 2825
show lacp sys-id 1414
show lacp-counter 1415
show ldp 4291
show ldp adjacency 4293
show ldp advertise-labels 4294
show ldp downstream 4295
show ldp fec 4297
show ldp igp sync 4299
show ldp interface 4300
show ldp lsp 4302
show ldp mpls-l2-circuit 4304
show ldp routes 4307
show ldp session 4308
show ldp statistics 4310
show ldp statistics advertise-labels 4312
show ldp targeted-peers 4313
show ldp upstream 4314
show license 1024
show list 469
show lldp 1540
show lldp 3274
show lldp interface 3256
show lldp neighbors 3253
show logging 898
show logging cli 470
show logging last 900
show logging logfile 901
show logging logfile last-index 902
show logging logfile start-seqn end-seqn 903
show logging logfile start-time end-time 904
show mac access-lists 404
show mac address-table bridge 1303
show mac address-table count bridge 1302
show mac-address-table bridge 1 learning 1305
show max-transaction limit 546
show mcec statistics 1437
show mlag detail 1439
show mlag domain 1441
show mlag phy-digest 1444
show monitor 979
show monitor running configuration 985
show monitor session 981
show mpls 4167
show mpls admin-groups 4169
show mpls bandwidth-class 4170

© 2021 IP Infusion Inc. Proprietary

show mpls counters ldp 4171
show mpls counters rsvp 4173
show mpls counters static 4175
show mpls cross-connect-table 4177
show mpls forwarding-table 4179
show mpls ftn-table 4182
show mpls ilm-table 4184
show mpls in-segment-table 4186
show mpls l2-circuit 4188
show mpls l2-circuit statistics 4190
show mpls ldp discovery 4316
show mpls ldp neighbor 4317
show mpls ldp parameter 4318
show mpls mapped-routes 4192
show mpls out-segment-table 4193
show mpls qos-resource 4195
show mpls vc-table 4197
show mpls vrf 4198
show mpls vrf-forwarding-table vrf 4199
show nsm client 471
show nsm forwarding-timer 472
show ntp authentication-keys 774
show ntp authentication-status 775
show ntp logging-status 776
show ntp peers 779
show ntp peer-status 777
show ntp statistics 780
show ntp trusted-keys 782
show nvo vxlan 3978
show nvo vxlan access-if-config 3980
show nvo vxlan arp-cache 3981
show nvo vxlan counters access-port 3983
show nvo vxlan counters network-port 3986
show nvo vxlan mac-table 3988
show nvo vxlan nd-cache 3991
show nvo vxlan route-count 4000
show nvo vxlan static host state 3993
show nvo vxlan tunnel 3995
show nvo vxlan vni-name 4002
show policy-map interface 3765
show policy-map 3764
show port etherchannel 1416
show port-security 1545
show priority-flow-control details 3345
show priority-flow-control statistics 3347
show privilege 473
show process 474
show qcn cnpv 3333
show qcn configuration 3331
show qcn cp 3335
show qos-profile 3768
show qos-profile interface 3770
show queuing interface 3771
show radius-server 796
show rbac-policy 937
show rbac-role 938
show route-map 2223
show router-id 2172
show rsvp 4483
show rsvp admin-groups 4486
show rsvp control-adjacency 4487
show rsvp data-link 4489
show rsvp diffserv-info 4224
show rsvp diffserv-info 4453
show rsvp dste-info 4458
show rsvp dste-info 4491
show rsvp graceful-restart 4490
show rsvp interface 4492
show rsvp local-addresses 4495
show rsvp neighbor 4494
show rsvp nexthop-cache 4497
show rsvp path 4498
show rsvp session 4500
show rsvp session count 4502
show rsvp session egress 4503
show rsvp session ingress 4507
show rsvp session LSP-NAME 4511
show rsvp session transit 4514
show rsvp summary-refresh 4517
show rsvp trunk 4518
show rsvp version 4520
show running-config 475
show running-config aaa 425
show running-config access-list 406
show running-config aclmgr 405
show running-config as-path access-list 2702
show running-config cfm 3173
show running-config community-list 2703
show running-config cpu-queue 3777
show running-config dhcp 612
show running-config dns 622
show running-config interface 725
show running-config interface igmp 2971
show running-config interface ip 727
show running-config interface ipv6 728
show running-config interface isis 2827
show running-config interface mpls 4200
show running-config interface multicast 2935
show running-config ip 729
show running-config ip sla 750
show running-config ipv6 730
show running-config ipv6 access-list 407
show running-config logging 905
show running-config mpls 4201
show running-config ntp 783
show running-config nvo vxlan 3996
show running-config prefix-list 731
show running-config qos 3772

© 2021 IP Infusion Inc. Proprietary

show running-config radius 798
show running-config route-map 2224
show running-config router 2173
show running-config router isis 2828
show running-config router vrrp 3397
show running-config router-id 2174
show running-config service-template 4202
show running-config snmp 840
show running-config ssh server 805
show running-config switch 1273
show running-config tacacs+ 939
show running-config telnet server 951
show running-config urpf 2175
show running-config vc 4203
show running-config vpls 4204
show running-config vrf 2176
show service-template 4205
show sflow 830
show sflow interface 832
show sflow statistics 833
show snmp 841
show snmp community 842
show snmp engine-id 843
show snmp group 844
show snmp host 845
show snmp user 846
show snmp view 847
show software-watchdog status 864
show spanning-tree 1351
show spanning-tree mlag operational-config 1445
show spanning-tree mlag sync-detail 1446
show spanning-tree mst 1355
show spanning-tree rpvst+ 1385
show spanning-tree statistics 1357
show ssh host-key 806
show ssh server 808
show startup-config 476
show static-channel load-balance 1420
show static-channel-group 1419
show strom-control 1377
show supported-transceiver 576
show system log 867
show system login 869
show system reboot-history 870
show system resources 871
show system uptime 873
show system-information 510
show sys-update details 1025
show tacacs-server 940
show tcp 1275
show techsupport 874
show techsupport status 876
show telnet-server 952
show tfo 993
show timezone 477
show transaction current 547
show transaction last-aborted 548
show udld 1562
show udld interface 1563
show user-account 1002
show username 809
show users 480
show vccv statistics 4206
show version 481
show vlan 1456
show vlan access-map 1455
show vlan brief 1458
show vlan classifier 1459
show vlog all 1006
show vlog clients 1007
show vlog terminals 1008
show vlog virtual-routers 1009
show vm 4043
show vm-bridge 4044
show vm-iptables 4045
show vm-iptables kernel 4046
show vm-nat details 4047
show vm-template 4048
show vrrp (global | ipv4) statistics 3403
show vrrp <1-255> 3401
show vrrp 3398
show vrrp summary 3400
shut 974
shutdown 2355
shutdown 2443
shutdown 4003
shutdown 732
snmp restart 924
snmp restart auth 1522
snmp restart bfd 3517
snmp restart bgp 2602
snmp restart isis 2789
snmp restart lacp 1421
snmp restart ldp 4284
snmp restart lldp 1541
snmp restart lldp 3258
snmp restart lldp 3275
snmp restart mribd 2936
snmp restart mstp 1360
snmp restart ospf 2356
snmp restart ospf6 2444
snmp restart pim 3045
snmp restart rib 2177
snmp restart rsvp 4419
snmp restart vrrp 3404
snmp-server community 848
snmp-server contact 849
snmp-server enable snmp 850

© 2021 IP Infusion Inc. Proprietary

snmp-server enable traps 851
snmp-server host 852
snmp-server location 854
snmp-server tcp-session 855
snmp-server user 856
snmp-server view 857
software-watchdog 877
software-watchdog keep-alive-time 879
source port 970
source vlan 971
spanning-tree autoedge 1361
spanning-tree bpdu-filter 1368
spanning-tree bpdu-guard 1369
spanning-tree edgeport 1362
spanning-tree guard 1363
spanning-tree instance restricted-role 1364
spanning-tree instance restricted-tcn 1365
spanning-tree link-type 1366
spanning-tree mst configuration 1367
spanning-tree restricted-domain-role 1370
spanning-tree restricted-role 1371
spanning-tree restricted-tcn 1372
spanning-tree rpvst+ configuration 1389
spanning-tree te-msti configuration 1373
spanning-tree vlan restricted-role 1390
spanning-tree vlan restricted-tcn 1391
speed 733
spf-interval-exp 2790
srlg-disjoint 4207
ssh 810
ssh keygen host 815
ssh login-attempts 816
ssh server algorithm encryption 813
ssh server port 817
ssh server session-limit 818
ssh6 811
start vm-name 4049
start-time (absolute) 962
start-time after (relative) 963
start-time now (current) 964
Static Configuration 1173
Static LAG Minimum Link Configuration 1112
static-bind 4050
static-channel-group 1422
stop vm-name 4051
storm-control 1374
storm-control 3778
String Parameters 71
Sub-ring with Virtual Channel 3081
Sub-ring without Virtual Channel on a LAG interface 3101
subscriber urpf enable 2178
summary-address 2357
summary-address 2445
summary-address 2791
summary-prefix 2792
switch-back-delay 3405
switching-mode 3192
switchover type 1447
switchport 1306
switchport 735
switchport access 1461
switchport allowed ethertype 1307
switchport allowed ethertype 736
switchport customer-edge 3204
switchport customer-edge default-svlan 3205
switchport customer-edge hybrid 3206
switchport customer-edge trunk 3207
switchport customer-edge vlan registration 3208
switchport customer-network vlan 3209
switchport customer-network vlan translation 3210
switchport ethertype 3212
switchport hybrid 1462
switchport mode 1464
switchport mode 3213
switchport mode access ingress-filter 1465
switchport mode customer-edge 3215
switchport mode customer-edge hybrid acceptable-frame-type 3216
switchport mode hybrid acceptable-frame-type 1466
switchport mode hybrid ingress-filter 1467
switchport mode ingress-filter 3214
switchport mode private-vlan 1473
switchport mode trunk ingress-filter 1468
switchport port-security 1546
switchport port-security logging 1547
switchport port-security mac-address 1548
switchport port-security maximum 1550
switchport private-vlan host-association 1474
switchport private-vlan mapping 1475
switchport protected 737
switchport provider-edge 3217
switchport provider-network vlan translation 3218
switchport trunk allowed 1469
switchport trunk allowed vlan dtag 1471
switchport trunk native 1472
synchronization 2603
Syslog Severities 882
sys-reload 483
sys-shutdown 484
system-load-average 514
sys-update commit 1026
sys-update delete 1027
sys-update get 1028
sys-update install 1029
sys-update list-version 1031
sys-update rollback 1032
sys-update un-install 1033
tacacs-server login host 942

