目 录

第 1 章 通用命令 14
1.1 模式命令 14
1.1.1 configure terminal 14
1.1.2 disable 14
1.1.3 enable 15
1.1.4 exit 15
1.2 文件管理命令 16
1.2.1 copy running-config startup-config 16
1.2.2 delete startup-config 16
1.2.3 download configure 17
1.2.4 download union 17
1.2.5 upload configure 18
1.2.6 write 18
1.3 系统管理命令 18
1.3.1 access-class 18
1.3.2 disable telnet 19
1.3.3 enable telnet 19
1.3.4 enable password 20
1.3.5 exec-timeout 20
1.3.6 hostname 21
1.3.7 password 21
1.3.8 reset 22
1.3.9 reset module 22
1.3.10 reset system 22
1.3.11 set date-time 23
1.3.12 show date-time 23
1.3.13 show history 24
1.3.14 show version 24
1.3.15 terminal 25
1.3.16 who 25
1.4 查看配置命令 26
1.4.1 show running-config 26
1.4.2 show startup-config 26
1.5 Mac地址表命令 27

1.5.1 bridge ageing-time 27
1.6 网络调试命令 27
1.6.1 ping 27
1.6.2 telnet 28
1.6.3 trace-route 29
1.7 多用户管理命令 29
1.7.1 username 30
1.8 系统监控命令 30
1.8.1 alarm 30
1.8.2 show temperature 30
1.8.3 show voltage 31
第 2 章 模块管理命令 32
2.1 模块配置命令 32
2.1.1 create module 32
2.1.2 remove module 32
2.2 模块查看命令 33
2.2.1 show bdver 33
2.2.2 show module 33
第 3 章 端口命令 35
3.1 端口通用配置 35
3.1.1 interface 35
3.1.2 description 35
3.1.3 flowcontrol 36
3.1.4 show flowcontrol 36
3.1.5 show interface 37
3.1.6 shutdown 38
3.1.7 speed 38
3.2 MIRROR命令 39
3.2.1 mirror 39
3.2.2 show mirror 40
3.3 端口限速命令 40
3.3.1 portrate 40
3.3.2 show portrate 41
3.4 广播风暴控制命令 41
3.4.1 storm-control 41
3.4.2 show storm-control 42
3.5 端口链路聚合命令 42

3.5.1 trunk 42
3.5.2 trunk interface 43
3.5.3 trunk load-balance 43
3.5.4 show trunk 44
第 4 章 vlan命令 46
4.1 vlan创建命令 46
4.1.1 vlan database 46
4.1.2 vlan 46
4.2 vlan端口配置命令 47
4.2.1 switchport access 47
4.2.2 switchport hybrid allowed vlan add 47
4.2.3 switchport hybrid allowed vlan all 48
4.2.4 switchport hybrid allowed vlan none 49
4.2.5 switchport hybrid allowed vlan remove 49
4.2.6 switchport hybrid vlan 50
4.2.7 switchport mode 50
4.2.8 switchport trunk allowed vlan add 51
4.2.9 switchport trunk allowed vlan all 52
4.2.10 switchport trunk allowed vlan none 52
4.2.11 switchport trunk allowed vlan remove 53
4.2.12 vlan classifier activate 53
4.3 vlan查看命令 54
4.3.1 show vlan 54
4.3.2 show vlan classifier 55
第 5 章 QinQ命令 57
5.1 配置命令 57
5.1.1 switchport link-type dot1q-in-q 57
5.2 查看命令 58
5.2.1 show dot1q-in-q 58
第 6 章 MSTP命令 59
6.1 MSTP配置命令 59
6.1.1 spanning-tree mst cisco-interoperability 59
6.1.2 spanning-tree mst configuration 59
6.1.3 spanning-tree mst enable 60
6.1.4 spanning-tree mst errdisable-timeout 60
6.1.5 spanning-tree mst forward-time 61

6.1.6 spanning-tree mst hello-time 61
6.1.7 spanning-tree mst max-age 62
6.1.8 spanning-tree mst max-hops 62
6.1.9 spanning-tree mst portfast 63
6.1.10 spanning-tree mst portfast bpdu-filter 63
6.1.11 spanning-tree mst portfast bpdu-guard 64
6.1.12 spanning-tree mst priority 64
6.1.13 instance 65
6.1.14 region 65
6.1.15 revision 66
6.1.16 spanning-tree mst force-version 66
6.1.17 spanning-tree mst guard root 67
6.1.18 spanning-tree mst instance 67
6.1.19 spanning-tree mst link-type 68
6.1.20 spanning-tree mst path-cost 69
6.1.21 spanning-tree mst priority 70
6.1.22 clear spanning-tree detected protocols 71
6.2 MSTP查看命令 71
6.2.1 show spanning-tree mst 71
6.3 MSTP调试命令 73
6.3.1 debug mstp 73
6.3.2 debug mstp all 73
6.3.3 debug mstp cli 74
6.3.4 debug mstp packet 74
6.3.5 debug mstp protocol 75
6.3.6 debug mstp timer 75
第 7 章 EAPS命令 77
7.1 配置命令 77
7.1.1 eaps control-vlan 77
7.1.2 eaps create 77
7.1.3 eaps disable 78
7.1.4 eaps enable 78
7.1.5 eaps extreme-interoperability 78
7.1.6 eaps fail-time 79
7.1.7 eaps hello-time 80
7.1.8 eaps mode 80
7.1.9 eaps primary-port 81

7.1.10 eaps protected-vlan 81
7.1.11 eaps remove 82
7.1.12 eaps secondary-port 82
7.2 查看命令 83
7.2.1 show eaps 83
7.3 调试命令 83
7.3.1 debug eaps 83
第 8 章 IGMP SNOOPING命令 85
8.1 IGMP SNOOPING配置命令 85
8.1.1 ip igmp snooping 85
8.1.2 ip igmp snooping fast-leave 85
8.1.3 ip igmp snooping fast-leave-timeout 86
8.1.4 ip igmp snooping group-membership-timeout 86
8.1.5 ip igmp snooping mrouter 87
8.1.6 ip igmp snooping query-membership-timeout 87
8.1.7 ip ip igmp snooping vlan 88
8.1.8 ip igmp snooping explicit-tracking 88
8.1.9 ip igmp snooping ssm-safe-reporting 89
8.2 IGMP SNOOPING查看命令 90
8.2.1 show ip igmp snooping 90
8.2.2 show ip igmp snooping age-table 91
8.2.3 show ip igmp snooping mrouter 91
8.2.4 show ip igmpv2 92
8.2.5 show ip igmp snooping explicit-tracking 92
8.2.6 show ip igmp snooping ssm-safe-reporting 93
8.2.7 show ip igmpv3 93
8.3 IGMP SNOOPING调试命令 94
8.3.1 debug igmp snooping 94
第 9 章 ACL命令 95
9.1 ACL配置命令 95
9.1.1 标准的ACL规则 95
9.1.2 扩展的ACL规则 96
9.1.3 字符类型的ACL规则 97
9.1.4 基于MAC的ACL规则 98
9.1.5 基于MAC ARP的ACL规则 99
9.1.6 access-group 100

9.1.7 删除ACL规则 100
9.2 ACL查看命令 101
9.2.1 show access-group 101
9.2.2 show access-list 101
第 10 章 QoS命令 103
10.1 QOS配置命令 103
10.1.1 qos class 103
10.1.2 qos cos-dscp 103
10.1.3 qos dscp-dscp 104
10.1.4 qos interdscp-queue 104
10.1.5 qos policy 105
10.1.6 qos prec-dscp 106
10.1.7 qos schedule 106
10.1.8 qos service-policy 107
10.1.9 qos trust 107
10.2 QOS查看命令 108
10.2.1 show qos 108
10.2.2 show qos class 108
10.2.3 show qos cos-dscp 108
10.2.4 show qos dscp-dscp 109
10.2.5 show qos interdscp-queue 109
10.2.6 show qos policy 110
10.2.7 show qos prec-dscp 110
10.2.8 show qos schedule 110
第 11 章 IP路由命令 112
11.1 配置命令 112
11.1.1 arp 112
11.1.2 arp lock 113
11.1.3 arp query 113
11.1.3 arp static 114
11.1.4 ip address 114
11.1.5 ip prefix-list 115
11.1.6 ip route 116
11.1.7 match interface 117
11.1.8 match ip 117
11.1.9 match metric 118

11.1.10 match route-type 118
11.1.11 policy route 119
11.1.12 match tag 120
11.1.13 router-id 120
11.1.14 route-map 121
11.1.15 set ip 122
11.1.16 set metric 122
11.1.17 set metric-type 123
11.1.18 set tag 123
11.2 显示命令 124
11.1.1 show arp 124
11.1.2 show ip interface 125
11.2.3 show ip prefix-list 125
11.2.4 show ip route 126
11.2.5 show ip route connected 127
11.2.6 show ip route database 128
11.2.7 show policy route 129
11.2.8 show route-map 130
第 12 章 RIP命令 131
12.1 配置命令 131
12.1.1 default-information originate 131
12.1.2 default-metric 131
12.1.3 distance 132
12.1.4 distribute-list 132
12.1.5 ip rip authentication 133
12.1.6 ip rip metric 134
12.1.7 ip rip receive version 134
12.1.8 ip rip receive-packet 135
12.1.9 ip rip send version 135
12.1.10 ip rip send-packet 136
12.1.11 ip rip split-horizon 136
12.1.12 maximum-prefix 137
12.1.13 neighbor 137
12.1.14 network 138
12.1.15 offset-list 138
12.1.16 passive-interface 139
12.1.17 recv-buffer-size 140

12.1.18 redistribute 140
12.1.19 route 141
12.1.20 router rip 141
12.1.21 timers 142
12.1.22 version 142
12.2 查看命令 143
12.2.1 show ip rip 143
12.2.2 show ip route rip 144
12.2.3 show running rip 145
12.3 调试命令 145
12.3.1 debug rip 145
12.3.2 debug rip all 146
12.3.3 debug rip events 146
12.3.4 debug rip packet 147
第 13 章 OSPF命令 148
13.1 配置命令 148
13.1.1 area authentication 148
13.1.2 area default-cost 148
13.1.3 area filter-list 149
13.1.4 area nssa 150
13.1.5 area range 150
13.1.6 area shortcut 151
13.1.7 area stub 152
13.1.8 area virtual-link 152
13.1.9 area virtual-link authentication 153
13.1.10 auto-cost reference-bandwidth 154
13.1.11 compatible rfc1583 155
13.1.12 default-information originate 155
13.1.13 default-metric 156
13.1.14 distance 156
13.1.15 distribute-list 157
13.1.16 host 158
13.1.17 ip ospf authentication 158
13.1.18 ip ospf authentication-key 159
13.1.19 ip ospf cost 159
13.1.20 ip ospf database-filter 160
13.1.21 ip ospf dead-interval 160

13.1.22 ip ospf disable all 161
13.1.23 ip ospf hello-interval 161
13.1.24 ip ospf message-digest-key 162
13.1.25 ip ospf mtu 162
13.1.26 ip ospf mtu-ignore 163
13.1.27 ip ospf network 163
13.1.28 ip ospf priority 164
13.1.29 ip ospf retransmit-interval 165
13.1.30 ip ospf transmit-delay 165
13.1.31 max-concurrent-dd 166
13.1.32 neighbor 166
13.1.33 network 167
13.1.34 passive-interface 167
13.1.35 redistribute 168
13.1.36 router ospf 169
13.1.37 router-id 169
13.1.38 summary-address 170
13.1.39 timers spf 170
13.2 查看命令 171
13.2.1 show ip ospf 171
13.2.2 show ip ospf database 172
13.2.3 show ip ospf interface 174
13.2.4 show ip ospf neighbor 175
13.2.5 show ip ospf route 176
13.2.6 show ip ospf virtual-links 176
13.2.7 show running ospf 177
13.3 调试命令 178
13.3.1 debug ospf 178
13.3.2 debug ospf all 178
13.3.3 debug ospf events 179
13.3.4 debug ospf ifsm 179
13.3.5 debug ospf lsa 180
13.3.6 debug ospf nfsm 180
13.3.7 debug ospf packet 181
13.3.8 debug ospf route 182
第 14 章 VRRP命令 183
14.1 配置命令 183

14.1.1 disable/enable 183
14.1.2 router vrrp 183
14.1.3 vrrp ip-address 184
14.1.4 vrrp advertisement-interval 185
14.1.5 vrrp authentication 185
14.1.6 vrrp preempt 186
14.1.7 vrrp priority 186
14.1.8 vrrp tracking 187
14.2 查看命令 188
14.2.1 show vrrp 188
14.3 调试命令 189
14.3.1 debug vrrp 189
14.3.2 debug vrrp all 189
14.3.3 debug vrrp events 190
14.3.4 debug vrrp packet 190
第 15 章 VLLP命令 192
15.1 配置命令 192
15.1.1 router vllp 192
15.1.2 vllp disable/enable 192
15.1.3 vllp port 193
15.1.4 vllp priority 193
15.1.5 vllp query-interval 194
15.2 查看命令 194
15.2.1 show vllp 194
15.2.2 show vllp map 196
15.2.3 show debugging vllp 197
15.3 调试命令 198
15.3.1 debug vllp 198
15.3.2 debug vllp all 198
15.3.3 debug vllp events 199
15.3.4 debug vllp packet 200
15.3.5 debug vllp efsm 202
15.3.6 debug vllp pfsm 203
第 16 章 DHCP-RELAY命令 205
16.1 配置命令 205
16.1.1 dhcp relay 205

16.1.2 dhcp server 205
16.1.3 dhcp snooping 206
16.2 查看命令 206
16.2.1 show debugging dhcp-relay 206
16.3 调试命令 207
16.3.1 debug dhcp-relay 207
16.3.2 debug dhcp-relay all 208
16.3.3 debug dhcp-relay events 208
16.3.4 debug dhcp-relay packet 209
第 17 章 IGMP命令 210
17.1 IGMP配置命令 210
17.1.1 ip igmp 210
17.1.2 ip igmp access-group 210
17.1.3 ip igmp immediate-leave group-list 211
17.1.4 ip igmp last-member-query-count 211
17.1.5 ip igmp last-member-query-interval 212
17.1.6 ip igmp querier-timeout 213
17.1.7 ip igmp query-interval 213
17.1.8 ip igmp query-max-response-time 214
17.1.9 ip igmp robustness-variable 214
17.1.10 ip igmp version 215
17.2 IGMP查看命令 215
17.2.1 show ip igmp groups 215
17.2.2 show ip igmp interface 216
17.3 IGMP调试命令 216
17.3.1 debug igmp 216
17.3.2 show debug igmp 217
第 18 章 PIM-SM命令 218
18.1 系统配置命令 218
18.1.1 ip mroute 218
18.1.2 ip multicast route-limit 219
18.1.3 ip multicast-routing 219
18.1.4 ip pim accept-register 220
18.1.5 ip pim bsr-candidate 220
18.1.6 ip pim cisco-register-checksum 221
18.1.7 ip pim crp-cisco-prefix 222

18.1.8 ip pim ignore-rp-set-priority 222
18.1.9 ip pim jp-timer 223
18.1.10 ip pim register-rate-limit 223
18.1.11 ip pim register-rp-reachability 224
18.1.12 ip pim register-source 224
18.1.13 ip pim register-suppression 225
18.1.14 ip pim rp-address 226
18.1.15 ip pim rp-candidate 226
18.1.16 ip pim rp-register-kat 227
18.1.17 ip pim spt-threshold 227
18.2 接口配置命令 228
18.2.1 ip pim dr-priority 228
18.2.2 ip pim exclude-genid 229
18.2.3 ip pim hello-holdtime 229
18.2.4 ip pim hello-interval 230
18.2.5 ip pim neighbor-filter 231
18.2.6 ip pim sparse-mode 232
18.2.7 ip pim sparse-mode passive 232
18.2.8 ip multicast ttl-threshold 233
18.3 查看命令 233
18.3.1 show debugging pim sparse-mode 233
18.3.2 show ip mroute 234
18.3.3 show ip mvif 235
18.3.4 show ip pim sparse-mode bsr-router 236
18.3.5 show ip pim sparse-mode interface 236
18.3.6 show ip pim sparse-mode local-members 237
18.3.7 show ip pim sparse-mode mroute 238
18.3.8 show ip pim sparse-mode neighbor 239
18.3.9 show ip pim sparse-mode nexthop 240
18.3.10 show ip pim sparse-mode rp 241
18.3.11 show ip pim sparse-mode rp-hash 241
18.4 诊断与调试命令 242
18.4.1 debug pim sparse-mode 242
18.4.2 debug pim sparese-mode all 243
18.4.3 debug pim sparse-mode event 243
18.4.4 debug pim sparse-mode mfc 244
18.4.5 debug pim sparse-mode mib 245

18.4.6 debug pim sparse-mode nexthop....246
18.4.7 debug pim sparse-mode packets....247
18.4.8 debug pim sparse-mode state....248
18.4.9 debug pim sparse-mode timer....248
第 19 章 SNMP命令....250
19.1 SNMP配置命令....250
19.1.1 snmp community....250
19.1.2 snmp trap....250
19.1.3 snmp system information contact....251
19.1.4 snmp engine-id local....252
19.1.5 snmp user....252
19.1.6 snmp group....253
19.2 SNMP查看命令....254
19.2.1 show snmp community....254
19.2.2 show snmp trap....254
19.2.3 show snmp system information....255
19.2.4 show snmp engine-id....255
19.2.5 show snmp user....256
19.2.6 show snmp group....256
第 20 章 系统日志命令....257
20.1 通用日志命令....257
20.1.1 debug ip....257
20.1.2 log display....257
20.1.3 no debug all....258
20.1.4 show debugging....258
20.1.5 show log....260
20.1.6 show log display....261

第 1 章 通用命令

1.1 模式命令

1.1.1 configure terminal

命令

configure terminal

模式

特权模式

参数

无。

描述

configure terminal命令用来进入配置模式

举例

#进入全局配置模式:

Switch#configure terminal

Switch(config)#

1.1.2 disable

命令

disable

模式

特权模式

参数

无

描述

disable命令用来关闭特权模式，退回到普通模式。

举例

#关闭并退回到普通模式:

Switch#disable

Switch>

1.1.3 enable

命令

enable

模式

普通模式

参数

无

描述

如果密码通过，进入特权模式。

举例

#从普通模式进入特权模式：

Switch> enable

password:******

switch#

1.1.4 exit

命令

exit

模式

所有模式

参数

无

描述

exit命令用来结束当前模式，回到前一个模式。

举例

#从特权模式退回到普通模式：

Switch#exit

Switch>

1.2 文件管理命令

1.2.1 copy running-config startup-config

命令

copy running-config startup-config

模式

特权模式

参数

无。

描述

copy running-config startup-config 命令将系统当前配置保存为启动配置文件。

举例

#拷贝当前使用的配置作为下次启动的配置：

Switch#copy running-config startup-config

Building and writing configuration ...