tacacs-server login key 944
tacacs-server login timeout 945
targeted-peer ipv4 4285
targeted-peer-hello-interval 4286
targeted-peer-hold-time 4287
tcn-propagation-instance 3194
tcn-propogation 3193
tcp 3321
telnet 953
telnet server port 955
telnet server session-limit 956
telnet6 954
terminal length 485
terminal monitor 486
tfo 995
threshold 751
timeout 752
timer 3195
time-range 965
timers bgp 2604
timers lsa arrival 2358
timers spf exp 2447
timers spf exp 2359
timers throttle lsa 2360
to A.B.C.D 4420
to X:X::X:X 4421
trace mpls 4208
traceroute 487
traceroute ethernet 3174
traffic 4480
traffic-class-group 3322
Transaction-based Command-line Interface 73
transceiver 738
transport-address ipv4 4288
trust dscp 3780
tunnel-id 4210
tunnel-name 4211
tunnel-select-policy 4212
udld 1558
udld message-time 1559
udld mode 1560
udld state 1561
udp 3323
undebug all ip pim 3046
undebug bgp 2606
undebug vrrp 3406
update-type 4422
username 1003
username keypair 820
username sshkey 819
v4-unnumbered-mode 2605
vccv cc-type 4213
vccv cv-type 4214
vcpu count 4052
virt-type 4053
virtual-channel 3196
virtual-ip 3407
virtual-nic 4054
vlan classifier activate 1477
vlan classifier group 1478
vlan classifier rule ipv4 1479
vlan classifier rule mac 1480
vlan classifier rule proto 1481
vlan database 1483
vlan dtag 1484
vlan state 1485
vlan type 3222
vlan type customer 3220
vlan type service 3221
vlan VLAN_RANGE bridge 1486
vlan VLAN_RANGE type customer 1487
vlan VLAN_RANGE type service 1488
vm-bridge-create 4055
vm-image delete 4056
vm-template 4057
vrrp compatible-v2 3408
vrrp vmac 3409
vxlan host-reachability-protocol evpn-bgp 4004
watch static-mac-movement 1277
write 488
write terminal 489
wrr-queue weight 3781
X:X::X:X 4423

© 2021 IP Infusion Inc. Proprietary

SECTION 18 # Index

Index

Numerics

802.1x Commands
  auth-mac auth-fail-action 1492
  auth-mac dynamic-vlan-creation disable 1494
  auth-mac enable 1495
  auth-mac system-auth-ctrl 1497
  debug dot1x 1498
  dot1x initialize interface 1499
  dot1x port-control 1501
  dot1x protocol-version 1502
  dot1x quiet-period 1503
  dot1x reauthentication 1505
  dot1x reauthMax 1504
  dot1x system-auth-ctrl 1506
  dot1x timeout re-authperiod 1507
  dot1x timeout server-timeout 1508
  dot1x timeout supp-timeout 1509
  dot1x timeout tx-period 1510
  ip radius source-interface 1511
  radius-server deadtime 1512
  radius-server host 1513
  radius-server key 1515
  radius-server retransmit 1516
  radius-server timeout 1517
  show debugging dot1x 1518
  show dot1x 1519

A

A.B.C.D (loose|strict) command 4326
aaa accounting default 410
aaa accounting details 411
aaa authentication attempts login 410
aaa authentication login 410
aaa authentication login console 412
aaa authentication login default 413
aaa authentication login default fallback error 415
aaa authorization config-commands default 416
aaa group server 416
aaa local authentication attempts max-fail 417
ABRs 2367
accept-lifetime 2712
ack-wait-timeout command 4436, 4439
adding multiple instances of same AS to administer route selection 1940
Adjacencies 4075
aggregate-nexthop-check 2465
area
  authentication 2230
area authentication 2230
Area Border Router 4087
  configuring 1614
Area Border Router in OSPFv3 1680
Area Border Routers 2367
area default cost 2231
area default-cost 2364
area filter-list 2236
area nssa 2237, 2365
area range 2239, 2367
area stub 2241, 2368
area virtual-link 2242, 2369
area-password 2716
area-password command 2716
arp A.B.C.D MAC 441
arp-cache disable 3943
arp-nd flood-suppress 3944, 4015
Authentication 217
authentication 1081, 3455
authentication key-chain 2717
authentication mode md5 2718
authentication OSPF 1630
authentication rip multiple keys 1588
authentication rip-multiple keys 1595
authentication send-only 2719
auth-mac auth-fail-action 1492
auth-mac dynamic-vlan-creation disable 1494
auth-mac enable 1495
auth-mac system-auth-ctrl 1497
auto-cost reference bandwidth 2245
auto-cost reference-bandwidth 2371
auto-summary 2464

B

backward compatibility 3375
bandwidth 4121
Bandwidth Configuration 3595
banner 429
begin modifier 68
bfd 3483
bfd all-interfaces 2246
bfd auth type 3482
BFD Configuration 3415
  Echo Function 3415
  Echo Interval 3422
  Multi-hop Peer Timer 3418
  Single-hop Session Timer 3420
  Slow Timer 3417
  Topology 3415, 3455
bfd echo 3484
bfd echo interval 3485
bfd interval 3488
bfd multihop-peer 3489
bfd multihop-peer A.B.C.D interval 3491
bfd multihop-peer X:X::X:X interval 3492
bfd notification 3493
BFD protocol commands 3519
  debug ospf bfd 3524
  IS-IS
    isis bfd 3526
BFD Protocol Configurations 3425
bfd slow-timer 3495
BFD Static Configurations 3451

© 2021 IP Infusion Inc. Proprietary

Topology 3451
bfd-firmware 3487
BGP 2135
BGP Commands
address-family 2461, 2610
aggregate-address 2463
auto-summary 2464
bgp aggregate-nexthop-check 2465
bgp always-compare-med 2466
bgp bestpath as-path ignore 2468
bgp bestpath compare-confed-aspath 2470
bgp bestpath compare-routerid 2471
bgp bestpath med 2473
bgp client-to-client reflection 2476
bgp cluster-id 2477
bgp confederation identifier 2478
bgp confederation peer 2479
bgp config-type 2480
bgp dampening 2481
bgp default local-preference 2483
bgp deterministic med 2484
bgp enforce-first-as 2485
bgp extended-asn-cap 2486
bgp fast-external-failover 2487
bgp g-shut 2490
bgp g-shut-capable 2491
bgp g-shut-local-preference 2492
bgp log-neighbor-changes 2493
bgp nexthop delay 2495
bgp nexthop enable 2496
bgp rfc1771-path-select 2497
bgp rfc1771-strict 2498
bgp router-id 2499
bgp scan-time 2500
bgp update-delay 2503
clear bgp * 2505
clear bgp A.B.C.D| X:X::X:X 2504
clear bgp external 2510
clear bgp peer-group 2513
clear ip bgp A.B.C.D
clear ip bgp A.B.C.D 2516
clear ip bgp ASN 2507, 2509
clear ip bgp dampening 2509
clear ip bgp flap-statistics 2512
clear ip bgp view 2516
debug bgp 2520
distance 2522
exit address family mode 2523
ip as-path access-list 2524
ip community-list 2525, 2529
ip community-list expanded 2527
ip community-list standard 2528
ip extcommunity-list
expanded 2532
extended 2531
standard 2530, 2533
neighbor
activate 2537
advertisement-interval 2538
capability dynamic 2544
capability graceful-restart 2545
capability orf prefix-list 2546
capability route-refresh 2548
collide-established 2549
default-originate 2550
distribute-list 2553
dont-capability-negotiate 2554
ebgp-multihop 2555
enforce-multihop 2556
fall-over bfd 2558
filter-list 2558
maximum-prefix 2563
next-hop-self 2564
peer-group add 2568
port 2571
remote-as 2575
remove private-as 2577
restart-time 2578
route-map 2579
route-reflector-client 2581
send-community 2583
shutdown 2584
soft-reconfiguration 2585
strict-capability-match 2586
timers 2587
unsuppress-map 2589
update-source 2590
version 2591
weight 2592
neighbor attribute-unchanged 2542
neighbor disallow-infinite-holdtime 2552
neighbor g-shut 2559
neighbor g-shut-timer 2560
neighbor passive 2567
neighbor prefix-list 2573
network 2595
redistribute 2598
restart bgp graceful 2600
router bgp 2601
show
ip bgp attribute-info 2687
ip bgp cidr-only 2687
ip bgp community 2640
ip bgp community-info 2689
ip bgp community-list 2642
ip bgp filter-list 2649
ip bgp view 2680
ip protocols bgp 2699
show bgp neighbors received prefix-filter 2664
show bgp neighbors received-routes 2665
show bgp neighbors routes 2666
show bgp paths 2671
show bgp prefix-list 2672
show bgp quote-regexp 2673
show bgp route-map 2675

© 2021 IP Infusion Inc. Proprietary

show bgp summary 2678
show ip bgp inconsistent-as 2651
show ip extcommunity-list 2698
synchronization 2603
timers 2604
BGP community value
command syntax 66
BGP configuration 1861
adding multiple instances of same AS to administer route selection 1940
configuring BGP Confederation 1881
configuring BGP distance 1977
configuring BGP Extended Community attributes 1948
configuring BGP Four-Byte AS 1945
configuring BGP weight per peer basis 1981
configuring Next-hop Tracking 1968
configuring Next-hop Tracking delay timer 1971
enabling BGP- different autonomous systems 1862
enabling EBGP Multihop 1894
enabling peer groups 1928
removing Multi-Exit Disc attribute from update messages 1942
route reflector 1866
route-map 1864
bgp dampening 2481
bgp g-shut 2490
bgp g-shut-capable 2491
bgp g-shut-local-preference 2492
bgp inbound-route-filter 2616
BGP VPN Commands
bgp inbound-route-filter 2616
clear ip bgp * vpnv4 2618
clear ip bgp <1-4294967295> vpnv4 2620
clear ip bgp A.B.C.D vpnv4 2622
debug bgp mpls 2623
import map 2625
ip vrf 2626
neighbor
send-community 2629
neighbor allow-egbp-vpn 2627
neighbor as-override 2628
neighbor send-community 2629
neighbor soo 2630
rd (route distinguisher) 2631
route-target 2632
show ip vrf 2701
site-of-origin 2630
Bidirectional Forwarding Commands 3479
Bootstrap Router 2886
bootstrap router 3032
Border Gateway BC Protocol (BGP) 2135
Border Gateway Protocol 87
braces
command syntax 65
break-before-make 4422
bridge acquire 1280
bridge address 1281
bridge ageing-time 1282
bridge cisco-interoperability 1311
Bridge commands
bridge acquire 1280
bridge address 1281
bridge ageing-time 1282
bridge protocol mstp 1318
bridge protocol rstp 1319
clear mac address-table 1295
show interface switchport bridge 1300
switchport 1306
bridge forward-time 1283
bridge instance priority 1313
bridge max-age 1286
bridge max-hops 1287
bridge multiple-spanning-tree enable 1316
bridge priority 1288
bridge protocol mstp 1318
bridge protocol provider-rstp 3199
bridge protocol rpvst+ 1383
bridge protocol rstp 1319
bridge rapid-spanning-tree enable 1321
bridge region 1322
bridge revision 1323
bridge shutdown 1289
bridge spanning-tree enable 1324
bridge spanning-tree errdisable-timeout enable 1325
bridge spanning-tree portfast bpdu-filter 1328
bridge te-msti 1330
bridge transmit-holdcount 1290
bridge-group instance 1331
bridge-group instance path-cost 1332
bridge-group path-cost 1292
bridge-group priority 1293
bridge-group vlan 1382
BSR 2886, 3032
BSR validation 2895

C

candidate status 3024
capability opaque 2249
capability restart 2250
capability restart graceful 2373
cc multicast 3155
CFM
configuration 3121
CFM commands
cc multicast 3155
mep crosscheck mpid 3162
show ethernet cfm ma status 3167
Chassis Management Module Commands 491
circuit-failover 3387
class map 3541
criteria 3541
class type qos 3706
class type queuing 3707
classification 3540
clear bgp
* 2505
A.B.C.D|X:X::X:X 2504

external 2510
peer-group 2513
clear bgp ipv6
A.B.C.D| X:X::X:X 2504
external 2510
peer-group 2513
clear clns is-neighbors 2723
clear clns neighbors 2722
clear ip bgp
ASN 2507, 2509
view 2516
clear ip bgp * vpnv4 2618
clear ip bgp <1-4294967295> vpnv4 2620
clear ip bgp A.B.C.D vpnv4 2622
clear ip igmp 2938
clear ip mroute 2922, 2989
clear ip ospf process 2253
clear ip prefix-list 635
clear ip route kernel 2151
clear ipv6 neighbors 636
clear ipv6 ospf process 2374
clear isis interface counter 2727
clear isis process 2728
clear isis route 2724
clear mac address table dynamic vxlan 3945
clear mac address-table 1295
clear ntp statistics 756
clear nvo vxlan counters 3947, 4013
clear rsvp session command 4327
clear rsvp trunk command 4328
clear snmp hostconfig 837
clear spanning-tree detected protocols 1337
clear ssh hosts 801
clear tfo counter 988
Client 217
clock timezone 430
collide-established 2549
command abbreviations 64
command completion 64
command line
errors 64
help 63
keyboard operations 67
command modes 71
configure 71
exec 71
interface 71
privileged exec 71
router 71
command negation 65
command syntax
? 66
. 66
() 65
{} 65
| 65
A.B.C.D/M 66
AA:NN 66
BGP community value 66
braces 65
conventions 65
curly brackets 65
HH:MM:SS 66
IFNAME 66
interface name 66
IPv4 address 66
IPv6 address 66
LINE 66
lowercase 65
MAC address 66
monospaced font 65
numeric range 66
parantheses 65
parentheses 65
period 66
question mark 66
square brackets 66
time 66
uppercase 65
variable placeholders 66
vertical bars 65
WORD 66
X:X::X:X 66
X:X::X:X/M 66
XX:XX:XX:XX:XX:XX 66
common commands 907, 2179
banner 429
clear ip prefix-list 635
configure terminal 432
copy running-config startup-config 436
disable 438, 465
enable 440
enable password 441
end 442
errdisable 1268
errdisable timeout 1270
exit 444
ip prefix-list 653
ip remote-address 656
ip unnumbered 657
ipv6 prefix-list 661
ipv6 unnumbered 663
log syslog 888
match as-path 2183
match community 2184
match interface 2186
match ip address 2187
match ip address prefix-list 2188
match ip next-hop 2189
match ip next-hop prefix-list 2190
match ipv6 address 2192
match ipv6 address prefix-list 2193
match ipv6 next-hop 2194
match metric 2197
match origin 2198
match route-type 2199
match tag 2200
reload 460

© 2021 IP Infusion Inc. Proprietary

route-map 2201
service advanced-vty 461
service password-encryption 462
service terminal-length 463
set as-path 2203
set atomic-aggregate 2204
set comm-list delete 2205
set community 2206
set dampening 2208
set extcommunity 2209
set ip next-hop 2212
set ipv6 next-hop 2213
set level 2214
set metric 2216
set metric-type 2217
set origin 2218
set originator-id 2219
set tag 2220
set vpnv4 next-hop 2221
set weight 2222
show access-list 465
show cli 465
show ip prefix-list 722
show list 469
show startup-config 476
show version 481
write terminal 489
Common Configure Mode Commands 907
Common NSM Layer 2 commands
flowcontrol off 645
show flowcontrol interface 673
storm-control level 1374
compatible rfc1583 2254
Configuration
BFD Configuration in BGP 3440
BFD Configuration in IS-IS 3437
BFD Configuration in RIP 3447
OSPF—BFD Multi-hop Session 3434
configuration 309
disable spanning tree 1087
configurations
Ethernet CFM 3121
configure
802.1x authentication 1081
Area Border Router for OSPFv3 1680
BGP 1861
configuring overload bit 1799
distance 1793
GMRP 191
graceful restart 1793
IGMP snooping 2905
IS-IS 1751
IS-IS-IPv6 1804
LACP 1107
LLDP 1149, 3051
metric 1764
MSTP 1193
OSPF 1605
OSPFv3 1673
passive interface 1799
Provider Bridging 3127
QoS 3539
RIPng 1603
route leaking 1783
route summarization 1788
route-map 1864
RSTP 1225
STP 1235
Configure LDP 4076
configure mode 71
Configure Multipath eBGP 1990
Configure Multipath iBPG 2002
configure OSPFv3 graceful restart 1719
configure terminal 432
configuring BGP Confederation 1881
configuring BGP Extended Community attributes 1948
configuring BGP Four-Byte AS 1945
configuring BSR
BSR topology 2894
validation commands 2895
configuring OSPF
redistributing routes into OSPF 1618
configuring overload bit in IS-IS 1799
Configuring port Breakout 230
Configuring port Breakout(100G to 4x10G) 230
configuring preempt mode 3393
configuring RIPng
enable RIPng 1603
configuring RP dynamically 2892
configuring RP statically 2889
configuring sFlow 255
Configuring VRRP
one virtual router 3355
two backup routers 3363
two virtual routers 3358
Conservative Retention Mode 4076
Control Port Group 309, 989, 991
copy 526
copy ftp running-config 527
copy ftp running-config (interactive) 529
copy ftp startup-config 525
copy ftp startup-config (interactive) 530
copy http startup-config 529
copy http startup-config (interactive) 535
copy running-config 519
copy running-config (interactive) 520
copy running-config start-config 436
copy scp (startup-config|running-config) 526
copy scp running-config 526
copy scp startup-config 526
copy scp startup-config (interactive) 532
copy sftp (startup-config|running-config) 527
copy sftp running-config 527
copy sftp startup-config 527
copy sftp startup-config (interactive) 533
copy startup-config 521
copy startup-config (interactive) 522
copy system file 523

copy system file (interactive) 524
copy tftp startup-config 528
copy tftp startup-config (interactive) 534
CoS to Queue Map Configuration 3549, 3553, 3555
CoS value 3539
cost
  OSPF 1620
curly brackets
  command syntax 65
customer-spanning-tree customer-edge path-cost 1339
customer-spanning-tree customer-edge priority 1340
customer-spanning-tree forward-time 1341
customer-spanning-tree hello-time 1342
customer-spanning-tree max-age 1343
customer-spanning-tree priority 1344
customer-spanning-tree provider-edge path-cost 1345
customer-spanning-tree provider-edge priority 1346
customer-spanning-tree transmit-holdcount 1347
cvlan registration table 3200

D

damped route 2685, 2687
data flow
  PIM-SM 2886
ddm monitor 568, 569
debug bfd all 3496
debug bgp events 2520
debug bgp filters 2520
debug bgp fsm 2520
debug bgp keepalives 2520
debug bgp mpls 2623
debug bgp updates 2520
debug cmm 492
debug ddm 571, 574
debug dns client 614
debug dot1x 1498
debug igmp 2939, 2973
debug ip ospf graceful-restart 2260
debug ip pim timer joinprune 2999, 3001
debug ipv6 ospf 2375
  ifsm 2378
  packet 2383
debug ipv6 ospf lsa 2379, 2380
debug ipv6 ospf nfsm 2381
debug ipv6 ospf nsm 2382
debug ipv6 ospf packet 2383
debug ipv6 ospf route 2386
debug isis 2729
debug lacp command 1397
debug logging 887
debug mcec 1427
debug mstp 1348
debug ntp 758
debug ospf 2255
  packet 2267
debug ospf database-timer rate-limit 2257
debug ospf events 2258
debug ospf ifsm 2259
debug ospf lsa 2264
debug ospf nfsm 2265
debug ospf nsm 2266
debug ospf packet 2267
debug ospf route 2269
debug ospf6 packet 2383
debug pim packet 2993
debug pim sparse-mode timer register 3001
debug radius 787
debug rib 2155
debug rsvp command 4330
debug sflow 823
debug snmp-server 839
debug ssh server 802
debug tacacs+ 928
debug telnet server 948
debug user-mgmt 998
debug vrrp 3388
debugging rsvp command 4420
default-information originate 2270, 2387, 2731
default-metric 2272, 2389
default-metric command 2389
description 2157
designated router priority 3008
detour identification 4426
DiffServ architecture 3539
DiffServ Commands
  elsp-preconfigured 4219, 4220, 4448, 4449
  elsp-signaled 4219, 4220, 4448, 4449
  map-route CLASS 4216, 4444
  override-diffserv 4217, 4446
disable 438, 465
disable spanning tree
  configuration 1087
  spanning-tree te-msti configuration 1373
disable VRRP session 3389
disable-igp-shortcut 4337
disable-rsvp command 4337
distance 2273, 2390, 2522
distance (OSPF command) 2273
distance in IS-IS 1793
distribute-list 1747, 2391
do 439
domain hello timeout 1429
domain priority 1430
domain system number 1431
domain-address 1428
domain-name, ip 617
domain-password 2734
dot1x initialize interface 1499
dot1x port-control 1501
dot1x protocol-version 1502
dot1x quiet-period 1503
dot1x reauthentication 1505
dot1x reauthMax 1504
dot1x system-auth-control 1506
dot1x timeout re-authperiod 1507
dot1x timeout server-timeout 1508
dot1x timeout supp-timeout 1509

 © 2021 IP Infusion Inc. Proprietary

dot1x timeout tx-period 1510
downstream 2886, 2901
Downstream on Demand 4076
Downstream Unsolicited 4076
DRNI 1165
DSCP to Queue Map Configuration 3545
DSCP value
  Differentiated Services Code Point 3540
dynamic-learning disable 3951, 4006