Switch#

1.2.2 delete startup-config

命令

delete startup-config

模式

特权模式

参数

无。

描述

删除启动配置文件。执行该命令后重启交换机，将恢复到出厂设置。

举例

#删除启动配置：

Switch#delete startup-config

Switch#

1.2.3 download configure

命令

download configure <ip-address> <file-name>

模式

特权模式

参数

ip-address：TFTP 服务器ip地址。

file-name: TFTP服务器上的配置文件名。

描述

从 TFTP 服务器上将配置文件下载到交换机作为启动配置文件，重启交换机后下载的配置文件生效。

举例

#将配置文件下载到主机 172.16.0.1.文件名为 conf.txt:

Switch#download configure 172.16.0.1 conf.txt

1.2.4 download union

命令

download union <ip-address> <file-name>

模式

特权模式

参数

ip-address: TFTP 服务器ip地址。

file-name：TFTP 服务器上的联合文件名。

描述

下载联合文件。联合文件包含主控与线卡的 image 文件和版本文件。联合文件下载到主控中后，会检查主控和线卡的 image 文件版本，若版本不一致则将其更新为下载的版本，并修改版本文件。

举例

#从主机 172.16.0.200 下载联合文件到交换机:

Switch#download union 172.16.0.200 iSpirit8806_4v01.uni

Do you wish to continue? [Y/N]:y

1.2.5 upload configure

命令

upload configure <ip-address> <file-name>

模式

特权模式

参数

ip-address: 表示文件上传的目的TFTP 服务器的IP 地址。

file-name：保存到 TFTP 服务器上的配置文件名。

描述

将交换机的启动配置文件保存到 TFTP 服务器上。

举例

#将启动配置文件保存到主机 172.16.0.200 上，命名为 conf：

Switch#upload configure 172.16.0.200 conf

1.2.6 write

命令

write

模式

特权模式。

参数

无。

描述

保存当前用户配置的设置信息。

举例

无。

1.3 系统管理命令

1.3.1 access-class

命令

access-class <list-name>

no access-class [<list-name>]

模式

终端配置模式

参数

list-name: 访问列表的名字(数字名或字符串名)。

描述

access-class 命令通过调用一条基于 IP 的访问控制列表,实现对用户的控制。

no access-class 命令删除对用户的访问控制配置。

举例

#调用名为 lenovo8800 的访问控制列表规律用户:

Switch(config-line)#access-class lenovo8800

Switch(config-line)#

1.3.2 disable telnet

命令

disable telnet

模式

终端配置模式。

参数

无。

描述

关闭 telnet 服务功能，用户不能 telnet 到设备。

举例

无。

1.3.3 enable telnet

命令

enable telnet [number]

模式

终端配置模式。

参数

number: telnet 终端最大个数，范围为 1-100，默认为 5。

描述

打开 telnet 服务功能，用户可以 telnet 到设备。默认打开。

举例

无。

1.3.4 enable password

命令

enable password <password>

no enable password

模式

全局配置模式

参数

password：密码字符串。缺省密码为空。

描述

enable password 命令用来修改交换机从普通模式进入特权模式的密码。

no enable password 命令用来取消密码。

举例

#修改交换机的密码为admin：

Switch(config)#enable password admin

1.3.5 exec-timeout

命令

exec-timeout <minutes> [<seconds>]

no exec-timeout

模式

终端配置模式

参数

minutes：分钟，范围 0-35791。

seconds：秒，范围 0-2147483。

描述

exec-timeout 命令用来配置 telnet 终端空闲超时时间。默认值 10 分钟。

no exec-timeout 命令用来取消配置，恢复默认值。

举例

#配置超时时间为 15 分钟：

Switch(config-line)#exec-timeout 15

Switch(config-line)#

1.3.6 hostname

命令

hostname <name>

no hostname

模式

全局配置模式。

参数

name: 系统的名字，要以字母开头。默认的系统名为 Switch。

描述

hostname 命令用来修改系统的名字。

no hostname 将系统名字恢复为出厂设置。

举例

#将系统名改为 i8806：

Switch(config)#hostname i8806

i8806(config)#

1.3.7 password

命令

password <password>

no password

模式

全局配置模式。

参数

password: 密码字符串。默认没有密码。

描述

password 命令用来设置 Telnet 连接密码。

no password 命令用来取消密码设置，恢复默认值。

举例

无。

1.3.8 reset

命令

reset

模式

特权模式。

参数

无。

描述

reset 命令用来重启交换机主控模块。

举例

无。

1.3.9 reset module

命令

reset module [<Module-id>]）

模式

特权模式

参数

module-id：模块编号，对于 8806 范围：1-5。

描述

reset module 命令用来重启交换机或指定的模块。

举例

#重启第一槽的模块：

Switch#reset module 1

1.3.10 reset system

命令

reset system

模式

特权模式。

参数

无。

描述

reset system 命令用来重启交换机所有模块。

举例

无。

1.3.11 set date-time

命令

set date-time <year> <month> <day> <hour> <minute> <second>

模式

特权模式

参数

year: 设置年，范围：2000-2050。

month: 设置月，范围：1-12。

day: 设置日，范围：1-31。

hour: 设置小时，范围：0-23。

minute: 设置分钟，范围：0-59。

second: 设置秒，范围：0-59。

描述

set date-time 命令用来设置系统时间。

举例

无。

1.3.12 show date-time

命令

show date-time

模式

普通模式/特权模式

参数

无

描述

show date-time 命令用来显示系统当前日期和时间

举例

```
Switch#show date-time
        System Date Time        : 2006/10/27 11:27:46
Switch#
```

1.3.13 show history

命令

show history

模式

普通模式/特权模式。

参数

无。

描述

show history 命令用来显示命令历史，可以显示本命令之前执行的 20 条命令。

举例

无。

1.3.14 show version

命令

show version

模式

普通模式/特权模式

参数

无

描述

show version 命令用来显示系统 image 文件版本信息。

举例

#显示系统版本

Switch>show version

iSpirit8806 4.0.1

Build time:Sep 09 2007, 16:35:19

Switch>

1.3.15 terminal

命令

terminal{length <number>|no length}

模式

普通模式/特权模式

参数

length: 指定每次显示到屏幕的行数。默认25行。

no length: 取消显示行数的设置。

描述

terminal 命令用来配置终端一次显示到屏幕的行数。

举例

#配置终端每次显示10行:

Switch>terminal length 10

1.3.16 who

命令

who

模式

普通模式/特权模式

参数

无

描述

who 命令用来显示当前 vty 的用户。

举例

#显示当前的VTY用户：

Switch#who

vty[0] connected from

1.4 查看配置命令

1.4.1 show running-config

命令

show running-config [access-list | interface | ip {igmp snooping | route} | key chain | mstp | ospf | prefix-list | rip | route-map | vlan]

模式

特权模式

参数

access-list: ACL的相关配置。

interface: 接口的相关配置，包括物理接口和虚拟接口。

ip igmp snooping：igmp snooping的相关配置。

ip route: 路由的相关配置。

key chain: 认证密钥链的相关配置。

mstp: mstp的相关配置。

ospf：ospf的相关配置。

prefix-list：前缀列表的相关配置。

rip: rip协议的相关配置。

route-map: 路由表的相关配置。

vlan： vlan 的相关配置。

描述

show running-config 命令用来显示当前的配置信息。

举例

无。

1.4.2 show startup-config

命令

show startup-config

模式

特权模式

参数

无

描述

show startup-config 命令用来显示系统启动配置文件内容。

举例

无。

1.5 Mac 地址表命令

1.5.1 bridge ageing-time

命令

bridge ageing-time <time>

no bridge ageing-time

模式

全局配置模式

参数

time：mac 表老化时间，范围：10-1000000 秒。默认 300 秒。

描述

bridge ageing-time 命令用来设置 mac 地址表的老化时间。

no bridge ageing-time 命令将 mac 地址表的 age 时间恢复出厂值。

举例

#设置交换机的老化时间为100 秒：

Switch(config)#bridge ageing-time 100

Switch(config)#

1.6 网络调试命令

1.6.1 ping

命令

ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*

模式

特权模式

参数

ip-address: 目标IP 地址。

-n: 发送请求的数目。

-l: 发送包长度。

-r: 记录指定跳数的路由。

-s: 记录指定跳数的时间。

-j: 源带松散路由，输入路由跳数和相关跳的IP 地址。可以重复输入多个IP 地址。

-k: 源带严格路由，输入路由跳数和相关跳的IP 地址。可以重复输入多个IP 地址。

-w: 等待每个回应的超时时间，单位秒。

描述

ping 是一个测试另一台主机是否可达的网络调试工具。简单的应用只要输入目标主机的IP地址就可以了；如果使用ping作为诊断工具，可以输入更详细的参数。

举例

#向主机172.16.0.1发5个请求包。

Switch#ping 172.16.0.1 -n 5

1.6.2 telnet

命令

telnet <ip-address>

模式

特权模式

参数

ip-address: 目标 IP 地址。

描述

Telnet协议是TCP/IP协议族中的一员，是Internet远程登陆服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。

举例

#登录目的地址为192.168.1.2

Switch#telnet 192.168.1.2

1.6.3 trace-route

命令

trace-route <ip-address> [-h <maximum-hops> | -j <count> <ip-address>* | -w <timeout>]*

模式

特权模式

参数

ip-address: 目标IP 地址。

-h: 最大跳数。

-j: 源带松散路由，输入路由跳数和相关跳的IP 地址。 可以重复输入多个IP地址。

-w: 超时时间(秒)。

描述

traceroute可以检测数据包从一台主机传到另一台主机所经过的路由。如果只是要实现这个功能，用户只需要输入目标IP 地址就可以了。如果要作为网络诊断可以输入相关参数。

Traceroute 的实现方式是这样的，从本主机向目的主机发送TTL递增的UDP数据包。如果TTL 为零，经过的路由器会发送TTL 耗尽，主机不可达的ICMP 包；如果到达主机但是主机没有该UDP包的端口，主机就会回应端口不可达的ICMP包。traceroute根据所经过的回应的ICMP包是主机不可达还是端口不可达来判断是否到达目的主机。如果是主机不可达说明经过的是路由器，打印这个路由器的IP地址，继续发送TTL 加1 的UDP包，直到TTL 等于Maxmum time to live。如果是端口不可达说明到达了目的主机，打印这个主机的IP地址，停止发送UDP包。

举例

#检测目的为192.168.10.2，最大跳数10跳的所经路由：

Switch#trace-route 192.168.10.2 -n 10

1.7 多用户管理命令

1.7.1 username

命令

username <username> password <password> {normal | privilege}

no username [username]

模式

全局配置模式

参数

username: 用户名字符串,最大长度为20个。

password: 密码字符串，最大长度为20个。

normal: 普通权限。

privilege: 特权权限。

描述

username命令可以添加用户，修改已经存在的用户的密码或权限。无默认用户，最多可添加十个用户。多用户只能用于telnet终端登陆使用。

no username命令用来删除已经存在的一个用户或所有用户。

举例

#添加一个用户名为abc, 密码为abc，权限为normal的用户。

Switch(config)#username abc password abc normal

Switch(config)#

1.8 系统监控命令

1.8.1 alarm

命令

alarm {disable | enable}

模式

模块配置模式

参数

disable: 停止告警音。

enable: 产生告警音。

描述

alarm命令用来控制当主控和线卡的电压或温度产生异常时是否发出告警音。

举例

#让当主控的电压异常时产生告警。

Switch(config-module)#alarm enable

Switch(config-module)#

1.8.2 show temperature

命令

show temperature [module-id]

模式

普通模式/特权模式

参数

module-id: 模块号，主控编号为 17，8806 线卡编号为 1-5。

描述

show temperature命令用来显示主控和线卡的各个部位的温度。

举例

```
Switch#show temperature
slotid     temp1              temp2              temp3              temp4
mgta     38.0C(70.0C)       34.0C(70.0C)       30.0C(70.0C)       NA
1        44.5C(70.0C)     47.0C(70.0C)     40.5C(70.0C)     39.0C(70.0C)
2        35.5C(70.0C)     35.0C(70.0C)     34.5C(70.0C)     29.0C(70.0C)
```

1.8.3 show voltage

命令

show voltage [module-id]

模式

普通模式/特权模式

参数

module-id: 模块号，主控编号为 17，8806 线卡编号为 1-5。

描述

show voltage命令用来显示主控和线卡的各个部位的电压。

举例

```
Switch#show voltage
slotid     voltage1 voltage2   voltage3   voltage4   voltage5     voltage6
mgta    2.25~2.75 1.13~1.38 2.97~3.63 4.50~5.50 10.80~13.20 1.80~2.20
mgta       2.50         1.23         3.18         4.91         12.06         2.00
1        2.25~2.75 1.13~1.38 2.97~3.63 1.80~2.20 10.80~13.20 1.08~1.32
1          2.52         1.24         3.20         2.03         12.06         1.20
4        2.25~2.75 1.13~1.38 2.97~3.63 1.80~2.20 10.80~13.20 2.97~3.63
4          2.51         1.25         3.20         2.00         12.06         3.24
5        2.25~2.75 1.13~1.38 2.97~3.63 1.80~2.20 10.80~13.20 2.97~3.63
5          2.51         1.25         3.20         2.00         12.06         3.24
Switch#
```

第 2 章 模块管理命令

2.1 模块配置命令

2.1.1 create module

命令

creat module <module-id> <module-type>

模式

模块配置模式

参数

module-id: 线卡编号，1-5。

module-type: 模块类型，包括：24gt、24gx、28xt、8806-12gt 等。

描述

creat module 命令用来创建线卡。该命令可在空槽位创建一个虚拟的线卡，并可进行端口配置。当该槽位插入类型相符的线卡时，之前的配置会下发到线卡并生效。当该槽位插入类型不相符的线卡时，主控终端会提示线卡类型不符，需删除该线卡，然后交换机会自动创建线卡。

在 1 号槽位中，只可以创建全尺寸线卡；在 2-5 号槽位中，只可以创建半尺寸线卡

举例

#在3号槽位创建12gt：

Switch(config-module)#create module 3 8806-12gt

2.1.2 remove module

命令

remove module <module-id>

模式

模块配置模式

参数

module-id: 线卡编号，1-5。

描述

remove module 命令用来删除线卡。若该槽位有线卡，则删除后会再自动创建线卡。

举例

#删除第二槽的线卡：

Switch(config-module)#remove module 2

2.2 模块查看命令

2.2.1 show bdver

命令

show bdver [module-id]

模式

特权模式

参数

module-id: 模块号，主控编号为 17，8806 线卡编号为 1-5。

描述

show bdver 命令用来显示模块的 image 文件版本。

举例

#Switch#sh bdver

slotid	modulename	ver
0	mgt-12xt	4.0.1
1	24gt	4.0.1
2	null	0.0.0
3	null	0.0.0
4	8806-12gt	4.0.1
5	8806-12gt	4.0.1
17	mgt-a	4.0.1

2.2.2 show module

命令

show module [<Module-id>]

模式

特权模式

参数

Module-id：模块号。8806 线卡编号为 1-5，主控编号为 17，电源编号为 19-21，风扇编号为 22。

描述

show module 命令用来显示模块类型和状态。

举例

#显示当前的模块类型和状态

```
Switch#show module
        slotid   modulename        online   other
          0      mgt-12xt          online   on /heartbeat
          1      24gt              online   on /heartbeat
          2      null              offline off/no heartbeat
          3      null              offline off/no heartbeat
          4      8806-12gt         online   on /heartbeat
          5      8806-12gt         online   on /heartbeat
          17     mgt-a             online   master
          19     power             online   null
          20     power             offline
          21     power             offline
          22     fan               offline null
        Switch#
```

第 3 章 端口命令

3.1 端口通用配置

3.1.1 interface

命令

interface <if-name>

模式

全局配置模式/接口配置模式

参数

if-name: 端口名。百兆端口以 fe 为前缀,千兆端口以 ge 为前缀，万兆端口以 xe 为前缀,后加模块号/端口号。聚合端口以 trunk 为前缀。例：第一槽的 24gt 的第一端口表示为 ge1/1；聚合端口 1 表示为 trunk1。

描述

interface命令用来进入某一个端口的配置模式。

举例

#进入第一槽的 24gt 的端口 24:

Switch(config)#interface ge1/24

#进入聚合端口 1：

Switch(config)#interface trunk1

3.1.2 description

命令

description <line>

no description

模式

接口配置模式。

参数

line: 端口描述字符串。

描述

description 命令设置端口描述，可对端口做说明。

no description 命令取消端口描述的配置。

举例

#设置端口ge1/1的描述为：bulid 1 floor 5

Switch(config-ge1/1)#description bulid 1 floor 5

3.1.3 flowcontrol

命令

flowcontrol {receive | send} {off | on}

模式

接口配置模式

参数

receive：接受流控帧的能力。

send: 发送流控帧的能力。

off：关闭功能。

on：打开功能。

描述

flowcontrol 命令用来打开或关闭端口的流控功能，可控制是否发送流控帧或是否处理接收到的流控帧。

举例

无。

3.1.4 show flowcontrol

命令

show flowcontrol [interface <if-name>]

模式

普通模式/特权模式

参数

if-name：接口名。

描述

查看端口流控的配置情况。

举例

无。

3.1.5 show interface

命令

show interface [<if-name> | statistics <if-name>]

模式

普通模式/特权模式

参数

if-name：接口名。

statistics: 显示端口收发包统计信息。

描述

show interface 命令不加参数显示所有的二层和三层接口的信息。指定接口名显示指定的二层或三层接口的信息。show interface statistics 显示指定接口的收发包统计信息。

举例

#显示 vlan1 接口的信息：

```
Switch>show interface vlan1
Interface vlan1
   Hardware Type:      VLAN
   MAC Address:        0009.ca1b.a011
   Flags:              <UP,BROADCAST,MULTICAST>
   Admin Status:       UP
   Operate Status:     DOWN
   Index:              3
   Metric:             1
   MTU:                1500
   IP Address:         192.168.0.1/24

Switch#show interface ge1/1
Interface ge1/1
   Hardware Type:      Ethernet
   MAC Address:        0009.ca1b.a210
   Flags:              <UP,BROADCAST,MULTICAST>
   Admin Status:       UP
   Operate Status:     DOWN
```

Index: 2001
Metric: 1
MTU: 1500
Duplex: unknown
Config Duplex: AutoNego
Bandwidth: 1g
Config Bandwidth: AutoNego
Switchport Mode: access
Default Vlan: 2

3.1.6 shutdown

命令

shutdown
no shutdown

模式

接口配置模式

参数

无

描述

shutdown 关闭端口，端口的管理状态为 DOWN。

no shutdown 打开端口，端口的管理状态为 UP。

举例

#关闭端口 ge1/1:
Switch(config-ge1/1)#shutdown
Switch(config-ge1/1)#

3.1.7 speed

命令

Speed {autonegtiate | full-10 | full-100 | full-1000 | half-10 | half-100}

模式

接口配置模式

参数

Autonegtiate：速率双工状态为自适应。

full-10：速率双工状态为 10M 全双工。

full-100：速率双工状态为 100M 全双工。

full-1000：速率双工状态为 1000M 全双工。

half-10：双工状态为 10M 半双工。

half-100：双工状态为 100M 半双工。

描述

设置端口的速率双工状态。

举例

#将端口 ge1/1 的速率双工状态配置为强制 100M 全双工：

Switch(config-ge1/1)#speed full-100

3.2 MIRROR 命令

3.2.1 mirror

命令

mirror interface <if-name> direction {both | receive | transmit}

no mirror interface <if-name> direction [receive | transmit]

模式

接口配置模式。

参数

if-name: 被侦听端口。

both： 侦听指定端口的进出数据流。

receive：侦听指定端口收到的数据流。

transmit：侦听指定端口输出的数据流。

描述

mirror interface命令指定被侦听的端口，用来侦听其它端口的数据流。

no mirror interface 命令取消端口的侦听设置。

举例

#用端口ge1/1侦听端口ge1/12的输入数据流：

Switch(config-ge1/1)#mirror interface ge1/12 direction receive
Switch(config-ge1/1)#

3.2.2 show mirror

命令

show mirror [interface <if-name>]

模式

特权模式

参数

interface <if-name>：端口名。

描述

show mirror 命令用来显示指定端口的 mirror 配置情况。

举例

无。

3.3 端口限速命令

3.3.1 portrate

命令

portrate egress <rate>

portrate ingress <rate>

模式

接口配置模式。

参数

egress：端口输出速率。

ingress：端口输入速率。

rate：设定的速率值，范围：1-1048512 kbits。

描述

设置端口最大的输入输出速率。最小限制值为 64Kbps，粒度也是 64 Kbps。

举例

#设置端口 ge1/2 输入限速 128Kbps：

Switch(config-ge1/2)#portrate ingress 128

Switch(config-ge1/2)#

3.3.2 show portrate

命令

show portrate [interface <if-name>]

模式

特权模式

参数

if-name： 端口名。

描述

show portrate 命令用来显示指定端口的限速配置。

举例

无。

3.4 广播风暴控制命令

3.4.1 storm-control

命令

storm-control {broadcast | dlf | multicast} level <level>

no storm-control {broadcast | dlf | multicast} level <level>

模式

接口配置模式

参数

broadcast： 控制广播包。

dlf：控制目的未知的单播包。

multicast：控制组播包。

level：控制的百分比，100%为 2097151 packets/s。精确到小数点后一位。实际控制值为 2097151*level/100。

描述

storm-control 命令用来设置端口对广播包、dlf 包、组播包的转发限制。设置了 storm-control 的端口收到符合设置的数据流时会限制转发速度。

no storm-control 命令用来取消设置。

举例

#限制端口 ge1/1 对广播流的转发速度为 20971 packets/s:

Switch(config-ge1/1)#storm-control broadcast level 1

3.4.2 show storm-control

命令

show storm-control [<if-name>]