E

elsp-preconfigured 4219, 4220, 4448, 4449
elsp-signaled 4219, 4220, 4448, 4449
enable 440
enable db-summary-opt 2276, 2393
enable IS-IS 1751
enable multiple OSPF instances 1634
enable multiple OSPFv3 instances 1705
enable OSPFv3 1673
enable password 441
enable VRRP sessions 3390
Enable/Disable Configuration 3542
encapsulation 3787
end 442
enhanced-transmission-selection advertise-local-config 3307
Equivalence Class 4075
errdisable 1268
errdisable timeout 1270
Ethernet Ring Protection Switching (ERPS)
  configuration 3069
ETS
  configuration 3281
ETS commands
  application-priority advertise-local-config 3300
  application-priority enable (interface) 3301
  application-priority enable (switch) 3302
  bandwidth-percentage 3303
  data-center-bridging 3304
  dcbx enable 3305
  enhanced-transmission-selection 3308
  enhanced-transmission-selection accept-peer-config 3306
  enhanced-transmission-selection advertise-local-config 3307
  enhanced-transmission-selection enable 3309
  ethertype 3310
  max-traffic-class-group 3312
  show application-priority interface 3314
  tcp 3321
  traffic-class-group add 3322
evpn esi holdtime 3953
evpn irb1 3956
evpn irb-if-forwarding anycast-gateway-mac 3956
evpn multi-homing enable 3954, 4010
exclude-any command 4369
exec command mode 71
exit 444
exit-address-family 2398
exit-address-family command 2523
ext-tunnel-id command 4341, 4342

F

Fail Over Group 309
Fast Reroute commands
  bandwidth 4426
  class-type 4426
  detour-identification 4426
  exclude-address 4426
  ext-tunnel-id A.B.C.D 4426
  from 4427
  primary fast-reroute 4428
  primary fast-reroute bandwidth 4428
  primary fast-reroute exclude-any 4429
  primary fast-reroute hold-priority 4429
  primary fast-reroute hop-limit 4430
  primary fast-reroute node protection 4431
  primary fast-reroute protection 4432
  primary fast-reroute setup-priority 4433
fast-external-failover 2487
feature dhcp 565, 580
feature ntp 758
feature sflow 824
feature ssh 803
feature tacacs+ 932
feature telnet 949
fec 644
fib retain 2158
filter command 4369
flowcontrol off 645
fog tfc 990
fog type 991
forwarding table
  view entries 4179
from command
  IPv6 address 4427

G

GARP Multicast Registration Protocol 191
GMRP
  configuring 191
graceful restart 2799
graceful restart commands
  neighbor capability graceful-restart 2545
  restart bgp graceful 2600
graceful restart in IS-IS 1793
graceful-restart enable 4348
group-to-RP mappings 2894

H

hardware-profile portmode 647, 911
hardware-profile portmode bundle 647
hello-interval 4390
hello-interval command 4348

hello-receipt 4349
hello-timeout command 4350
Hierarchical Queuing Configuration 3635, 3679, 3681, 3689
High Level Architecture 80
history 2685, 2687
hold-priority command 4404
Hop Count 4076
Host Address 4075
host area 2280
how to disable VRRP session 3389
how to enable
  authentication on an area 1630
  authentication on an interface 1630
  IS-IS 1751
  multiple OSPF instances 1634
  multiple OSPFv3 instances 1705
  OSPF on an interface 1605
  OSPFv3 1673
  RIP 1575
how to enable VRRP session 3390
how to enable/disable Virtual MAC 3409
how to redistribute routes 1684
how to redistribute routes into OSPF 1618
how to set priority in OSPF 1609
how to set priority in OSPFv3 1676
how to set priority-IS-IS 1754
how to set the Virtual IP address 3407
how to specify RIP version 1580

I

IEEE 802.1x 1081
if-arbiter 648
IFNAME 66
IGMP Commands
  clear ip igmp 2938
  debug igmp 2939, 2973
  ip igmp 2941
  ip igmp access-group 2942
  ip igmp immediate-leave 2943
  ip igmp last-member-query-count 2945
  ip igmp last-member-query-interval 2946
  ip igmp limit 2947
  ip igmp mroute-proxy 2948
  ip igmp proxy-service 2950
  ip igmp querier-timeout 2952
  ip igmp query-interval 2953
  ip igmp query-max-response-time 2954
  ip igmp robustness-variable 2956
  ip igmp snooping 2974
  ip igmp snooping fast-leave 2975
  ip igmp snooping mrouter 2976
  ip igmp snooping querier 2977
  ip igmp snooping report-suppression 2978
  ip igmp ssm-map enable 2957
  ip igmp ssm-map static 2958
  ip igmp static-group 2959
  ip igmp version 2962
  show ip igmp groups 2964
  show ip igmp interface 2966
  show ip igmp snooping mrouter 2980
  show ip igmp snooping statistics 2986
IGMP snooping
  configuration 2905
ignore-lsp-errors 2740
IGP areas 4087
import map 2625
interface 649
Interface Commands 623
interface display 4492
Interface irb 3957
interface mode 71
interface po 1398
interface sa 1399
Interior Gateway Protocol (IGP) 2135
Intermediate System to Intermediate System 88
Intermediate System to Intermediate System (IS-IS) 2131
intra-domain-link 1432
ip address 650
ip address dhcp 581, 651
ip bfd static all-interfaces 3528
ip dhcp client request 582
ip dhcp relay 594, 595
ip dhcp relay address 596
ip dhcp relay information option 597
ip domain-list 615
ip domain-lookup 616
ip domain-name 617
ip extcommunity-list
  expanded 2532
  extended 2531
  standard 2533
ip extcommunity-list standard 2530
ip forwarding 652
ip host 618
ip igmp 2941
ip igmp access-group 2942
ip igmp immediate-leave 2943
ip igmp last-member-query-count 2945
ip igmp last-member-query-interval 2946
ip igmp limit 2947
ip igmp mroute-proxy 2948
ip igmp proxy-service 2950
ip igmp querier-timeout 2952
ip igmp query-interval 2953
ip igmp query-max-response-time 2954
ip igmp robustness-variable 2956
ip igmp snooping 2974
ip igmp snooping fast-leave 2975
ip igmp snooping mrouter 2976
ip igmp snooping querier 2977
ip igmp snooping report-suppression 2978
ip igmp ssm-map enable 2957
ip igmp ssm-map static 2958
ip igmp static-group 2959
ip igmp version 2962

 © 2021 IP Infusion Inc. Proprietary

ip mroute 2924
ip multicast route-limit command 2925
ip multicast ttl-threshold 2926
ip multicast-routing 2927
ip name-server 619
ip ospf authentication 2281
ip ospf authentication-key 2282
ip ospf bfd 2284
ip ospf cost 2285
ip ospf database-filter 2286
ip ospf dead-interval 2287
ip ospf disable all 2288, 2290
ip ospf hello-interval 2291
ip ospf message-digest-key 2293
ip ospf mtu 2295
ip ospf mtu-ignore 2296
ip ospf network 2297
ip ospf priority 2298
ip ospf retransmit-interval 2299
ip ospf transmit-delay 2300
ip pim accept-register list 3003
ip pim anycast-rp 3004
ip pim bsr-border 3005
ip pim bsr-candidate 3006
ip pim cisco-register-checksum 3007
ip pim dr-priority 3008
ip pim exclude-genid 3009
ip pim hello-holdtime 3010
ip pim hello-interval 3011
ip pim ignore-rp-set-priority 3012
ip pim jp-timer 3013
ip pim neighbor-filter 3014
ip pim register-candidate 3024
ip pim register-rate limit 3017
ip pim register-rp-reachability 3018
ip pim register-source 3019
ip pim rp-address 3022
ip pim spt-threshold 3026
ip pim ssm 3027
ip pim unicast-bsm 3029
ip prefix-list 653
ip proxy-arp 655
ip radius source-interface 1511
ip remote-address 656
ip route 2159
ip router isis 2741
ip static bfd 3530
ip static fall-over bfd 3529
ip unnumbered 657
ip vrf 658, 2163, 2626
ip vrf forwarding 658
IPv4 address
  command syntax 66
ipv6 access-list filter 371
IPv6 address
  command syntax 66
ipv6 address 659
ipv6 bfd static all-interfaces 3531
ipv6 dhcp relay 600, 601, 604
ipv6 dhcp relay address 602
ipv6 dhcp relay subscriber-id 603
ipv6 forwarding 660
ipv6 mroute 2928
ipv6 nd current-hoplimit 2840
ipv6 nd link-mtu 2841
ipv6 nd managed-config-flag 2842
ipv6 nd other-config-flag 2843
ipv6 nd prefix 2844
ipv6 nd ra-interval 2846
ipv6 nd reachable-time 2848
ipv6 nd retransmission-time 2849
ipv6 nd suppress-ra 2850
ipv6 ospf cost 2398
ipv6 ospf dead-interval 2399
ipv6 ospf display route single-line 2400
ipv6 ospf link-lsa-suppression 2402
ipv6 ospf mtu-ignore 2403
ipv6 ospf neighbor 2404
ipv6 ospf network 2406
ipv6 ospf priority 2407
ipv6 ospf restart grace-period 2408
ipv6 ospf restart helper 2409
ipv6 ospf retransmit-interval 2411
ipv6 ospf6 transmit-delay 2412
ipv6 prefix-list 661
ipv6 router ospf 2413
ipv6 static bfd 3533
ipv6 static fall-over bfd 3532
ipv6 te-metric 2415
ipv6 unnumbered 663
isis authentication key-chain 2743
isis authentication mode md5 2744
isis authentication send-only 2745
isis circuit-type 2747
IS-IS commands 2728
  accept-lifetime 2712
  area-password 2716
  authentication key-chain 2717
  authentication mode md5 2718
  authentication send-only 2719
  clear clns is-neighbors 2723
  clear clns neighbors 2722
  clear isis interface counter 2727
  clear isis route 2724
  default-information originate 2731
  distance (IPv4) 2733
  isis authentication key-chain 2743
  isis authentication mode md5 2744
  isis authentication send-only 2745
  isis csnp-interval 2748
  isis hello-interval 2750
  isis hello-multiplier 2751
  isis metric 2755
  isis network 2756
  isis password 2757
  isis priority 2758
  isis restart grace-period 2795
  isis restart helper 2797

© 2021 IP Infusion Inc. Proprietary

isis restart-hello-interval 2796
isis retransmit-interval 2759
key 2767
key chain 2766
key-string 2767, 2768
max-area-address 2773
metric-style 2775
redistribute 2782
redistribute isis 2784
restart isis graceful 2799
send-lifetime 2787, 2789
set-overload-bit 2789
show clns is-neighbors 2802
show clns neighbors 2804
show cspf lsp 2807
show debugging isis 2807
show ip protocols 2813
show isis counter 2817
show isis counter command 2817
show isis database 2818
show isis interface 2821
show isis topology 2825
show running-config interface isis 2827
show running-config router isis 2828
summary-address 2791
ISIS Configuration 2131
IS-IS configuration 1751
configuring distance 1793
configuring metric 1764
configuring overload bit 1799
configuring passive interface 1799
enabling IS-IS on an interface 1751
graceful restart 1793
L1 L2 area routing with multiple instances 1777
L1 L2 area routing with single instance 1771
redistributing routes into IS-IS 1758
route leaking 1783
route summarization 1788
setting priority 1754
IS-IS configuration-IPv6 1804
isis csnp-interval 2748
isis csnp-interval command 2748
isis hello-interval 2750
isis hello-interval command 2750
isis hello-multiplier 2751
isis hello-multiplier command 2751
isis metric 2755
isis metric command 2755
isis network command 2756
isis password 2757
isis password command 2757
isis priority 2758
isis priority command 2758
isis restart grace-period 2795
isis restart helper 2797
isis restart-hello-interval 2796
isis retransmit-interval 2759
isis retransmit-interval command 2759
is-type 2765

K

keep multiplier 4393
key chain 2766, 3499
key command 2767
key 3498
key-string 2767, 2768

L

L1L2 area routing 1771, 1777
L2 circuit
view circuit parameters 4188
Label Distribution Modes 4076
Label Distribution Protocol Overview 4075
Label Generation 4075
Label Retention Mode 4076
Label Space 4063
LACP
configuring 1107
LACP Commands
debug lacp 1397
lacp port-priority 1402
lacp system-priority 1403
lacp timeout 1404
show debugging lacp 1410
show lacp-counter 1415
show port etherchannel 1416
static-channel-group 1422
LACP commands
port-channel load-balance 1405
lacp destination-mac 1400
lacp port-priority command 1402
lacp system-priority command 1403
lacp timeout command 1404
LAN segments 3787
Layer 2 Multicast Routing Information Base Daemon 89
Layer 2 VPNs 4087
Layer 3 Multicast Routing Information Base Daemon 90
LDP 4075
LDP Commands
show debugging ldp 4290
show ldp 4291
show ldp adjacency 4293
show ldp advertise-labels 4294
show ldp downstream 4295
show ldp fec 4297
show ldp interface 4299
show ldp lsp 4302
show ldp routes 4307
show ldp session 4308
show mpls ldp discovery 4316
show mpls ldp graceful-restart 4317
show mpls ldp neighbor 4317
show mpls ldp parameter 4318
LDP Inter-Area 4087
LDP inter-area 4087
LDP Session 4075
LDP VPLS Commands

© 2021 IP Infusion Inc. Proprietary

show ldp vpls 4315
Liberal Retention Mode 4076
LINE 66
Link aggregation 1165
Linkdown Policy 195
link-type 992
LLDP commands
lldp system-name 1537, 3250, 3271
set lldp disable 1531, 3241, 3265
set lldp enable 1532, 3241, 3266
set lldp locally-assigned 1533, 3244, 3267
set lldp msg-tx-hold 1535, 3245, 3269
set lldp msg-tx-interval 3247, 3250
set lldp too-many-neighbors 1539, 3251, 3273
show lldp port 1540, 3252, 3274
lldp system-name 1537, 3250, 3271
load-balance 915
load-balance rtag7 915
load-balance rtag7 vxlan inner-l2 3958
load-balance rtag7 vxlan inner-l3 3959
locator led 495
log syslog 888
Logging Console Configuration 275
logging level 890
logging logfile 892
logging source-interface 897
logging timestamp 897
log-neighbor-changes command 2493
logout 452
Loop Detection 4076
loose type 4326, 4423
LSP Control 4076
lsp-gen-interval 2770
lsp-refresh-interval 2772

M

mac 3960, 4132
MAC address
command syntax 66
MAC addresses 3787
mac vrf 3961
mac-holdtime 3962
make-before-break 4422
map vnid 3963
map-route command 4353
Marking/Remarking Configuration 3573
Match and Set Commands
match as-path 2183
match community 2184
match interface 2186
match ip address 2187
match ip address prefix-list 2188
match ip next-hop 2189
match ip next-hop prefix-list 2190
match ipv6 address 2192
match ipv6 address prefix-list 2193
match ipv6 next-hop 2194
match metric 2197
match origin 2198
match route-type 2199
match tag 2200
set as-path 2203
set atomic-aggregate 2204
set comm-list delete 2205
set community 2206
set dampening 2208
set extcommunity 2209
set ip next-hop 2212
set ipv6 next-hop 2213
set level 2214
set metric 2216
set metric-type 2217
set origin 2218
set originator-id 2219
set tag 2220
set vpnv4 next-hop 2221
set weight 2222
match as-path 2183
match command
origin 2198
match community 2184
match cos 3726
match dscp 3723
match interface 2186
match ip address 2187
match ip address prefix-list 2188
match ip next-hop 2189
match ip next-hop prefix-list 2190
match ip rtp 3723
match ipv6 address 2192
match ipv6 address prefix-list 2193
match ipv6 next-hop 2194
match mac 3721
match metric 2197
match origin 2198
match protocol 3723
match route-type 2199
match tag 2200
match vlan 3726
max-area-address 2773
max-concurrent-dd 2302, 2417
maximum-area 2303
maximum-paths 2164
max-lsp-lifetime 2774
Maxpoll and Minpoll Configuration 219
max-static-routes 2165
mcec domain configuration 1434
MC-LAG 1165
MC-LAG Configuration 1165
MED 2466
message-ack command 4436, 4437
metric in IS-IS 1764
metrics 87
metric-style command 2775
mlag 1435
Monitor Port Group 309, 989, 990, 991
Monitor Port Groups 990

MPLS
record 4385
mpls ac-group 4132
mpls admin-groups 4133
MPLS Commands
ftn-entry 4140
ilm-entry 4140, 4141, 4143
ingress-ttl 4144
local-packet-handling 4149
max-label-value 4155, 4161
min-label-value 4155, 4161
mpls admin-groups 4133
mpls bandwidth-class 4134
mpls disable-all-interfaces 4135
mpls enable-all-interfaces 4136
mpls ftn-entry 4140
mpls ilm-entry pop 4140
mpls ilm-entry swap 4141
mpls ilm-entry vpnpop 4143
mpls ingress-ttl 4144
mpls l2-circuit 4145
mpls l2-circuit GROUPNAME 4146
mpls l2-circuit-fib-entry 4148
mpls local-packet-handling 4149
mpls lsp-model 4152
mpls min-label-value 4155, 4161
mpls traffic-eng 4157
mpls-l2-circuit 4146
show mpls admin-groups 4169
show mpls bandwidth-class 4170
show mpls cross-connect-table 4177
show mpls forwarding-table 4179
show mpls ftn-table 4182
show mpls ilm-table 4184
show mpls index-manager 4186
show mpls in-segment-table 4186
show mpls l2-circuit 4188, 4190
show mpls ldp 4190
show mpls mapped-routes 4192
show mpls ms-pw 4193
show mpls out-segment-table 4193
show mpls qos-resource 4195
show mpls vc-table 4197
show mpls vrf 4198
show running-config interface mpls 4200
show running-config mpls 4201
show vccv statistics 4206
trace mpls 4165, 4208
MPLS commands
ilm-entry 4140, 4141, 4143
mpls enable-all-interfaces 4136
mpls ftn-entry 4140
mpls ilm-entry 4140, 4141, 4143
mpls ingress-ttl 4144
mpls l2-circuit-fib-entry 4148
mpls local-packet-handling 4149
MPLS LSPs 4107
mpls lsp-stitching 4153
mpls map-route 4154
mpls max-label-value 4155, 4161
mpls min-label-value 4155, 4161
mpls propagate-ttl 4156
mpls traffic-eng 4157
MPLS-TTL-Processing 4071
MRIB 2885
MSDP 2909
MSTP
configuring 1193
Multi Exit Discriminator 2466
multicast 672
Multicast Commands
clear ip mroute 2922
debug ip mrib
debug ip mrib 2923
ip mroute 2924
ip multicast route-limit 2925
ip multicast ttl-threshold 2926
ip multicast-routing 2927
multicast 672
show ip mroute 2930
show ip mvif 2933
show ip rpf 699
show ipv6 rpf 2170
multicast routing 2927
multicast routing table, displaying 3037
Multiple Spanning Tree Protocol 84

N

nd-cache disable 3983
neighbor 2304
passive 2567
peer-group add 2568
remove-private-AS 2577
unsuppress-map 2589
neighbor allow-egbp-vpn 2627
neighbor as-override 2628
neighbor attribute-unchanged 2542
neighbor command 4355
advertisement-interval 2538
capability dynamic 2544
capability graceful-restart 2545
capability orf prefix-list 2546
enforce-multihop 2556
neighbor disallow-infinite-holdtime 2552
neighbor display 4494
neighbor g-shut 2559
neighbor g-shut-timer 2560
neighbor send-community 2629
neighbor soo 2630
neighboring IGP areas 4087
net 2779
network area 2305
network command 2595
nexthop 2901
nexthop-cache display 4497
no nvo vxlan 3965
no-record command 4360, 4376, 4379, 4410

© 2021 IP Infusion Inc. Proprietary

Trunk mode 4410, 4413
no-refreshing-resv-parsing 4361
NSM Commands
arp A.B.C.D MAC 441
clear ipv6 neighbors 636
if-arbiter 648
interface 649
ip address 650
ip address dhcp 651
ip forwarding 652
ip proxy-arp 655
ipv6 address 659
ipv6 forwarding 660
ipv6 nd managed-config-flag 2842
ipv6 nd other-config-flag 2843
ipv6 nd prefix 2844
ipv6 nd ra-interval 2846
ipv6 nd ra-lifetime 2847
ipv6 nd reachable-time 2848
ipv6 nd suppress-ra 2850
multicast 672
show debugging nsm 468
show ip forwarding 701
show ip interface brief 702
show ipv6 forwarding 717
show ipv6 interface brief 718
show ipv6 route 720
show nsm client 471
show router-id 1271, 2172
ntp access-group 760
ntp authenticate 760
NTP Authentication 219
ntp authentication-key 761
NTP Configuration 218
ntp enable 763
ntp logging 764
ntp master 767
ntp peer 767
ntp server 769
ntp trusted-key 773
nvo vxlan 3966
nvo vxlan access-if 3967
nvo vxlan id 3969
nvo vxlan irb 3971
nvo vxlan mac-ageing-time 3993
nvo vxlan max-cache-disable 3970
nvo vxlan tunnel qos-map-mode 3971
nvo vxlan vtep-ip-global 3971