模式

特权模式

参数

if-name：端口名。

描述

show storm-control 命令用来显示 storm-control 的设置情况，显示内容包括广播包、dlf 包、组播包的控制值和丢弃的包数量。

举例

#显示端口 ge1/1 的 storm-control 配置：

Switch#show storm-control ge1/1

Port BcastLevel BcastDiscards McastLevel McastDiscards DlfLevel DlfDiscards

ge1/1 100.00% 0 100.00% 0 100.00% 0

Switch#

3.5 端口链路聚合命令

3.5.1 trunk

命令

trunk <trunk-id>

no trunk <trunk-id>

模式

全局配置模式。

参数

trunk-id：链路聚合号，范围<1-32>。缺省没有配置链路聚合。

描述

trunk 命令用于创建一个链路聚合，系统将一个链路聚合作为一个逻辑端口对待。需先创建链路聚合后才能配置聚合端口。每个 trunk 组最多支持 8 个端口。

no trunk 命令用于删除一个链路聚合。删除 trunk 组之前需先删除成员端口。

举例

#配置一个组号为 1 的聚合链路：

```
Switch(config)#trunk ?
<1-32>    Trunk id
Switch(config)#trunk 1
Switch(config)#
```

3.5.2 trunk interface

命令

trunk interface <if-name>

no trunk interface [<if-name>]

模式

接口配置模式。

参数

if-name：端口名。

描述

trunk interface <if-name>命令将物理端口加入 trunk 组，成为聚合端口。

no trunk interface 命令将物理端口从 trunk 组中删除；若输入端口名称则只删除指定端口，若不输入端口名称则删除该 trunk 组内所有物理端口。

举例

#配置端口 ge1/1 成为 trunk1 的成员端口：

```
Switch(config-trunk1)#trunk interfae ge1/1
```

3.5.3 trunk load-balance

命令

trunk load-balance { dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no trunk load-balance

模式

接口配置模式。

参数

dst-ip：根据目的 IP 地址对出端口方向的数据流进行负载均衡。

dst-mac：根据目的 MAC 地址对出端口方向的数据流进行负载均衡。

src-dst-ip：根据源 IP 地址和目的 IP 地址对出端口方向的数据流进行负载均衡。

src-dst-mac：根据源MAC地址和目的MAC 地址对出端口方向的数据流进行负载均衡。这是默认的负载均衡策略。

src-ip：根据源 IP 地址对出端口方向的数据流进行负载均衡。

src-mac：根据源 MAC 地址对出端口方向的数据流进行负载均衡。

描述

trunk load-balance命令设置TRUNK组的负载均衡策略。

no trunk load-balance命令取消配置的负载均衡策略，恢复为src-dst-mac策略。

举例

#配置 trunk 组 1 根据目的 IP 地址进行负载均衡：

Switch(config-trunk1)#trunk load-balance dst-ip

3.5.4 show trunk

命令

show trunk [<trunk-id>]

模式

特权模式。

参数

trunk-id：要查询的 TRUNK 组的 ID 号。

描述

显示链路聚合配置，包括 trunk 组名、负载均衡策略和成员端口。若不指定 trunk 组 ID 号则显示所有的聚合端口配置。

举例

#显示所有的链路聚合配置：

Switch#show trunk

% Trunk name: trunk15

% Load-balance: Source and Destination Mac address

% Member:

```
    ge2/6
    ge2/10
% Trunk name: trunk10
% Load-balance: Source and Destination Mac address
% Member:
    ge4/11
    ge4/12
Switch#
```

第 4 章 vlan 命令

4.1 vlan 创建命令

4.1.1 vlan database

命令

vlan database

模式

全局配置模式

参数

无。

描述

进入 vlan 配置模式。

举例

#进入 vlan 配置模式：

Switch(config)#vlan database

Switch(config-vlan)#

4.1.2 vlan

命令

vlan <vlan-id>

no vlan <vlan-id>

模式

vlan 配置模式

参数

vlan-id：要创建的 vlan 号。取值范围：2～4094

描述

vlan 命令用来创建VLAN。需要注意的是VLAN 1 为缺省VLAN无法删除。

no vlan命令用来删除一个vlan。

举例

#创建 vlan 2：

Switch(config-vlan)#vlan 2

Switch(config-vlan)#

4.2 vlan 端口配置命令

4.2.1 switchport access

命令

switchport access vlan <vlan-id>

no switchport access vlan

模式

接口配置模式

参数

vlan-id：端口的默认 VID，范围 2-4094。

缺省交换机中只有VLAN 1，所有端口都是VLAN1 的untagged成员。

描述

switchport access命令用来设置VLAN模式是ACCESS的二层接口为指定的VLAN。该命令只对VLAN模式是ACCESS模式的二层接口有效。设置此命令后，此二层接口的PVID是指定的VLAN，此二层接口只属于指定的VLAN的UNTAG成员。

no switchport access vlan命令把该接口的access vlan回复到缺省VLAN，即VLAN1。此命令设置后，此接口的pvid改为1，并且只属于VLAN1的untagged成员。

举例

#将端口 ge1/1 配置为 vlan2 的 untagged 端口：

Switch(config-ge1/1)#switchport access vlan 2

4.2.2 switchport hybrid allowed vlan add

命令

switchport hybrid allowed vlan add <vlan-list> egress-tagged { disable | enable}

模式

接口配置模式

参数

vlan-list：加入 vlan 的 vlan 号，范围 1-4094。

描述

switchport hybrid 命令用来把端口加入到指定的一个或多个 VLAN 中，如果是 egress-tagged enable，则是 TAG 成员，如果是 egress-tagged disable，则是 UNTAG 成员。

<vlan_list>有两种表达方式，一种是以逗号分开的多个 VLAN 号，如 1,3,5,10，另一种是一个 VLAN 范围，如 2-10，但两种方式不能同时存在。

表达方式 1,3-5 是错误的（，和-只能存在一种），2-4，6-7 也是错误的（-只能存在一次）。

举例

#将端口 ge1/1 设置为 vlan1-3 的 tagged 端口：

Switch(config-ge1/1)#switchport mode hybrid

Switch(config-ge1/1)#switchport hybrid allowed vlan add 1-3 egress-tagged enable

Switch(config-ge1/1)#

4.2.3 switchport hybrid allowed vlan all

命令

switchport hybrid allowed vlan all

模式

接口配置模式

参数

无

描述

switchport hybrid allowed vlan all 命令只对 hybrid 模式的二层接口有效。该接口加入到所有的 VLAN 中（VLAN1 除外），是所有的 VLAN 的 tagged 成员。以后新创建 VLAN 时，该端口也会加入到新 VLAN 中，是该 VLAN 的 TAG 成员。执行此命令后，原来该端口是属于激活 vlan 的 UNTAG 成员会变为 TAG 成员。

举例

#将端口 ge1/1 设置为 vlan1 的 untagged 成员，所有其它 vlan 的 tagged 成员:

Switch(config-ge1/1)#switchport mode hybrid
Switch(config-ge1/1)#switchport hybrid allowed vlan all

4.2.4 switchport hybrid allowed vlan none

命令

switchport hybrid allowed vlan none

模式

接口配置模式

参数

无

描述

此命令只对 hybrid 模式的二层接口有效。该接口不再是所有的 VLAN 的成员（VLAN1 除外）。执行此命令后，该端口的 native vlan 会恢复为 1。

举例

#端口 ge1/1 原是 vlan1 的 tagged 端口，vlan2、vlan3 的 untagged 端口，vid=2；将 ge1/1 从 vlan1 外的 vlan 删除:
Switch(config-ge1/1)#switchport hybrid allowed vlan none
执行该命令后，端口 ge1/1 是 vlan1 的 tagged 端口，vid=1。

4.2.5 switchport hybrid allowed vlan remove

命令

switchport hybrid allowed vlan remove <vlan-id>

模式

接口配置模式

参数

vlan-id：需移除的 vlan 号，范围 1-4094。

描述

此命令只对 hybrid 模式的二层接口有效。该接口不再是指定的一个或多个 VLAN 的成员。
如果指定的 VLAN 中有激活的 vlan，则 native vlan 恢复到 1。

举例

#将端口 ge1/1 从 vlan2 中删除：

Switch(config-ge1/1)#switchport hybrid allowed vlan remove 2

4.2.6 switchport hybrid vlan

命令

switchport hybrid vlan <vlan-id>

no switchport hybrid vlan

模式

接口配置模式

参数

vlan-id：加入的 vlan 的 vlan 号。

描述

此命令只对 hybrid 模式的二层接口有效。对于 hybrid 接口来说，把该接口的 native vlan 设置为指定的 VLAN。设置此命令后，此二层接口的 pvid 为指定的 VLAN，且该接口属于指定的 VLAN 的 untagged 成员（如果在设置此命令前，该端口已经属于该 VLAN 的 TAG 成员，则执行此命令后该端口继续保持为 TAG 成员，PVID 还是为指定的 VLAN）。

no switchport hybrid vlan 命令把该接口的 native vlan 恢复为缺省 VLAN（VLAN1）。执行此命令后，原来的 native vlan 删除（不再属于原来的 native vlan 的 UNTAG 或 TAG 成员），新的 native vlan 为 1，属于 VLAN1 的 UNTAG 成员（如果在执行此命令前，该端口已经是 VLAN1 的 TAG 成员，则执行此命令后继续保持为 VLAN1 的 TAG 成员），PVID 修改为 1。

举例

#配置端口 ge1/1 为 vlan2 的 untagged 成员，vlan1 的 tagged 成员，且 vid 为 2：

Switch(config-ge1/1)#switchport mode hybrid

Switch(config-ge1/1)#swi hybrid vlan 2

Switch(config-ge1/1)#switchport hybrid allowed vlan add 1 egress-tagged enable

4.2.7 switchport mode

命令

switchport mode { access | hybrid | trunk}

no switchport { access | hybrid | trunk}

模式

接口配置模式

参数

access：接口 vlan 模式为 access 模式。缺省为 access 模式。如果二层接口设置为 ACCESS 模式，该接口缺省为 VLAN1 的 UNTAG 成员，PVID 为 1。

hybrid：接口 vlan 模式为 hybrid 模式。如果接口设置为 HYBRID 模式，该接口缺省为 VLAN1 的 UNTAG 成员，PVID 为 1。

trunk：接口 vlan 模式为 trunk 模式。如果接口设置为 TRUNK 模式，该接口缺省为 VLAN1 的 TAG 成员，PVID 为 1。

描述

设置二层接口的 VLAN 模式，是 access、hybrid 或 trunk 中的一种。

no switchport 命令将接口模式恢复为缺省值，回到 access 模式，并且 access vlan 是 VLAN1。

举例

#设置端口 ge1/1 为 trunk 端口：

Switch(config-ge1/1)#switchport mode trunk

4.2.8 switchport trunk allowed vlan add

命令

switchport trunk allowed vlan add <vlan-list>

模式

接口配置模式

参数

vlan-id： 该接口加入的一个或多个 VLAN 号。VLAN ID 的范围是 1-4094。<vlan-id>有两种表达方式，一种是以逗号分开的多个 VLAN 号，如 1,3,5,10，另一种是一个 VLAN 范围，如 2-10，但两种方式不能同时存在。

描述

此命令只对 trunk 模式的二层接口有效。该接口加入到指定的一个或多个 VLAN 中，成为指定的 VLAN 的 tagged 成员。

举例

#端口 ge1/1 配置为 vlan1-10 的 tagged 成员：

Switch(config-ge1/1)#switchport trunk allowed vlan add 1-10

4.2.9 switchport trunk allowed vlan all

命令

switchport trunk allowed vlan all

模式

接口配置模式

参数

无

描述

此命令只对 trunk 模式的二层接口有效。该接口加入到所有的 VLAN 中（VLAN1 除外），是所有 VLAN 的 tagged 成员。以后新创建 VLAN 时，该端口也会加入到新 VLAN 中，是该 VLAN 的 TAG 成员。

举例

#端口 ge1/1 配置为所有 vlan 的 tagged 成员：

Switch(config-ge1/1)#switchport trunk allowed vlan all

4.2.10 switchport trunk allowed vlan none

命令

switchport trunk allowed vlan none

模式

接口配置模式

参数

无

描述

此命令只对 trunk 模式的二层接口有效。该接口不再是任何 VLAN 的成员（VLAN1 除外）。

举例

#将 trunk 端口 ge1/1 从 vlan1 外的其它 vlan 中删除：

Switch(config-ge1/1)#switchport trunk allowed vlan none

4.2.11 switchport trunk allowed vlan remove

命令

switchport trunk allowed vlan remove <vlan-list>

模式

接口配置模式

参数

vlan-list：将该接口删除的一个或多个 VLAN 号。VLAN ID 的范围是 1-4094。vlan-list 有两种表达方式，一种是以逗号分开的多个 VLAN 号，如 1,3,5,10，另一种是一个 VLAN 范围，如 2-10，但两种方式不能同时存在。

描述

此命令只对 trunk 模式的二层接口有效。该接口不再是指定的一个或多个 VLAN 的成员。

举例

#将端口 ge1/1 从 vlan 2、vlan3 中删除：

Switch(config-ge1/1)#switchport trunk allowed vlan remove 2,3

4.2.12 vlan classifier activate

命令

vlan classifier activate <classifier group id>

vlan classifier group <classifier group id> {add | delete} rule <classifier rule id>

vlan classifier rule {ipv4 | mac } <classifier rule id> {<ipv4 address> | <mac address> } vlan <vlan id>

no vlan classification {activate | group< classifier group id > | rule< classifier rule id >}

模式

全局配置模式

参数

classifier group id：VLAN 组 id。范围，1~16。

classifier rule id：VLAN 规则 id。范围，1~1152。

ipv4 address：ip 地址，主要是指应用的网段。

vlan id：VLAN 的 id。

mac address：mac 地址。

描述

vlan classifier activate 命令激活基于 MAC 或 IP 的 VLAN 的配置。

vlan classifier group 命令配置基于 MAC 或 IP 的 VLAN 的组信息。

vlan classifier rule 命令配置基于 MAC 或 IP 的 VLAN 的规则信息。

no vlan classification 命令是删除基于 MAC 或 IP 的 VLAN 配置或取消激活。

举例

#配置基于 192.168.3.0 网段，VLAN 为 5 的的 VLAN 规则 1

Switch(config)#vlan classifier rule ipv4 1 192.168.3.1/24 vlan 5

#配置基于 MAC 0011.2233.4455，VLAN 为 3 的 VLAN 规则 129

Switch(config)#vlan classifier rule mac 129 0011.2233.4455 vlan 3

#把规则加入组集合

Switch(config)#vlan classifier group 1 add rule 1

Switch(config)#vlan classifier group 1 add rule 129

#激活一个组

Switch(config)#vlan classifier activate 1

#取消激活的 VLAN 组

Switch(config)#no vlan classifier activate

4.3 vlan 查看命令

4.3.1 show vlan

命令

show vlan [<vlan-id>]

模式

普通模式/特权模式

参数

vlan-id： 需显示的 vlan 号，范围 1－4094。

描述

显示 VLAN 的信息，包括 VLAN 中的端口的信息。指定 vlan id 时只显示指定 vlan 的信息。

举例

#查看当前 vlan 划分情况：

Switch>show vlan

```
VLAN    Name         State        Member ports ([u]-Untagged, [t]-Tagged)
----    --------     ---------    ------------------------------------------------
1       vlan1        active       [u]ge0/1 [u]ge0/2 [u]ge0/3 [u]ge0/4 [t]ge0/5
                                  [u]ge0/6 [u]ge0/7 [u]ge0/8 [u]ge0/9 [u]ge0/10
                                  [u]ge0/11 [u]ge0/12[u]ge1/1[u]ge1/2 [u]ge1/3
                                  [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8
                                 [u]ge1/9[u]ge1/10[u]ge1/11[u]ge1/12[u]ge1/13
                                [u]ge1/14[u]ge1/15[u]ge1/16[u]ge1/17[u]ge1/18
                                [u]ge1/19[u]ge1/20[u]ge1/21 [u]ge1/22[u]ge1/23
                                [u]ge1/24 [u]ge4/1 [u]ge4/2 [u]ge4/3 [u]ge4/4
                                [u]ge4/5 [u]ge4/6 [u]ge4/7 [u]ge4/8 [u]ge4/9
                                [u]ge4/10 [u]ge4/11 [u]ge4/12 [u]ge5/1 [u]ge5/2
                                [u]ge5/3 [u]ge5/4 [u]ge5/5 [u]ge5/6 [u]ge5/7
                                [u]ge5/8 [u]ge5/9 [u]ge5/10 [u]ge5/11 [u]ge5/12
2       vlan2        active       [t]ge0/5
3       vlan3        active       [t]ge0/5
4       vlan4        active       [t]ge0/5
34      vlan34       active       [t]ge0/5
Switch>
```

4.3.2 show vlan classifier

命令

show vlan classifier activation group [<classifier group id>]

show vlan classifier group [<classifier group id>]

show vlan classifier rule [<classifier rule id>]

模式

普通模式/特权模式

参数

classifier group id：VLAN 组 id。范围，1~16。

classifier rule id：VLAN 规则 id。范围，1~1152。

描述

show vlan classifier activation group 命令是显示当前已经激活的组。

show vlan classifier group 命令是显示当前配置的组信息。

show vlan classifier rule 命令是显示当前配置的规则信息。

举例

#显示规则

Switch#show vlan classifier rule

#显示组

Switch#show vlan classifier group

#显示激活的组

Switch#show vlan classifier activation group

第 5 章 QinQ 命令

5.1 配置命令

5.1.1 switchport link-type dot1q-in-q

命令

switchport link-type dot1q-in-q [customer {tpid} | service-provider {tpid}]
no switchport link-type dot1q-in-q

模式

接口配置模式

参数

customer：配置端口为 QinQ 用户端口。该端口用于连接接入设备的 tag 端口。对从这个端口接收的数据包，都加上一个 vlan tag，形成双 tag 包；vid 由端口 pvid 指定，tpid 由配置命令指定，默认为 0x8100。

service-provider：配置端口为 QinQ 服务商端口。该端口用于连接服务商网络。

该端口收发的数据包可以是带一个或两个 vlan tag。对于收到的数据包，若包的第一个 tag 中的 tpid 与端口 tpid 一致则不处理；若包的第一个 tag 中的 tpid 与端口 tpid 不一致则加上一个 vlan tag。

tpid：tag protocol identifier，标签协议标识符，由 vlan tag 的前两个字节指定。值可以是 0x8100 或 0x9100。不指定 tpid 时默认为 0x8100。

描述

将端口配置为 QinQ 端口。可指定任一物理端口或链路聚合端口为 QinQ 用户端口或服务商端口。

注意：一个 QinQ 链路上端口的 tpid 配置一定要一致。

举例

在一台设备上配置 QinQ 收发端口：

```
Switch(config)# interface ge5/1
Switch(config-ge5/1)#switchport link-type dot1q-in-q customer
Switch(config-ge5/1)#inter ge5/2
Switch(config-ge5/2)#switchport link-type dot1q-in-q service-provider
```

5.2 查看命令

5.2.1 show dot1q-in-q

命令

show dot1q-in-q

模式

普通模式/特权模式

参数

无

描述

显示 QinQ 端口配置。

举例

```
Switch#show dot1q-in-q
Interface            :ge5/1
Customer port(Q in Q)
EtherType for SPVLAN: 0x8100

Interface            :ge5/2
Service Provider port(Q in Q)
EtherType for SPVLAN: 0x8100
```

第 6 章 MSTP 命令

6.1 MSTP 配置命令

6.1.1 spanning-tree mst cisco-interoperability

命令

spanning-tree mst cisco-interoperability {disable | enable}

模式

全局配置模式

参数

disable：关闭功能。默认关闭。

enable：打开功能。

描述

启动或关闭和 cisco 的生成树协议的兼容。

联想天工网络交换机采用基于 802.1s 的 MSTP 协议，每个 MSTI 消息的长度是 16 个字节；而 CISCO 交换机的 BPDU 每个 MSTI 消息的长度是 26 个字节。为了和 CISCO 交换机户用，配置联想天工网络的交换机时要启动和 CISCO 兼容的开关。

举例

无。

6.1.2 spanning-tree mst configuration

命令

spanning-tree mst configuration

模式

全局配置模式

参数

无

描述

进入 spanning-tree 的配置模式。

举例

无。

6.1.3 spanning-tree mst enable

命令

spanning-tree mst enable

模式

全局配置模式

参数

无

描述

启动 mstp 计算。

举例

无。

6.1.4 spanning-tree mst errdisable-timeout

命令

spanning-tree mst errdisable-timeout {enable | interval <seconds>}
no spanning-tree mst errdisable-timeout {enable | interval}

模式

全局配置模式

参数

seconds：超时时间，范围 10-1000000 秒。默认 300 秒。

描述

spanning-tree mst errdisable-timeout enable 命令启动 errdisable 机制，当启动 BPDU gurad 的端口收到 BPDU 时，会启动 errordisable timer。errordisable 会在系统配置的超时时间后重新启动这个端口。

spanning-tree mst errdisable-timeout interval 命令设置 errordisable 超时时间。

no spanning-tree mst errdisable-timeout 命令用来取消相应配置，恢复默认值。

举例

无。

6.1.5 spanning-tree mst forward-time

命令

spanning-tree mst forward-time <seconds>

no spanning-tree mst forward-time

模式

全局配置模式。

参数

seconds：端口从 discarding 到 learning 以及 learning 到 forwarding 等待的秒数。范围 4-30 秒。默认 15 秒。

根据生成数协议 forward-time 必须满足下列条件：

2*(forward-time – 1) >= max-age。

描述

spanning-tree mst forward-time 命令用来配置转发延迟时间。

no spanning-tree mst forward-time 命令用来取消转发延时配置，恢复默认值。

举例

无。

6.1.6 spanning-tree mst hello-time

命令

spanning-tree mst hello-time <seconds>

no spanning-tree mst hello-time

模式

全局配置模式

参数

seconds：根交换机产生配置信息的间隔时间。范围 1-10 秒。默认 2 秒。

根据生成数协议 hello-time 必须满足下列条件：

2*(hello-time + 1) =< max-age。

描述

spanning-tree mst hello-time 配置 MSTP hello 报文发送间隔时间。

no spanning-tree mst hello-time 命令取消配置，恢复默认值。

举例

#配置 hello 报文发送间隔为 10 秒：

Switch(config)#spanning-tree mst hello-time 10

6.1.7 spanning-tree mst max-age

命令

spanning-tree mst max-age <seconds>

no spanning-tree mst max-age

模式

全局配置模式

参数

seconds：交换机在触发一个重新配置前，等待接收生成树配置信息的秒数。范围 6-40 秒。默认 20 秒。

描述

配置侦听根桥的最大时间。

no 命令取消配置，恢复默认值。

举例

无。

6.1.8 spanning-tree mst max-hops

命令

spanning-tree mst max-hops <hops>

no spanning-tree mst max-hops

模式

全局配置模式

参数

hops：在一个域中在 BPDU 被丢弃前指定的跳数。范围 1-40。默认 20 跳。

描述

配置 BPDU 协议包有效的最大跳数。

no 命令取消配置，恢复默认值。

举例

无。

6.1.9 spanning-tree mst portfast

命令

spanning-tree mst portfast

no spanning-tree mst portfast

模式

接口配置模式

参数

无

描述

spanning-tree mst portfast 命令配置一个端口为 portfast 端口，可使端口从 blocking 状态到 forwarding 状态，绕过 listening 和 learning 状态。

no 命令取消配置，恢复默认值。

举例

#配置端口 ge1/1 为 portfast 接口：

Switch(config-ge1/1)#spanning-tree mst portfast

6.1.10 spanning-tree mst portfast bpdu-filter

命令

spanning-tree mst portfast bpdu-filter [default | disable | enable]

no spanning-tree mst portfast bpdu-filter

模式

全局配置模式/接口配置模式

参数

default：默认状态。

disable：关闭功能。

enable：启用功能。

描述

防止 portfast 端口接收或发送 BPDU。

在全局配置模式，spanning-tree mst portfast bpdu-filter 命令启动在 portfast bpdu-filter default 状态的端口的 BPDU filtering 功能。在接口配置模式，spanning-tree mst portfast bpdu-filter enable 在任意端口打开 BPDU filter。

no 命令取消配置，恢复默认值。

举例

#配置端口 ge1/1 为 portfast 接口，且不发送 mstp bpdu 包：

Switch(config-ge1/1)#spanning-tree mst portfast

Switch(config-ge1/1)#spanning-tree mst portfast bpdu-filte enable

6.1.11 spanning-tree mst portfast bpdu-guard

命令

spanning-tree mst portfast bpdu-guard [default | disable | enable]

no spanning-tree mst portfast bpdu-guard

模式

全局配置模式/接口配置模式

参数

default：默认状态。

disable：关闭功能。

enable：启用功能。

描述

当配置了 BPDU gurad 的端口收到 BPDU 时，spanning tree 会 shutdown 这个的端口。在一个有效的配置，Port Fast-enabled 的端口不接收 BPDU。在一个 portfast enabled 的端口接收到一个 BPDU 表示一个无效的配置，例如是一个未授权设备的连接，BPDU guard 进入到一个 error-disabled 状态。

no 命令取消配置，恢复默认值。

举例

#配置端口 ge1/1 为 portfast 接口，启用 BPDU 保护功能：

Switch(config-ge1/1)#spanning-tree mst portfast

Switch(config-ge1/1)#spanning-tree mst portfast bpdu-guard enable

6.1.12 spanning-tree mst priority

命令

spanning-tree mst priority <value>

模式

全局配置模式

参数

value：CIST bridge 的优先级，范围 0-61440，默认值为 32768。CIST 优先

级的值只能是 4096 的倍数。

描述

配置桥优先级。桥优先级低的设备更有可能成为根桥。

举例

#配置 CIST 桥优先级为 36862：

Switch#configure terminal

Switch(config)#spanning-tree mst priority 36862

6.1.13 instance

命令

instance <instance-id> [priority <value> | vlan <vlan-id>]

no instance <instance-id> [vlan <vlan-id>]

模式

MSTP 配置模式

参数

instance-id：要创建的实例号，范围 1-15。

value：优先级的值，范围 0-61440，粒度 4096。默认值为 32768。

vlan-id：添加到实例的 vlan 号。

描述

instance <instance-id>命令创建实例。

instance <instance-id> priority <value>命令配置 MSTI bridge 的优先级。

instance <instance-id> vlan <vlan-id>命令添加实例 vlan。

no instance <instance-id>命令删除实例。

no instance <instance-id> vlan <vlan-id>命令删除 vlan 与实例的关联。

举例

#创建 MSTP 实例 2，添加 vlan2、vlan3：

Switch(config-mst)#instance 2

Switch(config-mst)#instance 2 vlan 2

Switch(config-mst)#instance 2 vlan 3

6.1.14 region

命令

region <region-name>

no region

模式

MSTP 配置模式

参数

region-name：MSTP 域的域名，长度 1－32 个字符。

no 命令取消域名配置。

描述

配置域名。

举例

无。

6.1.15 revision

命令

revision <revision-num>

模式

MSTP 配置模式

参数

revision-num：修订版本号，范围 0-255。

描述

配置修订版本号。

举例

无。

6.1.16 spanning-tree mst force-version

命令

spanning-tree mst force-version <version>

no spanning-tree mst force-version

模式

接口配置模式

参数

version：协议的类型，范围 0-3，0 代表 STP 协议，1 代表不支持生成树，2

代表 RSTP 协议，3 代表 MSTP 协议。默认协议类型为 0。

描述

配置发送协议包的类型。

no 命令取消配置，恢复默认值。

举例

#配置端口 ge1/1 发送 stp 协议包：

Switch(config-ge1/1)# spanning-tree mst force-version 0

6.1.17 spanning-tree mst guard root

命令

spanning-tree mst guard root

no spanning-tree mst guard root

模式

接口配置模式

参数

无

描述

配置启动 root guard 功能，不接收桥优先级比自己高的 BPDU 包，指定该交换机为根交换机。默认关闭。

no 命令取消配置，恢复默认值。

举例

无。

6.1.18 spanning-tree mst instance

命令

spanning-tree mst instance <instance-id> [path-cost <cost> | priority <value>]

no spanning-tree mst instance <instance-id> [path-cost <cost>]

模式

接口配置模式

参数

instance-id：实例号。范围 1－15。

cost：路径开销值，范围 1-200000000。较低的路径开销更可能成为根。默认值 20000000。

priority <value>：MSTI 优先级的值，范围 0-240，只能是 16 的倍数。优先级值较低的更可能成为根。

描述

spanning-tree mst instance <instance-id>命令把接口加入实例。

spanning-tree mst instance <instance-id> path-cost <cost>命令设置 msti 路径开销。

spanning-tree mst instance <instance-id> priority <value>命令设置 msti 优先级。

no 命令取消配置，恢复默认值。

举例

#把端口 ge1/1 加入到实例 2，并配置端口的路径开销为 10，优先级为 160：

```
Switch(config-ge1/1)#spanning-tree mst ins 2 path-cost 10
Switch(config-ge1/1)#spanning-tree mst ins 2 priority 160
Switch#sh spanning-tree mst ins 2 inter ge1/1
%     ge1/1: Port 2001 - Id 87d1 - Role Disabled - State Forwarding
%     ge1/1: Designated Internal Path Cost 0    - Designated Port Id 0
%     ge1/1: Configured Internal Path Cost 10
%     ge1/1: Configured CST External Path cost 20000000
%     ge1/1: CST Priority 128    - MSTI Priority 160
%     ge1/1: Designated Root 0000000000000207
%     ge1/1: Designated Bridge 0000000000000207
%     ge1/1: Message Age 0 - Max Age 0
%     ge1/1: Hello Time 0 - Forward Delay 0
%     ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

6.1.19 spanning-tree mst link-type

命令

spanning-tree mst link-type { point-to-point | shared}

no spanning-tree mst link-type

模式

接口配置模式

参数

point-to-point：连接类型为点到点，允许端口状态快速转换。为默认类型。

shared：连接类型为共享，不允许端口状态快速转换，要经过 802.1D 的计算过程来确定端口的状态。。

描述

配置接口的连接类型。

no 命令取消配置，恢复默认值。

举例

无。

6.1.20 spanning-tree mst path-cost

命令

spanning-tree mst path-cost <cost>

no spanning-tree mst path-cost

模式

接口配置模式

参数

cost：cist 路径开销值，范围 1-200000000。默认值 20000000。较低的路径开销更可能成为根。

下面是带宽和路径花消映射表：

带宽(bps)	路径花消
100,000(100K)	200000000
1,000,000(1M)	20000000
10,000,000(10M)	2000000
100,000,000(100M)	200000
1,000,000,000(1G)	20000
10,000,000,000(10G)	2000
100,000,000,000(100G)	200
1,000,000,000,000(1T)	20
>1000000000000	2

描述

配置 cist 路径开销。

no 命令取消配置，恢复默认值。

举例

#配置实例 2 中端口 ge1/1 的 cist 路径开销为 200：

Switch(config-ge1/1)#spanning-tree mst path-cost 200

Switch#show spanning-tree mst instance 2 interface ge1/1

% ge1/1: Port 2001 - Id 87d1 - Role Disabled - State Forwarding

% ge1/1: Designated Internal Path Cost 0 - Designated Port Id 0

% ge1/1: Configured Internal Path Cost 20000000

% ge1/1: Configured CST External Path cost 200

% ge1/1: CST Priority 128 - MSTI Priority 128

% ge1/1: Designated Root 0000000000000207

% ge1/1: Designated Bridge 0000000000000207

% ge1/1: Message Age 0 - Max Age 0

% ge1/1: Hello Time 0 - Forward Delay 0

% ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

6.1.21 spanning-tree mst priority

命令

spanning-tree mst priority <value>

模式

接口配置模式

参数

value：cist 端口的优先级，范围 0-240，只能是 16 的倍数。默认值 128。

描述

配置接口的 cist 优先级。

举例

#配置实例 2 端口 ge1/1 的 cist 优先级为 240：

Switch(config-ge1/1)#spanning-tree mst priority 240

Switch#show spanning-tree mst instance 2 interface ge1/1

% ge1/1: Port 2001 - Id f7d1 - Role Disabled - State Forwarding

% ge1/1: Designated Internal Path Cost 0 - Designated Port Id 0

% ge1/1: Configured Internal Path Cost 10

% ge1/1: Configured CST External Path cost 20000000

% ge1/1: CST Priority 240 - MSTI Priority 160

% ge1/1: Designated Root 0000000000000207

% ge1/1: Designated Bridge 0000000000000207

% ge1/1: Message Age 0 - Max Age 0
% ge1/1: Hello Time 0 - Forward Delay 0
% ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

6.1.22 clear spanning-tree detected protocols

命令

clear spanning-tree detected protocols [interface <if-name>]

模式

特权模式

参数

if-name：需要复位 STP 协议侦察功能的端口。

描述

为了和 802.1D STP 协议的兼容，系统可以自动侦察对方系统运行的协议，根据对方运行的协议来决定这个端口运行的协议。clear spanning-tree detected protocols 命令复位这个协议协商的任务让它重新协商它和主机之间的协议。

举例

#关闭模块1端口1的STP协议侦察功能：
clear spanning-tree detected protocols interface ge1/1

6.2 MSTP 查看命令

6.2.1 show spanning-tree mst

命令

show spanning-tree mst [config | detail | instance <instance-id> [interface <if-name>] | interface <if-name>]

模式

普通模式/特权模式

参数

instance-id： 实例号，范围 0－15。
if-name：接口号。

描述

show spanning-tree mst 命令显示 cist 信息以及 vlan 和 instance 的对应表。

show spanning-tree mst config 命令显示 mstp 的配置信息。

show spanning-tree mst detail 命令显示 mstp 的详细信息，包括 cist 接口信息，实例信息和实例接口信息。

show spanning-tree mst instance <instance-id>命令显示一个实例的信息。

show spanning-tree mst instance <instance-id> interface <if-name>命令显示一个 cist 接口的信息。

show spanning-tree mst interface <if-name>：显示一个 msti 接口的信息。

举例

#显示 mstp 配置信息：

```
Switch#show spanning-tree mst config
%
%   MSTP Configuration Information for bridge 1 :
%----------------------------------------------------
%   Format Id          : 0
%   Name               : lenovo8800
%   Revision Level : 1
%   Digest             : 0xD042DCDBBC60C63B623C157F60A37A6F
%----------------------------------------------------
```

#显示实例 1 内接口 ge1/1 的 mstp 信息：

```
Switch#show spanning-tree mst instance 1 interface ge1/1
%    ge1/1: Port 2001 - Id 87d1 - Role Disabled - State Discarding
%    ge1/1: Designated Internal Path Cost 0    - Designated Port Id 0
%    ge1/1: Configured Internal Path Cost 20000000
%    ge1/1: Configured CST External Path cost 20000
%    ge1/1: CST Priority 128    - MSTI Priority 128
%    ge1/1: Designated Root 0000000000000000
%    ge1/1: Designated Bridge 0000000000000000
%    ge1/1: Message Age 0 - Max Age 0
%    ge1/1: Hello Time 0 - Forward Delay 0
%    ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

6.3 MSTP 调试命令

6.3.1 debug mstp

命令

debug mstp

no debug mstp

模式

特权模式。

参数

无。

描述

debug mstp 命令用来打开 mstp 协议相关的调试开关，将相关日志写入日志表中。

no debug mstp 命令关闭 mstp 的调试开关。

举例

#打开 mstp 调试开关

Switch#debug mstp

Switch#

6.3.2 debug mstp all

命令

debug mstp all

no debug mstp all

模式

特权模式。

参数

无。

描述

debug mstp all 命令用来打开所有 mstp 协议相关的调试开关，将相关日志写入日志表中。

no debug mstp all 命令关闭 mstp 的调试开关。

举例

#打开 mstp 协议所有调试开关：

Switch#debug mstp all
Switch#

6.3.3 debug mstp cli

命令

debug mstp cli
no debug mstp cli

模式

特权模式。

参数

无。

描述

debug mstp cli 命令用来打开 mstp 协议相关的命令调试开关，将相关日志写入日志表中。

no debug mstp cli 命令关闭 mstp 的命令调试开关。

举例

#打开 mstp 协议命令调试开关：
Switch#debug mstp cli
Switch#

6.3.4 debug mstp packet

命令

debug mstp packet [recv | send]
no debug mstp packet [recv | send]

模式

特权模式。

参数

无。

描述

debug mstp packet 命令用来打开 mstp 协议报文调试开关，将相关日志写入日志表中。

no debug mstp packet 命令用来关闭 mstp 的报文调试开关。

举例

#打开 mstp 协议报文接收调试开关：

Switch#debug mstp packet recv

Switch#

6.3.5 debug mstp protocol

命令

debug mstp protocol [detail]

no debug mstp protocol [detail]

模式

特权模式。

参数

无。

描述

debug mstp protocol 命令用来打开 mstp 协议报文调试开关，将相关日志写入日志表中。

no debug mstp protocol 命令用来关闭 mstp 的报文调试开关。

举例

#打开 mstp 协议详细调试开关：

Switch#debug mstp protocol detail

Switch#

6.3.6 debug mstp timer

命令

debug mstp timer [detail]

no debug mstp timer [detail]

模式

特权模式。

参数

无。

描述

debug mstp timer 命令用来打开 mstp 协议的定时器调试开关，将相关日志写

入日志表中。

no debug mstp timer 命令用来关闭 mstp 的定时器调试开关。

举例

#打开 mstp 协议定时器调试开关：

Switch#debug mstp timer detail

Switch#

第 7 章 EAPS 命令

7.1 配置命令

7.1.1 eaps control-vlan

命令

eaps control-vlan <ring-id> <vlan-id>

no eaps control-vlan <ring-id>

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

vlan-id：控制 vlan ID 号，范围 2-4094。

描述

配置指定的 EAPS 环的控制 vlan。控制 vlan 只用于传输 EAPS 协议包，只能包含 primary port 和 secondary port 两个端口。

no 命令删除控制 vlan 配置。

举例

配置 EAPS 环 1 的控制 vlan 为 vlan2：

Switch(config)#eaps control-vlan 1 2

7.1.2 eaps create

命令

eaps create <ring-id>

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

描述

创建一个指定 ID 号的 EAPS 环。

举例

创建 EAPS 环 1：

Switch (config)#eaps create 1

7.1.3 eaps disable

命令

eaps disable <ring-id>

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

描述

关闭指定 ID 号的 EAPS 环。关闭后配置保留。

举例

关闭 EAPS 1：

Switch(config)#eaps disable 1

7.1.4 eaps enable

命令

eaps enable <ring-id>

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

描述

使能指定 ID 号的 EAPS 环。

举例

使能 EAPS 1：

Switch(config)#eaps enable 1

7.1.5 eaps extreme-interoperability

命令

eaps extreme-interoperability <ring-id> {disable | enable}

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

描述

配置指定 ID 号的 EAPS 环是否兼容 Extreme 设备。若选择兼容模式，协议包将按照与 Extreme 设备相同的方式封装。若选择不兼容模式，协议包按照 RFC3619 指定的方式封装。

默认打开 Extreme 兼容模式。

举例

关闭 EAPS 环 1 与 Extreme 设备的兼容：

Switch(config)#eaps extreme-interoperability 1 disable

7.1.6 eaps fail-time

命令

eaps fail-time <ring-id> <fail-time>

no eaps fail-time <ring-id>

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

fail-time：环失败时间，范围 2-65535 秒，默认为 3 秒。

描述

配置指定 EAPS 环的环失败时间。若在 fail-time 时间内没有收到 Health 包则认为环已断开，会将 Master node 的 secondary port 打开。在一个 EAPS 环中，只有 Master node 的该配置生效。

no 命令将 fail-time 恢复为默认设置。

举例

配置 EAPS 1 的 fail-time 为 9 秒：

Switch(config)#eaps fail-time 1 9

7.1.7 eaps hello-time

命令

eaps hello-time <ring-id> <hello-time>

no eaps hello-time <ring-id>

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

Hello-time：Master node 发出 Health 包的间隔时间，范围 1-65535 秒，默认为 1 秒。

描述

配置 EAPS 的 health 包发出的间隔时间。在一个 EAPS 环中，只有 Master node 的该配置生效。配置条件：hello-time < fail-time。

no 命令将 hello-time 恢复为默认设置。

举例

配置 EAPS 1 发出 Health 包的间隔为 6 秒：

Switch(config)#eaps hello-time 1 6

7.1.8 eaps mode

命令

eaps mode <ring-id> {master | transit}

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

描述

配置设备在指定 EAPS 环中的角色，master 负责检查环路完整性和阻塞端口防止环路。一个 EAPS 环中只能有一个 master，可有多个 transit。