O

Open Shortest Path First 87
Open Shortest Path First (OSPF) 2123
origin codes 2685, 2688
ospf abr-type 2307
OSPF commands
area authentication 2230
area default-cost 2231
area filter-list 2236
area nssa 2365
area range 2239
area stub 2241
area virtual-link 2242
auto-cost reference-bandwidth 2245
bfd all-interfaces 2246
capability opaque 2249
capability restart 2250
clear ip ospf process 2253
compatible rfc1583 2254
debug ospf 2255
debug ospf database-timer rate-limit 2257
debug ospf events 2258
debug ospf ifsm 2259
debug ospf ism 2259
debug ospf lsa 2264
debug ospf nfsm 2265
debug ospf nsm 2266
debug ospf packet 2267
debug ospf route 2269
default-information originate 2270, 2387
default-metric 2272, 2389
distance 2273, 2390
distribute-list 2274
enable db-summary-opt 2276
host area 2280
ip ospf authentication 2281
ip ospf authentication-key 2282
ip ospf bfd 2284
ip ospf cost 2285
ip ospf database-filter 2286
ip ospf dead-interval 2287
ip ospf disable all 2288, 2290
ip ospf hello-interval 2291
ip ospf message-digest-key 2293
ip ospf mtu 2295
ip ospf mtu-ignore 2296
ip ospf network 2297
ip ospf priority 2298
ip ospf transmit-delay 2300
ipv6 ospf mtu-ignore 2403
max-concurrent-dd 2302
maximum-area 2303
neighbor 2304
network area 2305
ospf abr-type 2307
ospf router-id 2312
overflow database 2313
overflow database external 2314
passive-interface 2315, 2418
redistribute 2316
restart helper 2311
restart ospf graceful 2318
router ospf 2319
show debugging ospf 2321
show ip ospf 2322
show ip ospf brder-routers 2326
show ip ospf igp-shortcut-lsp 2336
show ip ospf igp-shortcut-route 2337

© 2021 IP Infusion Inc. Proprietary

show ip ospf interface 2338
show ip ospf neighbor 2343
show ip ospf route 2347
show ip ospf virtual-links 2350
show ip protocols ospf 2352
summary-address 2357
timers lsa arrival 2358
timers throttle lsa 2360
OSPF Configuration 2123
OSPF configuration 1605
Area Border Router 1614
configuring multiple OSPF instances on same subnet 1644
configuring OSPF as PE-CE protocol for VPNs 1984
configuring virtual links 1625
enable multiple OSPF instances 1634
enabling authentication 1630
enabling OSPF on an interface 1605
OSPF cost 1620
redistributing routes into OSPF 1618
setting priority 1609
ospf router-id 2312
OSPF VPN Commands
router ospf vrf 2451
OSPFv3 commands
abr-type 2363
area default-cost 2364
area nssa 2365
area range 2367
area stub 2368
area virtual-link 2369
auto-cost reference bandwidth 2371
capability restart graceful 2373
clear ipv6 ospf process 2374
debug ipv6 ospf 2375
debug ipv6 ospf ifsm 2378
debug ipv6 ospf lsa 2379, 2380
debug ipv6 ospf nfsm 2381
debug ipv6 ospf nsm 2382
debug ipv6 ospf packet 2383
debug ipv6 ospf route 2386
default-metric 2389
distribute-list 2391
enable db-summary-opt 2393
exit-address-family 2398
ipv6 ospf cost 2398
ipv6 ospf dead-interval 2399
ipv6 ospf display route single-line 2400
ipv6 ospf link-lsa-suppression 2402
ipv6 ospf neighbor 2404
ipv6 ospf network 2406
ipv6 ospf priority 2407
ipv6 ospf restart grace-period 2408
ipv6 ospf restart helper 2409
ipv6 ospf retransmit-interval 2411
ipv6 ospf transmit-delay 2412
ipv6 ospf6 transmit-delay 2412
ipv6 router ospf 2413
ipv6 te-metric 2415
max-concurrent-dd 2417
passive-interface 2418
redistribute 2419
restart ipv6 ospf graceful 2421
router ipv6 ospf 2423
router-id 2422
show debugging ipv6 ospf 2424
show ipv6 ospf database 2426
show ipv6 ospf interface 2430
show ipv6 ospf neighbor 2432
show ipv6 ospf route 2435
show ipv6 ospf topology 2438
show ipv6 ospf virtual-links 2440
show ipv6 ospf6 interface 2430
show ipv6 vrf 2442
summary-address 2445
OSPFv3 configuration 1673
configuring Area Border Router 1680
cost 1689
enable multiple OSPFv3 instances 1705
enable OSPFv3 on an interface 1673
OSPFv3 graceful restart 1719
redistribute routes into OSPFv3 1684
setting priority 1676
virtual links 1699
overflow database 2313
overflow database external 2314
override-diffserv 4217, 4446

P

parantheses
command syntax 65
parentheses
command syntax 65
passive interface in IS-IS 1799
passive-interface 2315, 2418
path display 4498
path message 4385
Path Vector 4076
Peer 217
Per-interface label space 4063
period
command syntax 66
Per-platform label space 4063
PFC commands
priority-flow-control accept-peer-config 3338
priority-flow-control link-delay-allowance 3343
priority-flow-control mode 3344
show priority-flow-control details 3345
PFC priority-flow-control advertise-local-config 3339
PIM-DM configuration 2877, 2901
downstream 2901
forwarding multicast packets 2901
nexthop 2901
Reverse Path Forwarding 2901
upstream 2901
PIM-SM commands
clear ip mroute 2989

© 2021 IP Infusion Inc. Proprietary

debug ip pim timer joinprune 2999, 3001
debug pim packet 2993
debug pim sparse-mode timer register 3001
ip pim accept-register list 3003
ip pim anycast-rp 3004
ip pim bsr-border 3005
ip pim bsr-candidate 3006
ip pim cisco-register-checksum 3007
ip pim dr-priority 3008
ip pim exclude-genid 3009
ip pim hello-holdtime 3010
ip pim hello-interval 3011
ip pim ignore-rp-set-priority 3012
ip pim jp-timer 3013
ip pim neighbor-filter 3014
ip pim register-rate limit 3017
ip pim register-rp-reachability 3018
ip pim register-source 3019
ip pim rp-address 3022
ip pim rp-candidate 3024
ip pim ssm 3027
ip pim unicast-bsm 3029
show debugging pim 3030
show ip pim bsr-router 3034
show ip pim rp-hash 3043
undebug all pim sparse-mode 3046
PIM-SM configuration 2885
bootstrap router 2886
configuring RP dynamically 2892
configuring RP statically 2889
data flow from source to receivers 2886
determining the RP 2886
downstream 2886
electing a designated router 2886
forwarding multicast packets 2887
group-to-RP mappings 2894
joining the shared tree 2887
Multicast Routing Information Base 2885
pruning the interface 2887
references 2885
registering with the RP 2887
rendezvous point 2885
reverse path forwarding 2885
sending out Hello messages 2886
sending Register-Stop messages 2887
shared trees 2886
source-based trees 2886
tree information base 2885
upstream 2885
PIMv4 Commands 2987
ping 454
ping mpls 4159
policer
attributes 3540
types
aggregate 3540
individual 3540
policing 3540
Policing Configuration 3587
policy traffic-type 3741
policy-map 3731
Port 221
port 1407, 1409
Port Breakout Configuration 221
port bundle enable 672
Port Mapping 3789
portal-system-number 1439
portal-topology 1439
port-channel load-balance 1405
port-channel min-links 1407, 1409
port-conv-id 1439
preempt-mode 3393
Prefix 4075
prefix-list 653
primary fast-reroute bandwidth 4428
primary fast-reroute exclude-any command 4429
primary fast-reroute policer 4433
primary fast-reroute protection 4432
priority 3733
Priority Configuration 3611
priority-delta 3368
Private-VLAN commands
switchport private-vlan host-association 1474
switchport private-vlan mapping 1475
privilege 458
privileged exec mode 71
Provider Bridging commands
bridge protocol provider-rstp 3199
cvlan registration table 3200
switchport customer-edge 3204
switchport customer-edge default-svlan 3205
switchport customer-edge hybrid allowed vlan 3206
switchport customer-edge vlan registration 3208
switchport customer-network vlan translation 3210
switchport mode 3214
switchport mode customer-edge access 3215
switchport mode customer-edge hybrid 3216
switchport mode ingress-filter 3214
switchport provider-edge vlan 3217
switchport provider-network vlan translation 3218
vlan type 3220
Provider Edge 4087
Provider-based MPLS 4087

Q

QoS
functionality 3539
terminology 3539
qos statistics 3741
QoS Statistics Configuration 3543
question mark
command syntax 66
queue-limit 3742

R

RADIUS Server Accounting 251

RADIUS Server Authentication 241
radius-server deadtime 788, 1512
radius-server directed-request 788
radius-server host 788, 1513
radius-server host acct-port 789
radius-server host auth-port 790
radius-server host key 793
radius-server key 793, 1515
radius-server retransmit 794, 1516
radius-server timeout 794, 1517
Rapid Spanning Tree Protocol 83
rd (route distinguisher) 2631
redistribute 2419, 2782
redistribute command 2316
redistribute isis 2784
redistribute routes 1618
redistribute routes in OSPFv3 1684
redistributing routes into IS-IS 1758
redistributing routes into OSPF 1618
redundancy using VRRP and OSPF 3378
references
  PIM-SM 2885
Refresh Reduction Commands
  ack-wait-timeout 4436
  message-ack 4437
  refresh-reduction 4438
  rsvp ack-wait-timeout 4439
  rsvp refresh-reduction 4441
refresh-reduction command 4438
refresh-resv-parsing 4361
refresh-time 4394
refresh-time command 4385
reload 460
removing Multi-Exit Disc attribute from update messages 1942
Rendezvous Point 2885
rendezvous point
  candidate status 3024
  mappings 3044
reservation lifetime 4393
reservation request messages 4385
reset log file 1006
restart bgp graceful 2600
restart helper 2311
restart ipv6 ospf graceful 2421
restart isis 2799
restart isis graceful 2799
restart ospf graceful 2318
restart-time 2578
Reverse Path Forwarding 2885, 2901
rfc1771-path-select 2497
rfc1771-strict 2498
RIP configuration
  enabling RIP 1575
  RIPv2 md5 authentication 1595
  RIPv2 text authentication-multiple keys 1588
  specifying the RIP version 1580
RIP version 1580
RIPng configuration 1603
root of the tree 2885
route leaking in IS-IS 1783
route summarization in IS-IS 1788
route-map 2201
Router Advertised Commands
  iipv6 nd current-hoplimit 2840
  iipv6 nd link-mtu 2841
  ipv6 nd managed-config-flag 2842
  ipv6 nd other-config-flag 2843
  ipv6 nd prefix 2844
  ipv6 nd ra-interval 2846
  ipv6 nd ra-lifetime ipv6 nd ra-lifetime 2847
  ipv6 nd reachable-time 2848
  ipv6 nd retransmission time 2849
  ipv6 nd suppress-ra 2850
router ipv6 ospf 2423
router isis 2786
router mode 71
router ospf 2319
router ospf vrf 2451
router vrrp 3395
route-reflector 1866
router-id 2422
route-target 2632
Routing Information Base Daemon 85
Routing Information Protocol 88
Routing Information Protocol (RIP) 2125
RP 2885
RPF 2885, 2901, 2909
RPVST+ commands
  bridge protocol rpvst+ 1383
  bridge-group vlan 1382
  spanning-tree rpvst+ configuration 1389
  spanning-tree vlan path-cost 1390
  spanning-tree vlan restricted-role 1390
  spanning-tree vlan restricted-tcn 1391
rsvp ack-wait-timeout command 4390, 4439
RSVP Commands
  A.B.C.D (loose|strict) 4326
  clear rsvp session 4327
  clear rsvp trunk 4328
  debug rsvp 4330
  disable-igp-shortcut 4337
  disable-rsvp 4337
  exclude-any 4369
  explicit-null 4340
  ext-tunnel-id 4341, 4342
  filter 4369
  from
    IPv6 address 4427
  graceful-restart enable 4348
  hello-interval 4348
  hello-timeout 4350
  hold-priority 4404
  map-route 4353
  message-ack 4436
  neighbor A.B.C.D 4355
  no-record 4360, 4376, 4379, 4410
    Trunk mode 4410, 4413