举例

配置设备在 EAPS 1 中的角色为 master：

Switch(config)#eaps mode 1 master

7.1.9 eaps primary-port

命令

eaps primary-port <ring-id> <if-name>

no eaps primary-port <ring-id>

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

if-name：端口名，可以是物理端口和链路聚合端口。

描述

配置设备的 EAPS 环主端口。主端口必须是 tag 端口，是控制 vlan 和保护 vlan 的 tag 成员。

no 命令删除指定环的 primary 端口。

举例

指定 EAPS 1 的主端口为 ge1/1：

Switch(config)#eaps primary-port 1 ge1/1

7.1.10 eaps protected-vlan

命令

eaps protected-vlan <ring-id> <vlan-id>

no eaps protected-vlan <ring-id> <vlan-id>

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

vlan-id：该 EAPS 环的保护 vlan 的 ID 号。

描述

配置指定 EAPS 环的保护 vlan。EAPS 环可以防止其保护 vlan 形成环路。

no 命令删除指定 EAPS 环的指定保护 vlan。

举例

配置 EAPS 1 的保护 vlan 为 vlan3、vlan4：

Switch(config)#eaps protected-vlan 1 3

Switch(config)#eaps protected-vlan 1 4

7.1.11 eaps remove

命令

eaps remove <ring-id>

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

描述

删除指定 ID 号的 EAPS 环的配置。删除前要先关闭该 EAPS 环。

举例

删除 EAPS 1：

Switch(config)#eaps remove 1

7.1.12 eaps secondary-port

命令

eaps secondary-port <ring-id> <if-name>

no eaps secondary-port <ring-id>

模式

全局配置模式

参数

ring-id：EAPS 环的 ID 号，范围 1-16。

if-name：端口名，可以是物理端口和链路聚合端口。

描述

配置设备的 EAPS 域从端口。从端口必须是 tag 端口，是控制 vlan 和保护 vlan 的 tag 成员。

no 命令删除指定环的 secondary 端口。

举例

配置 EAPS 1 的从端口为 ge1/2：

Switch(config)#eaps secondary-port 1 ge1/2

7.2 查看命令

7.2.1 show eaps

命令

show eaps [<ring-id>]

模式

普通模式/特权模式

参数

ring-id：已配置的 EAPS 环的 ID 号，范围 1-16。

描述

不输入 ring-id 参数则显示当前已配置的 eaps 环个数和启用情况。

指定 ring-id 则显示该 eaps 环的具体情况。

举例

Switch#show eaps
eaps enable 1
eaps disable 2
Switch#show eaps 1
% EAPS Ring 1 - enable, Version 1, Mode - Master, State - Complete.
% Hello Time Interval - 1 secs, Current - on.
% Fail Time Age - 3 secs, Current - on.
% Pre-forwarding Time Age - 0 secs, Current - off.
% Primary Port - ge5/5, State - Forwarding.
% Secondary Port - ge5/6, State - Blocking.
% Extreme interoperability admin - on, oper - on.
% Bridge Id - 00:09:CA:88:03:06.
% Control Vlan ID - 2.
% Protected Vlan list - 1,3.
% Last LinkDown Bridge - 00:09:CA:77:02:C1.

7.3 调试命令

7.3.1 debug eaps

命令

debug eaps [all | events | packet [recv | send]]

no debug eaps [all | events | packet [recv | send]]

模式

特权模式

参数

all：打开所有 eaps 相关的调试开关。

events：打开 eaps 事件处理的调试开关。

packet：打开 eaps 协议包的调试开关。

recv：只打开接收 eaps 协议报文调试开关。

send：只打开发送 eaps 协议报文调试开关。

描述

debug eaps 命令用来打开 eaps 调试开关，使用户能够看到 eaps 事件处理和协议报文收发情况。

no debug eaps 命令用来关闭 eaps 调试开关。

举例

打开 eaps 协议包的调试开关：

Switch#debug eaps packet

Switch#log display

第 8 章 IGMP SNOOPING 命令

8.1 IGMP SNOOPING 配置命令

8.1.1 ip igmp snooping

命令

ip igmp snooping

no ip igmp snooping

模式

全局配置模式

参数

无

描述

ip igmp snooping 命令用来启动所有 vlan 的 igmp snooping 功能。

no ip igmp snooping 命令关闭所有 vlan 的 igmp snooping 功能。

举例

无。

8.1.2 ip igmp snooping fast-leave

命令

ip igmp snooping fast-leave vlan <vlan-id>

no ip igmp snooping fast-leave vlan <vlan-id>

模式

全局配置模式

参数

vlan-id：启动立即离开的 vlan 号。

描述

启动一个 vlan 的 IGMP V2 立即离开功能。

no 命令关闭一个 vlan 的 IGMP V2 立即离开功能。

举例

#启动 vlan2 的组播成员立即离开功能：

Switch(config)#ip igmp snooping fast-leave vlan 2

Switch(config)#

8.1.3 ip igmp snooping fast-leave-timeout

命令

ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>

no ip igmp snooping fast-leave-timeout vlan <vlan-id>

模式

全局配置模式

参数

interval：延时时间，单位 ms，范围无限制。默认为 300000 ms。

vlan-id：所配置的 vlan 的 vlan 号，范围 1－4094。

描述

设置一个 vlan 的组播成员立即离开延时时间，收到 leave 包后等待 interval 指定的时间才将成员删除。

no 命令取消立即离开延时设置，interval 恢复默认值。

举例

#配置 vlan1 收到组播成员的 leave 包后立即删除该成员：

Switch(config)#ip igmp snooping fast-leave vlan 1

Switch(config)#ip igmp snooping fast-leave-timeout 0 vlan 1

Switch(config)#

8.1.4 ip igmp snooping group-membership-timeout

命令

ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>

no ip igmp snooping group-membership-timeout vlan <vlan-id>

模式

全局配置模式

参数

interval：成员生存时间，单位 ms，范围无限制。默认 400000 ms。

vlan-id：所配置的 vlan 的 vlan 号，范围 1－4094。

描述

配置收到 report 包后加入的组播组的生存时间。

no 命令取消成员生存时间的配置，恢复默认值。

举例

#配置 vlan2 的组播成员生存时间为 600 秒：

Switch(config)#ip igmp snooping group-membership-timeout 600000 vlan 2
Switch(config)#

8.1.5 ip igmp snooping mrouter

命令

ip igmp snooping mrouter interface <if-name> [vlan <vlan-id>]
no ip igmp snooping mrouter interface <if-name> [vlan <vlan-id>]

模式

全局配置模式

参数

if-name：接口名。

vlan-id：接口所属 vlan 号。

描述

配置查询端口，其它端口收到收到组播加入离开包都会转发到该端口；该端口会加入组播组。

no 命令删除配置的查询端口。

举例

#配置端口 ge1/1 为 vlan2 的查询端口：

Switch(config)#ip igmp snooping mrouter interface ge1/1 vlan 2
Switch(config)#

8.1.6 ip igmp snooping query-membership-timeout

命令

ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>
no ip igmp snooping query-membership-timeout vlan <vlan-id>

模式

全局配置模式

参数

interval :查询端口的生存时间，单位 ms，范围 60000-300000ms。默认 300000

ms。

vlan-id：所配置的 vlan 的 vlan 号，范围 1－4094。

描述

配置收到 QUERY 包后加入的查询组的生存时间。

no 命令取消查询组生存时间的配置，恢复默认值。

举例

#配置 vlan2 的查询端口时间为 600 秒：

Switch(config)#ip igmp snooping query-membership-timeout 600000 vlan 2

Switch(config)#

8.1.7 ip ip igmp snooping vlan

命令

ip igmp snooping vlan <vlan-id>

no ip igmp snooping vlan <vlan-id>

模式

全局配置模式

参数

vlan-id：vlan 号。

描述

启动一个 vlan 的 igmp snooping 功能，必须先执行 ip igmp snooping 后才能配置一个 vlan 的 igmpsnoop 功能。

no 命令关闭一个 vlan 的 igmp snooping 功能。

举例

#关闭 vlan3 的 igmp snooping 功能，其它 vlan 打开 igmp snooping 功能：

Switch(config)#no ip igmp snooping vl

Switch(config)#no ip igmp snooping vlan 3

Switch(config)#

8.1.8 ip igmp snooping explicit-tracking

命令

ip igmp snooping explicit-tracking vlan <vlan-id>

no ip igmp snooping explicit-tracking vlan <vlan-id>

模式

全局配置模式

参数

vlan-id：vlan 号。

描述

启动一个 vlan 的 igmp snooping explicit-tracking 功能。

no 命令关闭一个 vlan 的 igmp snooping explicit-tracking 功能。

举例

#打开 vlan1 的 igmp snooping explicit-tracking 功能

Switch(config)# ip igmp snooping explicit-tracking vlan 1

#关闭 vlan3 的 igmp snooping explicit-tracking 功能，：

Switch(config)#no ip igmp snooping explicit-tracking vlan 3

Switch(config)#

8.1.9 ip igmp snooping ssm-safe-reporting

命令

ip igmp snooping ssm-safe-reporting vlan <vlan-id>

no ip igmp snooping ssm-safe-reporting vlan <vlan-id>

模式

全局配置模式

参数

vlan-id：vlan 号。

描述

启动一个 vlan 的 igmp snooping ssm-safe-reporting 功能。

no 命令关闭一个 vlan 的 igmp snooping ssm-safe-reporting 功能。

举例

#打开 vlan1 的 igmp snooping ssm-safe-reporting 功能

Switch(config)# ip igmp snooping ssm-safe-reporting vlan 1

#关闭 vlan3 的 igmp snooping ssm-safe-reporting 功能，：

Switch(config)#no ip igmp snooping ssm-safe-reporting vlan 3

Switch(config)#

8.2 IGMP SNOOPING 查看命令

8.2.1 show ip igmp snooping

命令

show ip igmp snooping [fast-leave [vlan <vlan-id>] | fast-leave-timeout [vlan <vlan-id>] | forwarding-table | group-membership-timeout [vlan <vlan-id>] | interface [vlan <vlan-id>] | query-membership-timeout [vlan <vlan-id>] | vlan <vlan-id>]

模式

普通模式/特权模式

参数

fast-leave：显示立即离开功能的打开情况。

vlan <vlan-id>：显示指定 vlan 的配置。

fast-leave-timeout：显示立即离开延时时间的配置。

forwarding-table：显示组播转发表，包括组播组和对应的 vlan、端口。

group-membership-timeout：显示组成员生存时间配置。

interface：显示可使用的端口和 vlan 的关系。

query-membership-timeout：显示查询组生存时间配置。

vlan：显示指定 vlan 的 igmp snooping 配置。

描述

显示 igmp snooping 配置。

举例

#显示 vlan1 的 igmp snooping 配置：

```
Switch#show ip igmp snooping vlan 1
Bridge 1 VLAN 0:
IGMP Snooping is globally enabled
Bridge 1: VLAN 1
        IGMP Snooping is enabled
        IGMP Snooping fast-leave is enabled
        IGMP Snooping fast-leave-timeout is 300000 ms
        IGMP snooping query membership timeout is 300000 ms
        IGMP snooping group membership timeout is 400000 ms
Switch#
```

8.2.2 show ip igmp snooping age-table

命令

show ip igmp snooping age-table { group-membership | query-membership}

模式

普通模式/特权模式

参数

group-membership：显示成员组的 age 时间。

query-membership：显示查询组的 age 时间。

描述

显示组播组的 age 时间、所在端口的情况。

举例

#显示成员组的 age 时间：

```
Switch#show ip igmp snooping age-table group-membership
VLAN    Address                 Port       Seconds
3       239.255.255.250     ge1/2      340000 ms
Switch#
```

8.2.3 show ip igmp snooping mrouter

命令

show ip igmp snooping mrouter [interface <if-name> | vlan <vlan-id>]

模式

普通模式/特权模式

参数

interface <if-name>：显示指定端口能

vlan <vlan-id>：显示指定 vlan 的查询端口。

描述

显示查询端口信息。

举例

#显示 vlan3 的查询端口：

```
Switch#show ip igmp snooping mrouter vlan 3
```

```
Bridge              VLAN    Ports
---------------    ----- -----------------
                      1        3 ge1/2,
Switch#
```

8.2.4 show ip igmpv2

命令

show ip igmpv2 snooping statistics [vlan <vlan-id>]

模式

普通模式/特权模式

参数

vlan <vlan-id>：显示指定的 vlan 的情况。

描述

显示 igmpv2 协议包的统计数据。

举例

#显示 vlan1 的 igmpv2 协议包统计：

```
Switch#show ip igmpv2 snooping statistics vlan 1

IGMP-V2 Snooping Statistics: Bridge 1    VLAN default
  Total valid pkts rcvd : 0
  Total invalid pkts rcvd : 0
  Number of Reports rcvd : 0
  Number of Leaves rcvd : 0
  Number of Membership Queries rcvd : 0
  Number of Reports tx : 0
  Number of Leaves tx : 0
  Number of Group-Specific Queries tx : 0
  Number of General Queries tx : 0
Switch#
```

8.2.5 show ip igmp snooping explicit-tracking

命令

show ip igmp snooping explicit-tracking vlan <vlan-id>

模式

普通模式/特权模式

参数

vlan-id：vlan 号。

描述

显示一个 vlan 的 igmp snooping explicit-tracking 功能状态及明细。

举例

#显示 vlan1 的 igmp snooping explicit-tracking 功能

Switch#show ip igmp snooping explicit-tracking vlan 1

Switch#

8.2.6 show ip igmp snooping ssm-safe-reporting

命令

show ip igmp snooping ssm-safe-reporting vlan <vlan-id>

模式

普通模式/特权模式

参数

vlan-id：vlan 号。

描述

显示相关 vlan 的 igmp snooping ssm-safe-reporting 功能状态。

举例

#显示 vlan1 的 igmp snooping ssm-safe-reporting 功能状态

Switch#show ip igmp snooping ssm-safe-reporting vlan 1

8.2.7 show ip igmpv3

命令

show ip igmpv3 snooping statistics [vlan <vlan-id>]

模式

普通模式/特权模式

参数

vlan <vlan-id>：显示指定的 vlan 的情况。

描述

显示 igmpv3 协议包的统计数据。

举例

#显示 vlan1 的 igmpv3 协议包统计：

Switch#show ip igmpv3 snooping statistics vlan 1

8.3 IGMP SNOOPING 调试命令

8.3.1 debug igmp snooping

命令

debug igmp snooping [all] | [cli] | [events] | [packet] | [timer]

no debug igmp snooping [all] | [cli] | [events] | [packet] | [timer]

模式

特权模式。

参数

all：打开 igmp snooping 所有得调试开关。

cli：cli 命令提示。

events：打开 igmp snooping 时间调试开关。

packet：打开 igmp snooping 报文调试开关。

timer：打开 igmp snooping 定时器调试开关。

描述

debug igmp snooping 命令用来打开 igmp snooping 相关调试开关，使用户能够看到 igmp snooping 的相关事件和报文收发情况。

no debug igmp snooping 命令关闭对应的 igmp snooping 调试开关。

举例

#打开 igmp snooping 报文调试开关：

Switch#debug igmp snooping packet

Switch#

第 9 章 ACL 命令

9.1 ACL 配置命令

9.1.1 标准的 ACL 规则

命令

access-list {<group-id>} {permit | deny | remark} {<source-ip>}

模式

全局配置模式

参数

group-id：规则组号，范围：<1-99>|<1300-1999>。

permit：允许符合规则的数据包转发。

deny：禁止符合规则的数据包转发。

remark：给指定规则组添加注释。

source-ip：源IP，有三种输入方式：

1) A.B.C.D wildcard 可以控制来自一个网段的IP地址；

2) any 相当于A.B.C.D 255.255.255.255

3) host A.B.C.D相当于A.B.C.D 0.0.0.0

wildcard：反向掩码，决定哪些bits 需要匹配，’0’表示需要匹配，’1’表示不需要匹配。

描述

配置基于标准IP的ACL访问控制规则。这一类规则只是判断数据包的源IP地址是否匹配已经配置了的ACL 规则；如果匹配了根据deny/permit 作相应的处理。在所有的ACL规则中都有一条deny 所有IP包的隐藏规则，只要用户配置了一条ACL规则，系统会自动产生这条规则。因此用户不需要手动去deny any的配置。基于扩展IP规则和基于MAC地址规则也是如此。

举例

#配置一组规则，允许源地址为 192.168.0.0 网段的数据包转发，禁止源地址为 192.168.0.11 和其它地址的数据包转发：

Switch(config)#access-list 1 deny host 192.168.0.11

Switch(config)#access-list 1 permit 192.168.0.0 0.0.0.255

Switch(config)#access-list 1 deny any

9.1.2 扩展的 ACL 规则

命令

access-list {<group-id>} {permit | deny | remark} {protocol} {<source-ip>} [<source-port>] {<dest-ip>} [<type> | <dest-port>]

模式

全局配置模式

参数

group-id：规则组号，范围<100-199>|<2000-2699>。

permit：允许符合规则的数据包转发。

deny：禁止符合规则的数据包转发。

remark：给指定规则组添加注释。

protocol：在IP 层之上的协议类型，如：icmp，igmp，ospf，tcp，udp 等，也可以输入相应的数字，如6代表tcp。如果不需要对这些协议进行控制，可以输入ip 或(0)。

source-ip：源IP， 有三种输入方式：

1) A.B.C.D wildcard 可以控制来自一个网段的IP地址；

2) any 相当于A.B.C.D 255.255.255.255

3) host A.B.C.D相当于A.B.C.D 0.0.0.0

wildcard：决定哪些 bits 需要匹配，'0'表示需要匹配，'1'表示不需要匹配。

source-port：是对于 protocol 为 tcp 或 udp 的情况，可以控制数据包的源端口，输入方式可以是一些熟悉的端口服务名称，如：www，也可以是数字，如 80 代表 www 端口。

dest-ip：目的IP地址。有三种输入方式：

1) A.B.C.D wildcard 可以控制来自一个网段的IP地址；

2) any 相当于A.B.C.D 255.255.255.255

3) host A.B.C.D相当于A.B.C.D 0.0.0.0

type：是对于 protocol 为 icmp 或 igmp 的情况，可以控制消息类型，输入方式可以是消息类型名称，如 echo、leave，也可以是数字，如 8 代表 icmp echo 包。

dest-port：是对于protocol 为tcp 或udp的情况，可以控制数据包的目的端口，输入方式和srcPort 相同。

描述

配置一条扩展 ip 规则，匹配指定协议包，可根据数据包的源和目的 IP 地址、

消息类型或端口决定转发或丢弃。

举例

#配置规则禁止从 192.168.0.2 到 192.168.1.0 网段的 ip 包，允许 192.168.0.2 到 192.168.2.1 的 ospf 包：

Switch(config)#access-list 100 deny ip host 192.168.0.2 192.168.1.0 0.0.0.255

Switch(config)#access-list 100 permit ospf host 192.168.0.2 host 192.168.2.1

#配置一组规则，要实现10.1.0.0 255.255.0.0网段的地址不能访问任何的www服务器，但是10.1.1.1 不作上述的限制；可以作如下配置：

switch# access-list 200 deny tcp 10.1.0.0 0.0.255.255 any www

switch# access-list 200 permit tcp host 10.1.1.1 any www

9.1.3 字符类型的 ACL 规则

命令

access-list {<rule-name>} {permit | deny | remark} { <source-ip> }[exact-match]

模式

全局配置模式

参数

rule-name：规则名。

permit：允许符合规则的数据包转发。

deny：禁止符合规则的数据包转发。

remark：给指定规则组添加注释。

source-ip：源 IP，有两种输入方式：

1) A.B.C.D/M 需匹配的前缀，如 10.0.0.0/8

2) any 相当于 0.0.0.0/0

A.B.C.D/M 中 M 表示需要匹配的位数。

exact-match：精确匹配。如果配置 exact-match 相当于 host。

描述

配置一组以字符串命名的规则，只供路由协议调用。

举例

#配置一组名字为 room1 的规则，允许 172.16.2.0 网段的地址，禁止

172.16.2.1 的地址：

Switch(config)#access-list room1 deny 172.16.2.1/32 exact-match

Switch(config)#access-list room1 permit 172.16.2.0/24

9.1.4 基于 MAC 的 ACL 规则

命令

access-list <groupId> {deny | permit | remark} <source-mac> <destination-mac> <vlan-id> ip <protocol> <source-ip> <destination-ip>

模式

全局配置模式

参数

group-id：规则组号，范围 700~799。

permit：允许符合规则的数据包转发。

deny：禁止符合规则的数据包转发。

remark：给指定规则组添加注释。

source-mac：源 MAC。

destination-mac：目的 MAC。

vlan id：VLAN 序号。

protocol：在 IP 层之上的协议类型，如：icmp，igmp，ospf，tcp，udp 等，也可以输入相应的数字，如 6 代表 tcp。如果不需要对这些协议进行控制，可以输入 ip 或(0)。

source-ip：源 IP， 有三种输入方式：

1) A.B.C.D wildcard 可以控制来自一个网段的 IP 地址；

2) any 相当于 A.B.C.D 255.255.255.255

3) host A.B.C.D 相当于 A.B.C.D 0.0.0.0

wildcard：决定哪些 bits 需要匹配，’0’表示需要匹配，’1’表示不需要匹配。

dest-ip：目的 IP 地址。有三种输入方式：

1) A.B.C.D wildcard 可以控制来自一个网段的 IP 地址；

2) any 相当于 A.B.C.D 255.255.255.255

3) host A.B.C.D 相当于 A.B.C.D 0.0.0.0

描述

配置一条基于 MAC 的 ip 规则，匹配指定协议包，可根据数据包的源和目的 IP 地址、源和目的 MAC 及 VLAN ID 决定转发或丢弃。

举例

#配置规则禁止从 MAC 地址为 0009.ca10.0907 且 192.168.0.2 到 192.168.1.0 网段的 VLAN2 的 TCP 包，允许 MAC 地址为 0009.ca12.67ce 且 192.168.0.3 到 192.168.2.1 的 VLAN3 的 igmp 包：

Switch(config)# access-list 700 deny mac 0009.ca10.0907 any 2 ip tcp host 192.168.0.2 192.168.1.0 0.0.0.255

Switch(config)# access-list 700 permit mac 0009.ca12.67ce mac any 3 ip igmp host 192.168.0.3 host 192.168.2.1

9.1.5 基于 MAC ARP 的 ACL 规则

命令

access-list <groupId> {deny | permit | remark} <source-mac> <destination-mac> <vlan-id> arp <arp-operation> <sender-mac> <sender-ip>

模式

全局配置模式

参数

group-id：规则组号，范围 1100~1199。

permit：允许符合规则的数据包转发。

deny：禁止符合规则的数据包转发。

remark：给指定规则组添加注释。

source-mac：源 MAC。

destination-mac：目的 MAC。

vlan-id：VLAN 序号。

arp-operation：arp 协议包操作类型。

sender-mac：发送者的 MAC 地址。

sender-ip：发送者的 IP 地址。

描述

配置一条基于 MAC ARP 的 ACL 规则，匹配指定协议包，可根据数据包的源 IP 地址、源 MAC 及 VLAN ID 等决定转发或丢弃。

举例

#配置 ACL 规则 id 为 1100，允许 mac 源地址 0009.ca10.1122，VLAN ID 为 2，源 IP 为 192.168.0.10。

Switch(config)# access-list 1100 permit mac 0009.ca10.1122 any 2 arp any

192.168.0.10 0009.ca10.1122 host 192.168.0.10

9.1.6 access-group

命令

access-group <group-id>

模式

接口配置模式

参数

group-id：引用的规则组号，标准 IP 规则范围<1-99>|<1300-1999>，扩展 IP 规则范围<100-199>|<2000-2699>。

描述

在端口引用一组 acl 规则。

举例

#在端口 ge1/1 引用规则组 1：

Switch(config-ge1/1)#access-group 1

9.1.7 删除 ACL 规则

命令

no access-list {<group-id> | <access-list name>}

模式

全局配置模式

参数

group-id：规则组号。

access-list name：acl 规则名字。

描述

删除配置的 ACL 规则。

举例

#删除 ACL 规则 1：

Switch(config)# no access-list 1

9.2 ACL 查看命令

9.2.1 show access-group

命令

show access-group

模式

普通模式/特权模式

参数

无

描述

显示 acl 规则的引用情况。

举例

#Switch#show access-group
Interface ge1/1
access-list 100 is set

9.2.2 show access-list

命令

show access-list [<group-id>]

模式

特权模式

参数

group-id：要显示的规则号。

描述

显示配置的 acl 规则。

举例

#显示 ACL 配置信息
Switch#show access-list

Standard IP access list 1, Remark acl1
deny 192.168.1.0, wildcard bits 0.0.0.255
permit any

Extended IP access list 100,

permit ospf host 192.168.0.2 host 192.168.2.1

permit ip host 192.168.0.2 192.168.1.0 0.0.0.255

Switch#

第 10 章 QoS 命令

10.1 QOS 配置命令

10.1.1 qos class

命令

qos class <class id> match {acl <acl id>| cos<cos value> | dscp<dscp value> | ip-precedence<ip-precedence value>}

qos class <class id> name <class name>

no qos class <class id>

模式

全局配置模式

参数

class id：class 序号。范围：1~1000。

acl id：access-list 序号。

cos value：cos 数值，范围：0~7。

dscp value：dscp 数值，范围：0~63。

ip-precedence value：ip-precedence value 数值，范围：0~7。

class name：class 引用的标识名。长度：1~32。

描述

qos class 命令是配置 qos 使用的 class 中的参数及名字。

no qos class 命令是删除指定的 qos class。

举例

#配置名字为 private，id 为 1，引用 DSCP 值为 10,20,30 的 class：

Switch(config)#qos class 1 match dscp 10 20 30

Switch(config)#qos class 1 name private

#删除一个 qos class 1

Switch(config)#no qos class 1

10.1.2 qos cos-dscp

命令

qos cos-dscp <cos value> <internal dscp>

模式

全局配置模式

参数

cos value：cos 值。范围：0~7。

internal dscp：内部 dscp 值，范围：0~63。

描述

qos cos-dscp 命令是配置 cos 与内部 dscp 值的映射表。

举例

#配置 cos 值 1 对应内部 dscp 值 48。

Switch(config)#qos cos-dscp 1 48

10.1.3 qos dscp-dscp

命令

qos dscp-dscp <dscp value > < internal dscp value >

模式

全局配置模式

参数

dscp value：dscp 值。范围：0~63。

internal dscp value：内部 dscp 值，范围：0~63。

描述

qos dscp-dscp 命令是配置 dscp 与内部 dscp 的映射表。

举例

#配置引用的 dscp 值 1 对应内部 dscp 值 48。

Switch(config)#qos dscp-dscp 1 48

10.1.4 qos interdscp-queue

命令

qos interdscp-queue < internal dscp value > <output queue id>

模式

全局配置模式

参数

internal dscp value：内部 dscp 值，范围：0~63。

output queue id：调度队列 id。范围：1~8。

描述

qos interdscp-queue 命令是配置内部的 dscp 与调度队列的映射表。

举例

#配置内部的 dscp 值 1 对应调度队列 8。

Switch(config)# qos interdscp-queue 1 8

10.1.5 qos policy

命令

qos policy <policy id> class <class id> set {cos<cos value> |dscp<dscp value> | ip-precedence<ip-precedence value>}

qos policy <policy id> class <class id> meter <bandwidth> <burstsize>

qos policy <policy id> name <policy name >

no qos policy <policy id> [class <class id>[meter]]

模式

全局配置模式

参数

policy id：policy 序号，范围：1~256。

class id：class 序号。范围：1~1000。

cos value： cos 数值，范围：0~7。

dscp value：dscp 数值，范围：0~63。

ip-precedence value：ip-precedence value 数值，范围：0~7。

bandwidth：可提供限制的带宽。范围：0~1048512

burstsize：单个 burst 的大小。范围：0~512

policy name：policy 引用的标识名。长度：1~32。

描述

qos policy 命令是配置 qos 策略中的参数及名字。

no qos policy 命令是删除 qos 相关策略。

举例

#配置 qos 策略 id 为 1 ，名字为 private，引用 class 1,指定 cos 为 7，限制带宽为 64kbps,burstsize 为 512kbytes/s。

Switch(config)# qos policy 1 class 1 set cos 7

Switch(config)#qos policy 1 class 1 meter 64 512

Switch(config)#qos policy 1 name private

#删除 qos 策略 1。

Switch(config)#no qos policy 1

10.1.6 qos prec-dscp

命令

qos prec-dscp <ip precedence value> <internal dscp value>

模式

全局配置模式

参数

ip-precedence value：ip-precedence value 数值，范围：0~7。

internal dscp value：内部 dscp 值，范围：0~63。

描述

qos prec-dscp 命令是配置 ip precedence 与内部 dscp 的映射表。

举例

#配置引用的 ip precedence 值 1 对应内部 dscp 值 48。

Switch(config)#qos prec-dscp 1 48

10.1.7 qos schedule

命令

qos schedule {rr |spq | wrr<queue weight>}

模式

接口配置模式

参数

queue weight：调度队列权重，范围：1~15；

rr：循环调度；

spq：严格优先级调度；

wrr：加权循环调度。

描述

qos schedule 命令是配置端口的调度规则及队列比重。

举例

#配置 1/1 端口为 wrr 模式，且队列比重为 1 2 3 4 5 6 7 8 。

Switch(config-ge1/1)#qos schedule wrr 1 2 3 4 5 6 7 8

10.1.8 qos service-policy

命令

qos service-policy <policy id>

模式

接口配置模式

参数

policy id：策略 ID，范围：1~256。

描述

qos service-policy 命令是配置端口启用 qos 策略。

举例

#配置 1/1 端口启用 qos 策略 1 。

Switch(config-ge1/1)#qos service-policy 1

10.1.9 qos trust

命令

qos trust {cos | dscp | ip-precedence}

模式

接口配置模式

参数

无

描述

qos trust 命令是配置端口成为 qos 信任端口。

举例

#配置 1/1 端口成为 qos 信任 dscp 端口 。

Switch(config-ge1/1)#qos trust dscp

10.2 QOS 查看命令

10.2.1 show qos

命令

show qos

模式

普通模式/特权模式

参数

无

描述

show qos 命令是显示目前 qos 在端口上配置信息。

举例

#显示目前 qos 配置信息 ：

Switch# show qos

10.2.2 show qos class

命令

show qos class [class id]

模式

普通模式/特权模式

参数

class id：class 序号。范围：1~1000。

描述

show qos class 命令是用来显示目前配置的 class。

举例

#显示目前配置的 class:

Switch#show qos class

10.2.3 show qos cos-dscp

命令

show qos cos-dscp

模式

普通模式/特权模式

参数

无

描述

show qos cos-dscp 命令是用来显示目前配置的 cos-dscp 映射表。

举例

#显示目前配置的 cos-dscp 映射表:

Switch#show qos cos-dscp

10.2.4 show qos dscp-dscp

命令

show qos dscp-dscp

模式

普通模式/特权模式

参数

无

描述

show qos dscp-dscp 命令是显示当前 DSCP-DSCP 的映射表。

举例

#显示当前 qos 中 dscp-dscp 的映射表:

Switch#show qos dscp-dscp

10.2.5 show qos interdscp-queue

命令

show qos interdscp-queue

模式

普通模式/特权模式

参数

无

描述

show qos interdscp-queue 命令是显示当前 DSCP-QUEUE 映射表。

举例

#显示当前 DSCP-QUEUE 映射表:

Switch#show qos interdscp-queue

10.2.6 show qos policy

命令

show qos policy [policy id]

模式

普通模式/特权模式

参数

policy id：policy 序号，范围：1~256。

描述

show qos policy 命令是显示 qos 所配置的策略。

举例

#显示 qos 策略 1；

Switch#show qos policy 1

10.2.7 show qos prec-dscp

命令

show qos prec-dscp

模式

普通模式/特权模式

参数

无

描述

show qos prec-dscp 命令是显示当前 PREC-DSCP 映射表

举例

#显示当前 PREC-DSCP 映射表

Switch#show qos prec-dscp

10.2.8 show qos schedule

命令

show qos schedule

模式

普通模式/特权模式

参数

无

描述

show qos schedule 命令是显示当前 qos 调度方法

举例

#显示当前 qos 调度方法

Switch#show qos schedule

第 11 章 IP 路由命令

11.1 配置命令

11.1.1 arp

命令

arp <ip-address> <mac-address> [if-name]

no arp {<ip-address> | <ip-prefix> | all |dhcp-relay | dynamic | static}

模式

全局配置模式

参数

ip-address：绑定的 IP 地址，用 32 位点分十进制表示；

mac-address：绑定的物理地址，用 48 位 16 进制表示；mac 地址，格式为 HHHH.HHHH.HHHH；

if-name：接口名，指定 IP 和 MAC 绑定的接口，该接口必须是二层接口；

ip-prefix：ip 前缀，使用 ip 地址/掩码形式，表示一个网络;

dynamic：动态学习的 arp 表项；

static：静态配置的或动态学习后转化为静态类型的 arp 表项。

描述

arp 命令用来配置静态 arp 表项，跟[if-name]参数时可以将 IP 和 MAC 与二层接口对应绑定，配置成功后该 IP 和 MAC 地址对应数据只能从指定的二层端口转发。

no arp 命令用来删除对应的 arp 表项或静态配置。

举例

#配置 ip 地址 192.168.1.1 与 MAC 地址 0003.0010.1011 映射

Switch(config)#arp 192.168.1.1 0003.0010.1011

Switch(config)#

#配置 IP 地址 192.168.8.3，MAC 地址为 0009.ca10.0011 的主机只能通过接口 ge5/4 上连：

Switch(config)#arp 192.168.8.3 0009.ca10.0011 ge5/4

Switch(config)#

11.1.2 arp lock

命令

arp lock <ip-prefix>

arp unlock {<ip-prefix> | all}

模式

全局配置模式

参数

ip-prefix：IP 地址段，格式 A.B.C.D/M。

all:所有网络。

描述

arp lock 命令用来锁住一个网段，执行该命令后，对应网段内所有动态 arp 表项被删除且不再学习新的 arp 表项。仅保留静态 arp 表项，且不会过期。

arp unlock 命令用来对对应网段进行解锁定。

举例

#对 172.20.0.0/16 网段上锁，不再学习新的 arp

Switch(config)#arp lock 172.20.0.0/16

Switch(config)#

11.1.3 arp query

命令

arp query <ip-address> [<interval>]

no arp query [<ip-address>]

模式

全局配置模式

参数

ip-address：IP 地址，32 位点分十进制表示，格式 A.B.C.D/M；

interval：发送 arp 请求的时间间隔，取值范围为 1～255，缺省值为 5 秒。

描述

arp query：命令用来配置指定 ip 地址对应的 arp 查询时间，配置后每隔指定的时间系统会发出指定 ip 的 arp 查询，以此更新对应的 arp 表项；

no arp query：命令用来删除 arp 查询时间的配置对 arp 表项操作。

举例

#通过配置指定 ip 地址 192.168.1.1 的 arp 更新时间为 3S：

Switch(config)#arp query 192.168.1.1 3
Switch(config)#

11.1.3 arp static

命令

arp static {<ip-prefix> | all}
no arp static

模式

全局配置模式

参数

ip-prefix：IP 地址段，格式 A.B.C.D/M。
all：所有的动态 arp 表项。

描述

arp static：命令用来将参数指定的范围内的动态 arp 转化位静态 arp 表项；
no arp static：命令用来删除静态 arp 表项。

举例

#将所有动态 arp 表项设置为静态表项：
Switch(config)#arp static all
Switch(config)#

11.1.4 ip address

命令

ip address <address/mask>
no ip address [<address/mask>]

模式

接口配置模式

参数

address/mask：ip 地址和掩码长度。取值范围 address：0.0.0.0～
223.255.255.255；mask：0～32。

描述

ip address：命令用来为一个三层接口配置IP地址。该命令目前只在三层接口（vlan）下有效。

no ip address命令用来删除接口上配置的IP地址。

举例

#配置接口 vlan4 的 ip 地址为 192.168.192.32，掩码长度为 24 位：

```
Switch#conf ter
Switch(config)#inter vlan24
Switch(config-vlan24)#ip addr 192.168.192.32/24
Switch(config-vlan24)#end
Switch#show ip interface vlan24 brief
Interface                  IP-Address          Status
Protocol
vlan24          192.168.192.32    up                  up
Switch#
```

11.1.5 ip prefix-list

命令

ip prefix-list <prefix-list> [seq <seq-num>] {deny | permit} {any | <ip-prefix> [ge <min-len> | le <max-len>]}

no ip prefix-list <prefix-list> [seq <seq-num>] {deny | permit} {any | <ip-prefix> [ge <min-len> | le <max-len>]}

模式

全局配置模式

参数

prefix-list：前缀列表名。

seq-num：前缀列表的序号。

deny：指定匹配模式为拒绝。

permit：指定匹配模式为允许。

any：拒绝/允许所有网络。

ip-prefix：指定拒绝/允许的网络。使用网络/掩码形式表示。

min-len：匹配的最小前缀长度，取值大于掩码长度。

max-len：匹配的最大前缀长度，取值大于或等于 min-len。

描述

ip prefix-list命令用来配置一条前缀列表。

no ip prefix-list命令用来删除一条前缀列表。

举例

#配置一条名为 limit，序号为 15 的前缀列表，拒绝 200.1.1.0/24 的网络：

Switch(config)#ip prefix-list limit seq 15 deny 200.1.1.0/24

Switch(config)#

11.1.6 ip route

命令

ip route {<ip-address>/<mask-length> | <ip-address> <mask>} <gateway > [<distance>]

no ip route {<ip-address>/<mask-length> | <ip-address> <mask>} [<gateway >]

模式

全局配置模式

参数

ip-address：目的 IP 地址，32 位点分十进制格式。

mask-length：掩码长度，十进制表示。

mask：IP地址的掩码，点分十进制格式。

gateway：指定路由的下一跳网关的IP 地址，点分十进制格式。

distance：协议优先级（管理距离）,缺省值为1。

描述

ip route命令用来配置静态路由，并可以根据distance参数的控制选路和实现路由的备份。

no ip route命令用来删除静态路由，在存在多条到达同一网络的路由时，不指定网关将删除所有与目的网络匹配的静态路由。

举例

#配置一条到 210.1.1.0/24 网段的路由，下一跳为 172.20.2.2，协议优先级为 33：

Switch#configure terminal

Switch(config)#ip route 210.1.1.0/24 172.20.2.2 33

#删除一条静态路由

Switch#configure terminal

Switch(config)#no ip route 210.1.1.0/24

Switch(config)#

11.1.7 match interface

命令

match interface <if-name>

no match interface [<if-name>]

模式

route-map 配置模式

参数

if-name：指定需要匹配的接口名。

描述

match interface命令用来配置一条以接口名为基础的匹配条件。

no match interface命令用来删除一条以接口名为基础的匹配条件。

举例

#配置一条规则，匹配条件为接口 vlan55

Switch(config-route-map)#match interface vlan55

Switch(config-route-map)#

11.1.8 match ip

命令

match ip {<ip-address> | <next-hope>} {<acl> | prefix-list <prefix-list>}

no match ip {<ip-address> | <next-hope>} [<acl> | prefix-list <prefix-list>]

模式

route-map 配置模式

参数

ip-address：指定需要匹配路由的 ip 地址。

next-hope：指定需要匹配路由的下一跳地址。

acl：匹配条件需要调用的 acl 规则。

prefix-list：匹配条件需要调用的前缀列表名。

描述

match ip命令用来配置一条以ip地址为基础的匹配条件。

no match ip命令用来删除一条以ip地址为基础的匹配条件。

举例

#配置一条规则，匹配条件为下一跳满足前缀列表 permitnext 的条件：

Switch(config-route-map)#match ip next-hop prefix-list permitnext

Switch(config-route-map)#

11.1.9 match metric

命令

match metric <metric>

no match metric [<metric>]

模式

route-map 配置模式

参数

metric：路由的花销。

描述

match metric命令用来配置一条以路由metric值为基础的匹配条件。

no match metric命令用来删除一条以路由metric值为基础的匹配条件。

举例

#配置一条规则，匹配条件为路由的 metric 值为 3：

Switch(config-route-map)#match metric 3

Switch(config-route-map)#

11.1.10 match route-type

命令

match route-type external {type-1 | type-2}

no match route-type external [type-1 | type-2]