 © 2021 IP Infusion Inc. Proprietary

no-refresh-resv-parsing 4361
refresh-time 4385
rsvp ack-wait-timeout 4390, 4439
rsvp hello-interval 4390
rsvp keep-multiplier 4393
rsvp message-ack 4394, 4440
rsvp refresh-time 4394
rsvp-path 4395
rsvp-trunk-restart 4397
show debugging rsvp 4420
show rsvp 4487
show rsvp interface 4492
show rsvp neighbor 4494
show rsvp nexthop-cache 4497
show rsvp path 4498
show rsvp session 4500, 4502
show rsvp session egress 4503
show rsvp session ingress 4507
show rsvp session LSP-NAME 4511
show rsvp session transit 4514
show rsvp version 4520
update-type 4422
rsvp data display 4487
RSVP DiffServ Commands
map-route 4217, 4445
override-diffserv 4217, 4446
primary class-to-exp-bit 4447
primary elsp-preconfigured 4219, 4448
primary elsp-signaled 4219, 4448
primary llsp 4220, 4449
secondary class-to-exp-bit 4221, 4450
secondary elsp-signaled 4222, 4451
secondary lls 4223, 4452
show rsvp diffserv-info 4224, 4453
RSVP DiffServ-TE Commands
primary class-type 4456
rsvp hello-interval command 4390
rsvp message-ack command 4394, 4440
rsvp refresh-reduction command 4441
rsvp refresh-time command 4394
RSVP Show Commands
show rsvp 4483
show rsvp admin-groups 4486
show rsvp control-adjacency 4487
show rsvp data-link 4489
show rsvp diffserv-info 4491
show rsvp dste-info 4491
show rsvp graceful-restart 4492
show rsvp interface 4492
show rsvp neighbor 4494
show rsvp nexthop-cache 4497
show rsvp path 4498
show rsvp session 4500
show rsvp session egress 4503
show rsvp session ingress 4507
show rsvp session LSP-NAME 4511
show rsvp session transit 4514
show rsvp summary-refresh 4517
show rsvp trunk 4518
show rsvp version 4520
sshow rsvp session count 4502
rsvp-path command 4395
RSVP-TE Commands
A.B.C.D 4326
clear rsvp session 4327
clear rsvp trunk 4328
cspf 4329
debug rsvp all 4330
debug rsvp cspf 4331
debug rsvp events 4332
debug rsvp fsm 4333
debug rsvp hexdump 4334
debug rsvp nsm 4335
debug rsvp packet 4336
disable-igp-shortcut 4337
disable-rsvp 4337
enable-rsvp 4339
ext-tunnel-id 4342
ext-tunnel-id A.B.C.D 4341
from 4344
from A.B.C.D 4343
graceful-restart 4348
hello-interval 4348
hello-receipt 4349
hello-timeout 4350
keep-multiplier 4351
loop-detection 4352
map-route 4354
map-route A.B.C.D 4353
neighbor 4356
neighbor A.B.C.D 4355
no-cspf 4357
no-loop-detection 4358
no-php 4359
no-record 4360
no-refresh-path-parsing 4360
no-refresh-resv-parsing 4361
php 4362
primary ADMIN-GROUP-NAME 4363
primary affinity 4364
primary bandwidth 4365
primary cspf 4366
primary cspf-retry-limit 4367
primary cspf-retry-timer 4368
primary filter 4369
primary hold-priority 4370
primary hop-limit 4371
primary label-record 4372
primary local-protection 4373
primary no-affinity 4374
primary no-cspf 4375
primary no-record 4376
primary path 4377
primary record 4379
primary retry-limit 4380
primary retry-timer 4381
primary reuse-route-record 4382
primary setup-priority 4383

primary traffic 4384
refresh-path-parsing 4386
refresh-resv-parsing 4387
refresh-time 4385
router rsvp 4389
rsvp hello-interval 4390
rsvp hello-receipt 4391
rsvp hello-timeout 4392
rsvp keep-multiplier 4393
rsvp refresh-time 4394
rsvp-path 4395
rsvp-trunk 4396
rsvp-trunk-restart 4397
secondary ADMIN-GROUP-NAME 4398, 4406
secondary bandwidth 4399
secondary cspf 4400
secondary cspf-retry-limit 4401
secondary cspf-retry-timer 4402
secondary filter 4403
secondary hold-priority 4404
secondary hop-limit 4405
secondary label-record 4406
secondary local-protection 4407
secondary no-affinity 4408
secondary no-cspf 4409
secondary no-record 4410
secondary path 4411
secondary record 4413
secondary retry-limit 4414
secondary retry-timer 4415
secondary reuse-route-record 4416
secondary setup-priority 4417
secondary traffic 4418
to 4421
to A.B.C.D 4420
update-type 4422
X:X::X:X 4423
RSVP-TE P2MP LSP Commands
affinity 4460
bandwidth 4461
class-type 4462
clear rsvp p2mp-session 4463
destination 4464
exit-p2mp-lsp 4465
ext-tunnel-id 4466
filter 4467
from 4468
hold-priority 4469
hop-limit 4470
label-record 4471
pack-affinity 4472
primary-lsp 4473
retry-limit 4474
retry-timer 4475
RSVP-TE Refresh Reduction Commands
ack-wait-timeout 4436
message-ack 4437
refresh-reduction 4438
rsvp ack-wait-timeout 4439
rsvp message-ack 4440
rsvp refresh-reduction 4441
rsvp-trunk-restart command 4397

S

scan-time 2500
scheduling
SP 3541
WRR 3541
WRR with SP 3541
send-lifetime 2787, 2789
send-lifetime 3502
Server 217
server 420
service advanced-vty 461
service password-encryption 462
service terminal-length 463
service-policy 3745
service-policy type qos 3746
session display 4500, 4502
set as-path 2203
set atomic-aggregate 2204
set bridge cos 3748
set comm-list delete 2205
set community 2206
set dampening 2208
set extcommunity 2209
set interface null0 2211
set ip next-hop 2212
set ipv6 next-hop 2213
set level 2214
set lldp disable 3241
set lldp enable 1532, 3241, 3266
set lldp locally-assigned 1533, 3244, 3267
set lldp msg-tx-hold 1535, 3245, 3269
set lldp msg-tx-interval 3247, 3250
set lldp too-many-neighbors 1539, 3251, 3273
set metric 2216
set metric-type 2217
set origin 2218
set originator-id 2219
set precedence 3755
set tag 2220
set vpnv4 next-hop 2221
set weight 2222
set-overload-bit 2789
setting priority 1676
setting-priority 1754
sFlow 824
sflow collector 826
Shaping Configuration 3603
shared trees 2886
show 3032
rsvp 4487
show aaa accounting 421
show aaa authentication 421
show aaa authentication login 422
show access-list 465

© 2021 IP Infusion Inc. Proprietary

show access-lists 399
show bfd 3503
show bfd interface 3504
show bfd session 3506
show bfd session A.B.C.D 3510
show bfd session ipv6 3513
show bgp ipv6 2652
show bgp l2vpn evpn 3972
show bgp l2vpn evpn summary 3976
show bgp neighbors received prefix-filter 2664
show bgp neighbors received-routes 2665
show bgp neighbors routes 2666
show bgp paths command 2671
show bgp prefix-list command 2672
show bgp quote-regexp command 2673
show bgp route-map command 2675
show cli 465
show clns is-neighbors 2802
show clns is-neighbors command 2802
show clns neighbors command 2804
Show commands
  show mpls forwarding-table 4179
  show mpls ilm-table 4184
  show mpls l2-circuit 4188
  show mpls mapped-routes 4192
  show mpls vc-table 4197
show commands 68
  exclude modifier 69
  include modifier 69
  redirect modifier 70
show cspf lsp 2807
show debug radius 795
show debug ssh server 804
show debug tacacs+ 936
show debug telnet server 950
show debugging bfd 3516
show debugging dot1x 1518
show debugging ipv6 ospf 2424
show debugging isis 2807
show debugging lacp command 1410
show debugging ldp 4290
show debugging mstp 1350
show debugging nsm 468
show debugging ospf 2321
show debugging pim 3030
show debugging rib 2167
show debugging vrrp 3396
show dot1x 1519
show errdisable details 1271
show flowcontrol interface 673
show hardware-information 496
show hosts 620
show interface errdisable status 1272
show interface irb 4002
show interface switchport bridge 1300
show ip bgp rtfilter all 2692
show ip dhcp relay 605
show ip dhcp relay address interface 607
show ip extcommunity-list 2698
show ip forwarding 701
show ip igmp groups 2964
show ip igmp interface 2966
show ip igmp snooping mrouter 2980
show ip igmp snooping statistics 2986
show ip interface brief 702
show ip mroute 2930
show ip mvif 2933
show ip ospf 2322
  border routers 2326
show ip ospf border-routers 2326
show ip ospf igp-shortcut-lsp 2336
show ip ospf igp-shortcut-route 2337
show ip ospf interface 2338
show ip ospf neighbor 2343
show ip ospf route 2347
show ip ospf virtual-links 2350
show ip pim bsr-router 3034
show ip pim rp-hash 3043
show ip prefix-list 722
show ip protocols 2813
show ip protocols bgp 2699
show ip protocols ospf 2352
show ip vrf 716
show ipv6 dhcp relay 610
show ipv6 dhcp relay address 611
show ipv6 dhcp vendor-opts 589
show ipv6 forwarding 717
show ipv6 interface brief 718
show ipv6 isis route 2817
show ipv6 ospf database 2426
show ipv6 ospf database, router 2421
show ipv6 ospf interface 2430
show ipv6 ospf neighbor 2432
show ipv6 ospf route 2435
show ipv6 ospf topology 2438
show ipv6 ospf virtual-links 2440
show ipv6 ospf6
  interface 2430
show ipv6 route 720
show ipv6 rpf 2170
show ipv6 vrf 2442
show isis counter 2817
show isis database command 2818
show isis interface 2821
show isis topology 2825
show lacp-counter command 1415
show ldp 4291
  adjacency 4293
  downstream 4295
  fec 4297
  interface 4299
  session 4308
show ldp advertise-labels 4294
show ldp lsp 4302
show ldp routes 4307
show ldp vpls 4315
show list 469
show lldp interface 3256