模式

route-map 配置模式

参数

type-1：类型 1 的 ospf 外部路由。

type-2：类型 2 的 ospf 外部路由。

描述

match route-type external命令用来配置一条以路由类型为匹配条件的匹配

规则，该规则对ospf外部路由有效。

no match route-type external命令用来删除一条以路由类型为匹配条件的匹配规则。

举例

#配置一条规则，匹配条件为 ospf 类型 1 的路由：

Switch(config-route-map)#match match route-type external type-1

Switch(config-route-map)#

11.1.11 policy route

命令

policy route <vlan-id> <nextehop>

no policy route <vlan-id>

模式

配置模式

参数

vlan-id：使用策略路由的 vlan 号。

nextehop：策略路由的下一跳 ip 地址。

描述

policy route：命令用来配置一条策略路由，策略路由的下一跳需要有有效的缺省路由（即缺省路由配置正确，下一跳可达）与之对应；否则缺省路由不能生效。策略路由生效后，在数据对应接口收到数据包，不能匹配到详细路由时，自动调用策略路由，通过策略路由配置的下一跳转发数据包。策略路由失效时使用缺省路由转发，否则丢弃数据包。

no policy route命令用来删除一条策略路由。

举例

#配置一条策略路由，使 vlan24 收到的数据缺省时经过下一跳 192.168.100.2 转发：

Switch#ping 192.168.100.2 -n 2

PING 192.168.100.2: 56 data bytes

64 bytes from 192.168.100.2 : icmp_seq=0. time=5. ms

64 bytes from 192.168.100.2 : icmp_seq=1. time=0. ms

----192.168.100.2 PING Statistics----

2 packets transmitted, 2 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/2/5

Switch#

Switch(config)#ip route 0.0.0.0/0 192.168.100.2

Switch(config)#policy route 24 192.168.100.2

Switch(config)#end

Switch#show policy route

Policy route information:

  vlan id:24 nexthop ip address:192.168.100.2

Switch#

11.1.12 match tag

命令

match tag <tag>

no match tag [<tag>]

模式

route-map 配置模式

参数

tag：ospf 外部路由的标记值。

描述

match tag命令用来配置一条以路由tag值为匹配条件的匹配规则，该规则对ospf外部路由有效。

no match tag命令用来删除一条以路由tag值为匹配条件的匹配规则。

举例

#配置一条规则，匹配条件为 ospf 外部路由中 tag 值为 3 的路由：

Switch(config-route-map)#match match tag 3

Switch(config-route-map)#

11.1.13 router-id

命令

router-id <router-id>

no router-id [router-id]

模式

全局配置模式

参数

router-id：需要指定的路由器标识，采用 32 位点分十进制格式。

描述

router-id 命令用来配置路由管理中的路由器ID。一些动态路由协议要求使用路由器ID，如果在启动这些路由协议时没有显示指定路由器ID，则缺省使用路由管理的路由器ID。

no router-id 命令用来删除已配置的路由器ID。

举例

#配置交换机的 router-ID 为 1.1.1.1

Switch(config)#router-id 1.1.1.1

Switch(config)

#删除交换机配置的 router-id

Switch(config)#no router-id

Switch(config)

缺省情况下，路由管理的路由器ID 是0.0.0.0。

11.1.14 route-map

命令

route-map <map-tag> {permit | deny} <sequence>

no route-map <map-tag> {permit | deny} <sequence>

模式

全局配置模式

参数

map-tag：route-map 名。

permit：允许通过。

deny：拒绝通过。

sequence：匹配顺序号。

描述

route-map命令用来创建route-map规则并进入该规则的配置模式下，配置后的route-map规则可以供rip，ospf等协议调用对路由进行控制。

no route-map命令用来删除一组route-map规则中的一条或全部。

举例

#为 route-map“lenovo8800”增加顺序号为 10 的允许通过的规则

Switch(config)#route-map lenovo8800 permit 10

Switch(config-route-map)#

11.1.15 set ip

命令

set ip next-hope <ip-address>

no set ip next-hope [<ip-address>]

模式

route-map 配置模式

参数

ip-address：路由的下一跳地址。

描述

set ip命令用来设置符合条件的路由的ip属性。

no set ip命令用来取消对符合条件的路由的ip属性设置。

举例

#将符合匹配条件的路由的下一跳设置为 172.20.1.2：

Switch(config-route-map)#set ip next-hop 172.20.1.2

Switch(config-route-map)#

11.1.16 set metric

命令

set metric {+/-<metric> | <metric>}

no set metric [+/-<metric> | <metric>]

模式

route-map 配置模式

参数

metric：路由的花销值。

描述

set metric命令用来设置符合条件的路由的metric值。

no set metric命令用来取消设置符合条件的路由的metric值。

举例

#将符合匹配条件的路由的 metric 值增加 2：

Switch(config-route-map)#set metric +2

Switch(config-route-map)#

11.1.17 set metric-type

命令

set metric-type {type-1 | type-2}

no set metric-type [type-1 | type-2]

模式

route-map 配置模式

参数

type-1：类型 1 的 ospf 外部路由。

type-2：类型 2 的 ospf 外部路由。

描述

set metric-type命令用来改变符合条件的路由的类型。

no set metric-type命令用来取消对路由类型的改变。

举例

#将符合匹配条件的 ospf 外部路由属性改变为 type-1：

Switch(config-route-map)#set metric-type type-1

Switch(config-route-map)#

11.1.18 set tag

命令

set tag <tag>

no set tag [<tag>]

模式

route-map 配置模式

参数

tag：ospf 外部路由的标记值。

描述

set tag命令用来设置符合匹配条件的路由tag值。

no set tag命令用来取消对路由tag值的设置。

举例

#设置符合条件的路由的 tag 值为 10：

Switch(config-route-map)#set tag 10

Switch(config-route-map)#

11.2 显示命令

11.1.1 show arp

命令

show arp [<ip-address> | dynamic | lock | static]

模式

普通模式/特权模式

参数

ip-address: ip地址段。

dynamic： 动态学习到的arp表。

lock： 锁定的arp表信息。

static： 静态 arp 表。

描述

显示地址解析表。

举例

#显示动态学习到的arp表：

Switch#show arp dynamic

ARP TABLE

Internet Address	Physical Address	Type
210.21.223.113	0001.30ba.9c00	dynamic
210.21.223.117	0005.6401.22ad	dynamic

Total Number: 2

Switch#

11.1.2 show ip interface

命令

show ip interface [<ifname>] brief

模式

普通模式/特权模式

参数

ifname：需要指定的接口名接口名，可以是二层接口，也可以是三层接口。

缺省显示所有二、三层接口。

描述

show ip interface 命令用来显示接口的摘要信息。

举例

#显示接口vlan24的信息：

```
Switch#show ip interface vlan24 brief
Interface                  IP-Address      Status                Protocol
vlan24                     192.168.192.32  up                    up
Switch#
```

11.2.3 show ip prefix-list

命令

show ip prefix-list [<prefix-list>] [detail] [summary]

模式

特权模式/普通模式

参数

缺省：显示所有的前缀列表信息。

prefix-list：前缀列表名。

detail：详细信息。

summary：概要信息。

描述

show ip prefix-list命令用来显示前缀列表的相关配置信息。

举例

#查看前缀列表的详细信息：

```
Switch#show ip prefix-list detail
Prefix-list with the last deletion/insertion: limit
```

ip prefix-list limit:
count: 1, range entries: 0, sequences: 15 - 15
Switch#

11.2.4 show ip route

命令

show ip route [<network>]

模式

特权模式/普通模式

参数

缺省参数：显示当前路由表中激活的路由。

network：指定显示相关网络的路由，使用 32 位点分十进制或地址前缀/掩码形式表示。

描述

show ip rout命令用来显示路由信息。内容包括目的地址、掩码长度、协议、优先级、权值、下一跳和输出接口。

该命令只显示当前激活的路由（最佳路由）。

举例

#显示当前使用的路由

Switch#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

R 1.0.0.0/24 [120/2] via 172.20.1.3, vlan2, 00:00:19
R 1.0.1.0/24 [120/2] via 172.20.1.3, vlan2, 00:00:19
R 1.0.2.0/24 [120/2] via 172.20.1.3, vlan2, 00:00:19
C 172.20.1.0/24 is directly connected, vlan2
C 172.20.2.0/24 is directly connected, vlan3
O 172.21.0.128/25 [110/12] via 172.20.2.3, vlan3, 00:00:14
O 172.21.1.0/24 [110/12] via 172.20.2.3, vlan3, 00:00:14

```
O IA      172.21.2.0/24 [110/20] via 172.20.2.3, vlan3, 00:00:14
O IA      172.21.3.0/24 [110/20] via 172.20.2.3, vlan3, 00:00:14
O E1      172.21.4.0/24 [110/1010] via 172.20.2.3, vlan3, 00:00:14
O E1      172.21.5.0/24 [110/1010] via 172.20.2.3, vlan3, 00:00:14
S         192.1.1.0/24 [1/0] via 172.20.2.2, vlan3
S         200.1.1.0/24 [1/0] via 172.20.1.2, vlan2
```

Switch#

#显示指定网络的路由

```
Switch#show ip route 1.0.2.0
Routing entry for 1.0.2.0/24
  Known via "rip", distance 120, metric 2, best
  Last update 00:05:37 ago
  * 172.20.1.3, via vlan2
```

Switch#

11.2.5 show ip route connected

命令

show ip route connected [count]

模式

特权模式/普通模式

参数

缺省参数：显示当前路由表中激活的直接路由。

count：显示当前激活的直接路由的条数。

描述

show ip rout connected命令用来显示直接路由信息。内容包括目的地址、掩码长度、协议和输出接口。

*该命令只显示当前激活的路由。

举例

#显示当前直接路由

```
Switch#show ip route connected
C         172.20.1.0/24 is directly connected, vlan2
```

C 172.20.2.0/24 is directly connected, vlan3

Switch#

#显示当前直接路由条数

Switch#show ip route connected count

total routes: 2

Switch#

11.2.6 show ip route database

命令

show ip route database [<protocol>]

模式

特权模式/普通模式

参数

缺省参数：显示路由表中的所有路由，包括激活和未激活路由。

protocol：跟参数 bgp/connected/isis/ospf/rip/static，显示指定协议的路由。

描述

show ip rout database命令用来整个路由表中的路由信息，包括非激活的路由。

举例

#显示所有的路由

Switch#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

R *> 1.0.0.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22

R *> 1.0.1.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22

R *> 1.0.2.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22
C *> 172.20.1.0/24 is directly connected, vlan2
O 172.20.2.0/24 [110/10] is directly connected, vlan3, 04:43:19
C *> 172.20.2.0/24 is directly connected, vlan3
O *> 172.21.0.128/25 [110/12] via 172.20.2.3, vlan3, 04:36:17
O *> 172.21.1.0/24 [110/12] via 172.20.2.3, vlan3, 04:36:17
O IA *> 172.21.2.0/24 [110/20] via 172.20.2.3, vlan3, 04:36:17
O IA *> 172.21.3.0/24 [110/20] via 172.20.2.3, vlan3, 04:36:17
O E1 *> 172.21.4.0/24 [110/1010] via 172.20.2.3, vlan3, 04:36:17
O E1 *> 172.21.5.0/24 [110/1010] via 172.20.2.3, vlan3, 04:36:17
S *> 192.1.1.0/24 [1/0] via 172.20.2.2, vlan3
> [1/0] via 172.20.2.4, vlan3
S *> 200.1.1.0/24 [1/0] via 172.20.1.2, vlan2

Switch#

#显示所有的静态路由

Switch#show ip route database static

S *> 192.1.1.0/24 [1/0] via 172.20.2.2, vlan3
> [1/0] via 172.20.2.4, vlan3
S *> 200.1.1.0/24 [1/0] via 172.20.1.2, vlan2

Switch#

11.2.7 show policy route

命令

show policy route

模式

特权模式/普通模式

参数

无。

描述

show policy route命令用来显示系统当前的策略路由配置情况。

举例

#显示系统当前配置的策略路由信息

Switch>show policy route

```
Policy route information:
  vlan id:24       nexthop ip address:192.168.100.2
  vlan id:124      nexthop ip address:192.168.93.2
Switch#
```

11.2.8 show route-map

命令

show route-map

模式

特权模式/普通模式

参数

无。

描述

show route-map命令用来显示route-map的配置信息前缀列表的相关信息。

举例

#查看当前 route-map 的配置信息：

```
Switch#show route-map
route-map lenovo8800, permit, sequence 10
  Match clauses:
  Set clauses:
    metric-type type-1
    tag 10
route-map lenovo8800, deny, sequence 15
  Match clauses:
  Set clauses:
Switch#
```

第 12 章 RIP 命令

12.1 配置命令

12.1.1 default-information originate

命令

default-information originate

no default-information originate

模式

rip 配置模式

参数

无

描述

default-information originate命令用来启动rip协议产生缺省路由并向其他路由器扩散。

no default-information originate命令用来禁止本地rip产生缺省路由。

举例

#启动 rip 产生缺省 rip 路由的功能

Switch(config-rip)#default-information originate

Switch(config-rip)#

12.1.2 default-metric

命令

default-metric <metric>

no default-metric [<metric>]

模式

rip 配置模式

参数

metric：引入路由的缺省花销，取值范围 1～16，默认为 1。

描述

default-metric命令用来指定rip引入路由时的缺省花销。

no default-metric命令用来恢复引入路由的缺省值，恢复metric值为默认值。

举例

#配置 rip 引入路由的缺省值为 7

Switch(config-rip)#default-metric 7

Switch(config-rip)#

12.1.3 distance

命令

distance <distance-value>

no distance [<distance-value>]

模式

rip 配置模式

参数

distance-value：指定 rip 路由的管理距离（或称协议优先级）值，取值范围 1～255。默认值为 120。

描述

distance命令用来指定rip路由的管理距离（协议优先级）。

no distance命令用来删除对管理距离的配置，恢复到默认值。

举例

#配置 rip 的管理距离为 100

Switch(config-rip)#distance 100

Switch(config-rip)#

12.1.4 distribute-list

命令

distribute-list {<acl-name> | prefix [<prefix-list>]} {in | out} [<if-name>]

no distribute-list {<acl-name> | prefix [<prefix-list>]} {in | out} [<if-name>]

模式

rip 配置模式。

参数

acl-name：访问控制列表名。

prefix-list：前缀列表名。

in：在入接口上使用过滤。

out：在出接口上使用过滤。

if-name：指定使用过滤功能的接口，缺省为所有启动 RIP 协议的接口。

描述

distribute-list命令用来配置使用访问控制列表和前缀列表在输入输出接口上过滤路由。

no distribute-list命令用来取消路由过滤的配置。

举例

#配置在接口 vlan3 上使用名为 list123 的访问控制列表过滤进入的路由

Switch(config-rip)#distribute-list list123 in vlan3

Switch(config-rip)#

12.1.5 ip rip authentication

命令

ip rip authentication {mode <mode> | key-chain <key-chain> | string <string>}

no ip rip authentication [mode <mode> | key-chain <key-chain> | string <string>]

模式

接口配置模式。

参数

mode：认证的方式，取值为 md5 方式和 text（简单文本方式）。

key-chain ：key-chainming，配置后调用对应 key-chain 中配置的认证码。

string：认证码，字符串形式，不超过 16 个字符。

描述

ip rip authentication 命令用来使能接口对 RIP 报文的认证功能并配置相关参数。

no ip rip authentication 命令用来取消接口对 RIP 报文的认证功能或修改和删除相关参数。

举例

#配置接口 vlan55 上运行 RIP 协议时使用认证功能，认证方式为 md5，认证密码为 pass123。

Switch(config-vlan55)#ip rip authentication mode md5

Switch(config-vlan55)#ip rip authentication string pass123

Switch(config-vlan55)#

12.1.6 ip rip metric

命令

ip rip metric <metric>

no ip rip metric [<metric>]

模式

接口配置模式。

参数

metric：metric 值，取值范围 1～16。

描述

ip rip metric 命令用来配置接口接收 RIP 路由时的 metric 值的增量，缺省为 1。

no ip rip metric 命令用来取消对入接口 metric 增量的配置，恢复到默认值。

举例

#配置接口 vlan55 上发送 RIP 路由时 metric 值增加 3。

Switch(config-vlan55)#ip rip metric 3

Switch(config-vlan55)#

12.1.7 ip rip receive version

命令

ip rip receive version <version>

no ip rip receive version [<version>]

模式

接口配置模式。

参数

version：允许接收的 RIP 报文的版本，取值为 1，2 或 1 2，即两者皆可。缺省为 2。

描述

ip rip receive version 命令用来配置接口接收 RIP 报文的版本。

no ip rip receive version 命令用来恢复接口接收 RIP 报文的版本为缺省值。

举例

#配置接口 vlan55 上允许接收版本号为 1 的 RIP 报文。

Switch(config-vlan55)#ip rip receive version 1
Switch(config-vlan55)#

12.1.8 ip rip receive-packet

命令

ip rip receive-packet
no ip rip receive-packet

模式

接口配置模式。

参数

无。

描述

ip rip receive-packet 命令用来使能接口接收 RIP 报文。

no ip rip receive-packet 命令用来配置接口不能接收 RIP 报文。

举例

#配置接口 vlan55 上允许接收 RIP 报文。
Switch(config-vlan55)# ip rip receive-packet
Switch(config-vlan55)#
#配置接口 vlan55 上不能接收 RIP 报文
Switch(config-vlan55)#no ip rip receive-packet
Switch(config-vlan55)#

12.1.9 ip rip send version

命令

ip rip send version <version>
no ip rip send version [<version>]

模式

接口配置模式。

参数

version：允许发送的 RIP 报文的版本，取值为 1 或 2。缺省为 2。

描述

ip rip send version 命令用来配置接口发送 RIP 报文的版本。

no ip rip send version 命令用来恢复接口发送 RIP 报文的版本为缺省值。

举例

#配置接口 vlan55 上允许发送版本号为 1 的 RIP 报文。

Switch(config-vlan55)#ip rip send version 1

Switch(config-vlan55)#

12.1.10 ip rip send-packet

命令

ip rip send-packet

no ip rip send-packet

模式

接口配置模式。

参数

无。

描述

ip rip send-packet 命令用来使能接口发送 RIP 报文。

no ip rip send-packet 命令用来配置接口不能发送 RIP 报文。

举例

#配置接口 vlan55 上允许发送 RIP 报文。

Switch(config-vlan55)# ip rip send-packet

Switch(config-vlan55)#

#配置接口 vlan55 上不能发送 RIP 报文

Switch(config-vlan55)#no ip rip send-packet

Switch(config-vlan55)#

12.1.11 ip rip split-horizon

命令

ip rip split-horizon [poisoned]

no ip rip split-horizon

模式

接口配置模式。

参数

poisoned：带毒性逆转的水平分割方式。

描述

ip rip split-horizon 命令用来使能接口上的水平分割功能。缺省情况为带毒性逆转的水平分割方式。

no ip rip split-horizon 命令用来配置接口上不使用水平分割功能。

举例

#配置接口 vlan55 上使能带毒性逆转的水平分割。

Switch(config-vlan55)# ip rip split-horizon poisoned

Switch(config-vlan55)#

12.1.12 maximum-prefix

命令

maximum-prefix <max-num> [<waring-num>]

no maximum-prefix [<max-num>] [<waring-num>]

模式

rip 配置模式。

参数

max-num：RIP 路由的最大条数，取值范围 1～65535。

waring-num：发出路由报警的百分比，取值范围 1～100。

描述

maximum-prefix命令用来配置路由表容量及告警容限。

no maximum-prefix命令用来取消对路由表的容量限制和告警配置。

举例

#配置 RIP 路由上限为 1000 条，达到 60%时发出告警

Switch(config-rip)#maximum-prefix 1000 60

Switch(config-rip)#

12.1.13 neighbor

命令

neighbor <neighbor-address>

no neighbor <neighbor-address>

模式

rip 配置模式。

参数

neigubor-address：邻居的 ip 地址，点分 10 进制格式。

描述

neighbor命令为RIP在非广播网络上指定邻居。

no neighbor命令取消指定邻居。

举例

#指定邻居 10.80.50.111

Switch(config-rip)#neighbor 10.80.50.111

Switch(config-rip)#

12.1.14 network

命令

network {<ip-prefix>/<mask-length> | < ip-prefix > <mask>}

no network {<ip-prefix>/<mask-length> | < ip-prefix > <mask>}

模式

rip 配置模式。

参数

ip-prefix：ip 地址前缀。

mask-length：10 进制掩码长度。

mask：32 位点分 10 进制掩码。

描述

network命令用来使能一个子网运行RIP协议。

no network命令用来禁止一个子网使能RIP协议。

举例

#指定子网 192.168.1.0/24 运行 RIP 协议

Switch(config-rip)#network 192.168.1.0/24

Switch(config-rip)#

12.1.15 offset-list

命令

offset-list <acl-name> {in | out} <metric> [<if-name>]

no offset-list <acl-name> {in | out} <metric> [<if-name>]