show lldp port 1540, 3252, 3274
show logging 898
show logging last 900
show logging logfile 901
show logging logfile last-index 902
show logging logfile start-seqn end-seqn 903
show logging logfile start-time end-time 904
show mac address-table count bridge 1302
show mcec statistics 1437
show mlag conversation-id 1439
show mlag detail 1439
show mlag summary 1441
show mpls in-segment-table 4186
show mpls l2-circuit 4190
show mpls ldp
  discovery 4316
  neighbor 4317
  parameter 4318
show mpls ldp graceful-restart 4317
show nsm client 471
show ntp authentication-keys 774
show ntp authentication-status 775
show ntp client 776
show ntp logging-status 776
show ntp peers 779
show ntp peer-status 777
show ntp statistics 780
show ntp status 782
show ntp trusted-keys 782
show nvo vxlan 3978
show nvo vxlan arp-cache 3981
show nvo vxlan counters access-port 3983
show nvo vxlan counters network-port 3986
show nvo vxlan interface counters 3988
show nvo vxlan mac-table 3988
show nvo vxlan nd-cache 3991
show nvo vxlan static host state 3993
show nvo vxlan tunnel 3995
show policy-map 3764
show policy-map interface 3765
show port etherchannel command 1416
show priority-flow-control details 574
show process 474
show radius-server 796
show role name 1002
show router-id 1271, 2172
show rsvp down ingress sessions 4507
show rsvp down sessions 4500, 4502
show rsvp egress down sessions 4503
show rsvp egress up sessions 4503
show rsvp session egress command 4503
show rsvp session ingress 4507
show rsvp session LSP-NAME 4511
show rsvp session transit command 4514
show rsvp transit down sessions 4514
show rsvp transit up sessions 4514
show rsvp up ingress sessions 4507
show rsvp up sessions 4500, 4502
show running-config 475
show running-config aaa 425
show running-config as-path access-list 2702
show running-config community-list 2703
show running-config dhcp 612
show running-config dns 622
show running-config interface 725
show running-config interface igmp 2971
show running-config interface ip 727
show running-config interface ipv6 728
show running-config interface isis 2827
show running-config interface multicast 2935
show running-config ipv6 access-list 730
show running-config ntp 783
show running-config nvo vxlan 3996
show running-config prefix-list 731
show running-config radius 798
show running-config route-map 2224
show running-config router isis 2828
show running-config router vrrp 3397
show running-config router-id 2174
show running-config snmp 840
show running-config ssh server 805
show running-config switch 1273
show running-config syslog 905
show running-config tacacs+ 939
show running-config telnet server 951
show running-config vrf 2176
show sflow 830
show sflow interface 832
show snmp 841
show snmp community 842
show snmp engine-id 843
show snmp group 844
show snmp host 845
show snmp user 846
show snmp view 847
show spanning-tree 1351
show spanning-tree mst 1355
show spanning-tree statistics 1357
show ssh server 808
show startup-config 476
show system-information 510
show tacacs-server 940
show telnet server 952
show tfo 993
show transceivers details 576
show user-account 1002
show username 809
show users 480
show version 481
show vlan access-map 1455
show vlan all 1456
show vlan auto 1458
show vlan brief 1458
show vlan classifier 1459
show vlog all 1006
show vlog clients 1007
show vlog terminals 1008
show vlog virtual-routers 1009

© 2021 IP Infusion Inc. Proprietary

shutdown 3962, 4002, 4003
Simple Network Management Protocol 259
snmp restart bfd 3517
snmp restart mstp 1360
snmp-server community 848
snmp-server contact 849
snmp-server enable snmp 850
snmp-server enable traps 851
snmp-server group 852
snmp-server host 852
snmp-server location 854
snmp-server tcp-session 855
snmp-server user 856
snmp-server view 857
soft-reconfiguration 2585
source-based trees 2886
spanning-tree autoedge 1361
spanning-tree edgeport 1362
spanning-tree guard root 1363
spanning-tree hello-time 1364
spanning-tree instance restricted-role 1364
spanning-tree instance restricted-tcn 1365
spanning-tree link-type 1366
spanning-tree mst configuration 1367
spanning-tree restricted-role 1371
spanning-tree restricted-tcn 1372
spanning-tree spvts+ configuration 1389
spanning-tree te-msti configuration 1373
spanning-tree vlan path-cost 1390
spanning-tree vlan restricted-role 1390
spanning-tree vlan restricted-tcn 1391
specify DiffServ class name 4216, 4444
square brackets
  command syntax 66
SSH Client session 266
ssh key 815
ssh login-attempts 816
ssh server port 817
stale route 2685, 2687
static-channel-group 1422
statistics 4107
storm-control level 1374
STP
  configuring 1235
STP commands
  bridge cisco-interoperability 1311
  bridge forward-time 1283
  bridge instance priority 1313
  bridge max-age 1286
  bridge max-hops 1287
  bridge multiple-spanning-tree enable 1316
  bridge priority 1288
  bridge rapid-spanning-tree enable 1321
  bridge region 1322
  bridge revision 1323
  bridge shutdown 1289
  bridge spanning-tree enable 1324
  bridge spanning-tree errdisable-timeout enable 1325
  bridge spanning-tree portfast bpdu-filter 1328
  bridge transmit-holdcount 1290
  bridge-group path-cost 1292
  bridge-group priority 1293
  clear spanning-tree detected protocols 1337
  customer-spanning-tree customer-edge path-cost 1339
  customer-spanning-tree customer-edge priority 1340
  customer-spanning-tree forward-time 1341
  customer-spanning-tree hello-time 1342
  customer-spanning-tree max-age 1343
  customer-spanning-tree priority 1344
  customer-spanning-tree provider-edge path-cost 1345
  customer-spanning-tree provider-edge priority 1346
  customer-spanning-tree transmit-holdcount 1347
  debug mstp 1348
  show debugging mstp 1350
  show spanning-tree 1351
  show spanning-tree mst 1355
  show spanning-tree statistics 1357
  spanning-tree autoedge 1361
  spanning-tree edgeport 1362
  spanning-tree guard root 1363
  spanning-tree hello-time 1364
  spanning-tree instance restricted-role 1364
  spanning-tree instance restricted-tcn 1365
  spanning-tree link-type 1366
  spanning-tree mst configuration 1367
  spanning-tree restricted-role 1371
  spanning-tree restricted-tcn 1372
strict type 4326, 4423
summary-address 2357, 2445, 2791
suppressed route 2685, 2687
switchport 1306
switchport access vlan 1461
switchport customer-edge 3204
switchport customer-edge default-svlan 3205
switchport customer-edge hybrid allowed vlan 3206
switchport customer-edge vlan registration 3208
switchport customer-network vlan translation 3210
switchport hybrid allowed vlan 1462
switchport mode 3214
switchport mode access 1465
switchport mode customer-edge access 3215
switchport mode customer-edge hybrid 3216
switchport mode hybrid 1466, 1467
switchport mode ingress-filter 3214
switchport mode trunk 1468
switchport private-vlan host-association 1474
switchport private-vlan mapping 1475
switchport provider-edge vlan 3217
switchport provider-network vlan translation 3218
switchport trunk allowed vlan 1469
switchport trunk native vlan 1472
synchronization command 2603

T

tacacs-server deadtime 942
tacacs-server directed-request 942
tacacs-server host 942

tacacs-server key 944
Tail-Drop Configuration 3625
Telnet 947
telnet server port 955
tenant 3787
TIB 2885
time
  command syntax 66
Time To Live 4071
timers lsa arrival 2358
timers throttle lsa 2360
Topology 1165
traceroute 487
transmit delay 2338
transmit-delay 2412
Tree Information Base 2885
trigger failover 995
Trigger Failover Commands 987
Trust DSCP on Layer 2 Interface Configuration 3557, 3559
TTL Value 4071
Tunnel End Point 3787

U

UDLD configuration 1261
undebug all pim sparse-mode 3046
unicast configuration 3789
update-delay 2503
update-type command 4422
username 1003
username keypair 820
username sshkey 819

V

valid route 2685, 2688
VC Commands
  show mpls l2-circuit 4190
version display 4520
vertical bars
  command syntax 65
Virtual eXtensible Local Area Network (VXLAN) 3787
virtual IP address 3407
virtual links 1625
Virtual Local Area Network 82
Virtual MAC command 3409
Virtual routing and forwarding (VRF) 2121
virtual-ip 3407
vlan classifier ipv4 1481
VLAN commands
  show vlan access-map 1455
  show vlan all 1456
  show vlan auto 1458
  show vlan brief 1458
  show vlan classifier 1459
  switchport access vlan 1461
  switchport hybrid allowed vlan 1462
  switchport mode access 1465
  switchport mode hybrid 1466, 1467
  switchport mode trunk 1468
  switchport trunk allowed vlan 1469
  switchport trunk native vlan 1472
  vlan classifier ipv4 1481
  vlan database 1483
  vlan state 1485
vlan database command 1483
vlan state 1485
vlan type 3220
VLOG commands 1005
  reset log file 1006
  show vlog all 1006
  show vlog clients 1007
  show vlog terminals 1008
  show vlog virtual-routers 1009
VPN Commands
  ip vrf 658
  ip vrf forwarding 658
  show ip vrf 716
VRF 2451
VRF Configuration 2121
VRRP 88
VRRP Commands 3383
  debug vrrp 3388
  disable 3389
  enable 3390
  preempt-mode 3393
  show debugging vrrp 3396
  show running-config router vrrp 3397
  virtual-ip 3407
  vrrp vmac 3409
VRRP process 3353
VXLAN Architecture 3787
VXLAN Commands 3941, 4005
vxlan host-reachability-protocol evpn-bgp 4004
VXLAN Network Identifier (VNI) 3787
VXLAN Tunnel EndPoints 3787
VXLAN Unicast Configuration 3789

W

Weights for Queues Configuration 3563
WORD 66
WRED Configuration 3619
write terminal 489

© 2021 IP Infusion Inc. Proprietary