模式

rip 配置模式。

参数

acl-name：调用的访问控制列表名。

in：在入接口上应用。

out：在出接口上应用。

metric：路由 metric 值的偏移量。

if-name：应用该规则的接口，缺省为所有接口。

描述

offset-list 命令用来配置 RIP 通过 ACL 过滤对接口的输入或输出的路由增加一定的偏移值。

no offset-list 命令用来取消特定路由的偏移增量配置。

举例

#对通过名为“list123”的访问控制列表过滤的路由出接口 vlan3 上 metric 值增加 3

Switch(config-rip)#offset-list list123 out 3 vlan3

Switch(config-rip)#

12.1.16 passive-interface

命令

passive-interface <if-name>

no passive-interface <if-name>

模式

rip 配置模式。

参数

if-name：指定接口。

描述

passive-interface 命令用来配置接口为被动接口，配置后接口能够收 RIP 报文，但不能发送 RIP 报文。

no passive-interface 命令用来恢复接口为可收发状态。

举例

#配置接口 vlan3 为被动接口

Switch(config-rip)#passive-interface vlan3

Switch(config-rip)#

12.1.17 recv-buffer-size

命令

recv-buffer-size <buffer-size>

no recv-buffer-size [<buffer-size>]

模式

rip 配置模式。

参数

buffer-size：接收缓冲区大小值，取值范围 8192～2147483647。

描述

recv-buffer-size 命令用来配置 RIP 报文接收缓冲区的大小。

no recv-buffer-size 命令用来取消对 RIP 接收缓冲区大小的指定

举例

#配置接收缓冲区大小为 102400

Switch(config-rip)# recv-buffer-size 102400

Switch(config-rip)#

12.1.18 redistribute

命令

redistribute <protocol> [metric <metric>] [route-map <route-map>]

no redistribute <protocol> [metric <metric>] [route-map <route-map>]

模式

rip 配置模式。

参数

protocol:需要引入到 RIP 中的路由协议类型如 is-is，ospf，bgp，static，connect 等。

metric：指定引入路由时的 metric 值。

route-map：引入路由时需要引用的 route-map 名。

描述

redistribute 用来引入其他协议的路由到 RIP 中。

no redistribute 用来取消对其他协议路由的引入。缺省情况下不做引入。

举例

#引入直连路由到 RIP 路由表中，并通过 route-map 规则“list123”规则，指定引入路由的 metric 值为 9。

Switch(config-rip)#redistribute connected metric 9 route-map list123

Switch(config-rip)#

12.1.19 route

命令

route <network>/<mask-length>

no route <network>/<mask-length>

模式

rip 配置模式。

参数

network：路由的目的网络。

mask-length：目的网络的掩码长度。

描述

route 命令用来增加一条静态路由到 RIP 路由表中，再 RIP 域内扩散该路由。

no route 命令用来取消一条加入到 RIP 中的静态路由。

举例

#增加一条到目的网络 200.1.1.0/24 的静态路由到 RIP 路由表中

Switch(config-rip)# route 200.1.1.0/24

Switch(config-rip)#

12.1.20 router rip

命令

router rip

no router rip

模式

全局配置模式

参数

无

描述

router rip命令用来启动rip协议并进入rip配置模式。

no router rip命令用来关闭rip协议，并删除配置。

举例

#启动并进入 rip 配置模式

Switch(config)#router rip

Switch(config-rip)#

12.1.21 timers

命令

timers basic <update-interval> <dead-interval> <garbage-interval>

no timers basic

模式

rip 配置模式。

参数

update-interval：发送 RIP 周期性更新报文的时间间隔。默认为 30 秒。

dead-interval：没有得到更新的被设置为不可用的 RIP 路由的等待时间。默认为 180 秒。

garbage-interval：从 RIP 路由设置为不可用到彻底从路由表中删除的时间间隔。默认为 120 秒。

描述

timers basic 命令用来配置与 RIP 相关的定时器值。

no timers basic 命令用来恢复 RIP 定时器到缺省值。

举例

#配置 RIP 协议的周期性更新时间为 20 秒，死亡时间为 100 秒，垃圾收集时间为 60 秒。

Switch(config-rip)#timers basic 20 100 60

Switch(config-rip)#

12.1.22 version

命令

version <version>

no version [<version>]

模式

rip 配置模式。

参数

version：RIP 的版本，取值范围：1～2。

描述

version 命令用来指定 RIP 协议的版本，默认值为 2。

no version 命令用来恢复到系统默认的版本。

举例

#配置 RIP 协议的版本为版本 1。

Switch(config-rip)#version 1

Switch(config-rip)#

12.2 查看命令

12.2.1 show ip rip

命令

show ip rip [database [count] | interface [<if-name>]]

模式

特权模式/普通模式。

参数

缺省：显示当前系统 rip 的相关信息。

database：查看 rip 路由信息数据库。

count：显示 rip 路由信息数据库中的条数。

interface：查看启动了 rip 协议的接口相关信息。

if-name：查看指定接口上的 rip 相关信息

描述

show ip rip 命令用来显示当前的 rip 信息。

举例

#显示接口 vlan51 上当前的 rip 配置。

Switch#show ip rip interface vlan51

vlan51 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:
172.20.6.2/24

Switch#

12.2.2 show ip route rip

命令

show ip route rip [count]

模式

特权模式/普通模式。

参数

缺省：显示当前激活的 rip 路由。

count：显示当前激活的 rip 路由的条数。

描述

show ip route rip 命令用来显示当前激活的 rip 路由信息。

举例

#显示当前激活的 rip 路由。

Switch#show ip route rip

R 1.0.0.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22

R 1.0.1.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22

R 1.0.2.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22

Switch#

#显示当前激活的 rip 路由的条数。

Switch#show ip rout rip count

total routes: 3

Switch#

12.2.3 show running rip

命令

show running rip

模式

特权模式/普通模式。

参数

无。

描述

show running rip 命令用来显示当前的 RIP 配置。

举例

#显示当前的 rip 配置。

Switch#show running-config rip

!

router rip

network 172.20.13.0/24

network 172.20.14.0/24

!

Switch#

12.3 调试命令

12.3.1 debug rip

命令

debug rip

no debug rip

模式

特权模式。

参数

无。

描述

debug rip 命令用来打开当前 rip 的调试开关，使用户能够看到 rip 的协商过程和报文收发情况。

no debug rip 命令用来关闭 rip 的调试开关。

举例

#打开 rip 的调试开关：

Switch#debug rip

Switch#

12.3.2 debug rip all

命令

debug rip all

no debug rip all

模式

特权模式。

参数

无。

描述

debug rip all 命令用来打开所有 rip 相关的调试开关，使用户能够看到 rip 的协商过程和报文收发情况。

no debug rip all 命令用来关闭所有 rip 相关的调试开关。

举例

#打开 rip 相关的所有调试开关：

Switch#debug rip packet all

Switch#

12.3.3 debug rip events

命令

debug rip events

no debug rip events

模式

特权模式。

参数

无。

描述

debug rip events 命令用来打开 rip 的事件调试开关，使用户能够看到 rip 的协商过程。

no debug rip events 命令用来关闭 rip 的事件调试开关。

举例

#打开 rip 的事件调试开关：

Switch#debug rip events

Switch#

12.3.4 debug rip packet

命令

debug rip packet [recv | send] [detail]

no debug rip packet [recv | send] [detail]

模式

特权模式。

参数

recv：打开接收报文调试开关。

send：打开发送报文调试开关。

detail：打开 rip 报文的详细信息调试开关。

描述

debug rip packet 命令用来打开 rip 报文调试开关，使用户能够看到 rip 报文收发情况。

no debug rip packet 命令用来关闭 rip 报文调试开关。

举例

#打开 rip 的接收报文详细信息调试开关：

Switch#debug rip packet recv detail

Switch#

第 13 章 OSPF 命令

13.1 配置命令

13.1.1 area authentication

命令

area <area-id> authentication [message-digest]

no area <area-id> authentication

模式

ospf 配置模式。

参数

area-id：ospf 区域 id，可以十进制表示，取值范围 0～4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0～255.255.255.255。

message-digest：指定使用 MD5 密文验证。若无参数则使用明文认证。

描述

area <area-id> authentication 命令用来配置区域使用验证，并指定验证方式。

no area <area-id> authentication 命令用来取消区域验证功能。

举例

#配置 ospf 进程 11 的区域 1 使用 MD5 验证：

Switch(config-ospf-11)#area 1 authentication message-digest

Switch(config-ospf-11)#

13.1.2 area default-cost

命令

area <area-id> default-cost <cost>

no area <area-id> default-cost

模式

ospf 配置模式。

参数

area-id：ospf 区域 id，可以十进制表示，取值范围 0～4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0～255.255.255.255。

cost：路由花销值，取值范围 0～16777214。

描述

area <area-id> default-cost 命令用来配置从 ABR 发送到 stub 区域和 nssa 区域的 summary 路由的缺省代价。

no area <area-id> default-cost 命令用来取消区域的缺省花销配置，恢复到默认值。

举例

#配置区域 1 的默认 cost 为 224：

Switch(config-ospf-11)#area 1 default-cost 224

Switch(config-ospf-11)#

13.1.3 area filter-list

命令

area <area-id> filter-list {access <access-list> | prefix <prefix-list>} {in | out}

no area <area-id> filter-list {access <access-list> | prefix <prefix-list> } {in | out}

模式

ospf 配置模式。

参数

area-id：ospf 区域 id，可以十进制表示，取值范围 0～4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0～255.255.255.255。

access access-list：访问控制列表名。

prefix prefix-list：地址前缀列表名。

in：指定为入方向有效。

out：指定为出方向有效。

描述

area <area-id> filter-list 命令用来在 ABR 上配置过滤器，可使用 access list 也可使用 prefix list 过滤 summary 路由，in 为灌入本 area 的方向，out 为从本 area 广播出去的方向。

no area <area-id> filter-list 命令用来取消在 ABR 上对区域 summary 路由进行过滤。

举例

#配置 ospf 进程 11 的区域 1 的 ABR 上使用名为 list123 的前缀列表对收到的路由进行过滤：

Switch(config-ospf-11)#area 1 filter-list prefix list123 in
Switch(config-ospf-11)#

13.1.4 area nssa

命令

area <area-id> nssa [default-information-originate] [no-redistribution] [no-summary] [translator-role]
no area <area-id> nssa [default-information-originate] [no-redistribution] [no-summary] [translator-role]

模式

ospf 配置模式。

参数

area-id：ospf 区域 id，可以十进制表示，取值范围 0～4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0～255.255.255.255。
default-information-originate：生成一条类型为 7 的缺省路由发向 nssa 区域。
no-redistribution：指定该 nssa 区域不能使用路由引入。
no-summary：配置 ABR 不发送 summary 类型的 LSA 到 NSSA 区域内。
translator-role：指定为 nssa 区的 ABR。

描述

area <area-id> nssa 命令用来配置区域为 nssa 区域，并可同时指定相关参数。
no area <area-id> nssa 命令用来恢复区域为普通区域或删除 nssa 区域的参数。

举例

#配置 ospf 进程 11 的区域 1 为 nssa 区域，路由器生成一条类型 7 的缺省路由，ABR 不扩散 summaryLSA 到 nssa 区域内：
Switch(config-ospf-11)#area 1 nssa default-information-originate no-summary
Switch(config-ospf-11)#

13.1.5 area range

命令

area <area-id> range <ip-prefix> [advertise | not-advertise]

no area <area-id> range <ip-prefix> [advertise | not-advertise]

模式

ospf 配置模式。

参数

area-id：ospf 区域 id，可以十进制表示，取值范围 0～4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0～255.255.255.255。

ip-prefix：聚合的路由范围，网络/掩码格式。

advertise：聚合后通告聚合的路由。

not-advertise：不通告聚合的路由。

描述

area <area-id> range 命令用来配置区域内的路由聚合或附加参数。

no area <area-id> range 命令用来取消区域的路由聚合或删除附加参数。

举例

#配置 ospf 进程 11 的区域 1 进行路由聚合，并通告聚合后的路由：

Switch(config-ospf-11)#area 1 range 1.1.1.1/8 advertise

Switch(config-ospf-11)#

13.1.6 area shortcut

命令

area <area-id> shortcut [default | disable | enable]

no area <area-id> shortcut [default | disable | enable]

模式

ospf 配置模式。

参数

area-id：ospf 区域 id，可以十进制表示，取值范围 0～4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0～255.255.255.255。

default：缺省模式。

disable：禁止。

enable：强制。

描述

area <area-id> shortcut 命令用来配置 area 的 shortcut 功能，当使能时，数据流可以仅花费较小的代价穿过非骨干区域而无需考虑 ABR 是否连接到骨干区域上。

no area <area-id> shortcut 命令用来取消区域的 shortcut 配置。

举例

#配置 ospf 进程 11 的区域 1 的 shortcut 功能：

Switch(config-ospf-11)#area 1 shortcut enable

Switch(config-ospf-11)#

13.1.7 area stub

命令

area <area-id> stub [no-summary]

no area <area-id> stub [no-summary]

模式

ospf 配置模式。

参数

area-id：ospf 区域 id，可以十进制表示，取值范围 0～4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0～255.255.255.255。

no-summary：配置 ABR 不向 stub 区域通告 summary 路由。缺省允许通告。

描述

area <area-id> stub 命令用来指定区域为 stub 区域。

no area <area-id> stub 命令用来取消指定区域为 stub 区域。

举例

#配置 ospf 进程 11 的区域 1 为 stub 区域，不学习 summary 路由：

Switch(config-ospf-11)#area 1 stub no-summary

Switch(config-ospf-11)#

13.1.8 area virtual-link

命令

area <area-id> virtual-link <neighbor-id> [dead-interval <dead-interval>] [hello-interval <hello-interval>] [retransmit-interval <retran-interval>] [transmit-delay <delay-interval>]

no area <area-id> virtual-link <neighbor-id> [dead-interval <dead-interval>] [hello-interval <hello-interval>] [retransmit-interval <retran-interval>] [transmit-delay <delay-interval>]

模式

ospf 配置模式。

参数

area-id：ospf 区域 id，可以十进制表示，取值范围 0～4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0～255.255.255.255。

neighbor-id：虚连接对端的路由器 Router-id。

dead-interval：配置虚连接上路由器失效的死亡时间。缺省为 4 倍 hello 报文周期（40s）。

hello-interval：配置虚连接上的 hello 报文发送的时间间隔。缺省为 10s。

retran-interval：配置虚连接上的报文重传时间间隔。缺省为 5s。

delay-interval：配置虚连接上的报文传输延迟时间。缺省为 40s。

描述

area <area-id> virtual-link 命令用来配置一条虚连接及相关参数。

no area <area-id> virtual-link 命令用来删除虚连接或恢复虚连接上的参数到默认配置。

举例

#配置 ospf 进程 11 的区域 1 里与邻居 1.1.1.1 建立虚连接，hello 时间间隔为 5s：

Switch(config-ospf-11)#area 1 virtual-link 1.1.1.1 hello-interval 5
Switch(config-ospf-11)#

13.1.9 area virtual-link authentication

命令

area <area-id> virtual-link <neigubor-id> [authentication] [authentication-key <key-string>] [message-digest] [message-digest-key <key-id> md5 <key-string>] [null]

no area <area-id> virtual-link <neigubor-id> [authentication] [authentication-key <key-string>] [message-digest] [message-digest-key <key-id> md5 <key-string>] [null]

模式

ospf 配置模式。

参数

neigubor-id：虚连接对端的路由器 Router-id。

area-id：ospf 区域 id，可以十进制表示，取值范围 0～4294967295；也可以

是 32 位的点分十进制表示。取值范围为 0.0.0.0～255.255.255.255。

authentication：配置虚连接使用认证功能。

authentication-key key-string：配置使用简单验证的验证字。

message-digest：配置使用秘文验证。

message-digest-key key-id md5 key-string：配置使用 md5 秘文验证及验证字的 id 和验证字。

null：不使用验证功能。

描述

area <area-id> virtual-link authentication 命令用来为一条虚连接配置验证功能及相关参数。

no area <area-id> virtual-link authentication 命令用来删除虚连接上的验证或验证的相关参数。

举例

#配置 ospf 进程 11 的区域 1 上与邻居 1.1.1.1 建立虚连接使用简单文本验证：

Switch(config-ospf-11)#area 1 virtual-link 1.1.1.1 authentication authentication-key pass123

Switch(config-ospf-11)#

13.1.10 auto-cost reference-bandwidth

命令

auto-cost reference-bandwidth <bandwidth>

no auto-cost reference-bandwidth

模式

ospf 配置模式。

参数

bandwidth：参考带宽，单位为 Mbits/s，取值范围 1～4294967，缺省为 10000Mbits/s。

描述

auto-cost reference-bandwidth 命令用来配置参考带宽值，ospf 协议根据配置值计算路由的花销。

no auto-cost reference-bandwidth 命令用来删除参考带宽值的配置，恢复到缺省值。

举例

#配置 ospf 进程 11 的参考带宽为 1000Mbits/s：

Switch(config-ospf-11)#auto-cost reference-bandwidth 1000

Switch(config-ospf-11)#

13.1.11 compatible rfc1583

命令

compatible rfc1583

no compatible rfc1583

模式

ospf 配置模式。

参数

无。

描述

compatible rfc1583 命令用来配置本机 ospf 协议兼容 rfc1583。

no compatible rfc1583 命令用来配置本机 ospf 不兼容 rfc1583。

举例

#配置 ospf 进程 11 兼容 rfc1583：

Switch(config-ospf-11)#compatible rfc1583

Switch(config-ospf-11)#

13.1.12 default-information originate

命令

default-information originate [always] [metric] [metric-type] [route-map]

no default-information originate [always] [metric] [metric-type] [route-map]

模式

ospf 配置模式。

参数

always：总是通告缺省路由。

metric：通告缺省路由的花销。

metric-type：通告缺省路由的类型，取值为 1 或 2，缺省为 2。

route-map：通告缺省路由时调用 route-map 规则。

描述

default-information originate 命令用来配置本地路由器生成一条缺省的 ospf 路由及相关参数，并通告到邻居。

no default-information originate 命令用来取消生成缺省路由或改变相关参数。

举例

#配置 ospf 进程 11 生成一条 metric 为 12 的缺省路由：

Switch(config-ospf-11)#default-information originate metric 12

Switch(config-ospf-11)#

13.1.13 default-metric

命令

default-metric <metric>

no default-metric [<metric>]

模式

ospf 配置模式。

参数

metric：引入路由的缺省花销，取值范围为 0～16777214，缺省为 1。

描述

default-metric 命令用来配置 ospf 引入路由的缺省 metric 值。

no default-metric 命令用来恢复引入路由的 metric 值为缺省值。

举例

#配置 ospf 进程 11 引入路由的缺省 metric 为 12：

Switch(config-ospf-11)#default-metric 12

Switch(config-ospf-11)#

13.1.14 distance

命令

distance {<distance> | ospf external <distance> | ospf inter-area <distance> | ospf intra-area <distance>}

no distance {<distance> | ospf external <distance> | ospf inter-area <distance> | ospf intra-area <distance>}

模式

ospf 配置模式。

参数

distance：路由的管理距离，取值范围 1～255，缺省为 110。

external：通过路由引入获得的外部路由。

inter-area：区域间路由。

intra-area：区域内路由。

描述

distance 命令用来配置 ospf 路由的管理距离。

no distance 命令用来恢复 ospf 路由的管理距离到缺省值。

举例

#配置 ospf 路由的管理距离为 120：

Switch(config-ospf-11)#distance 120

Switch(config-ospf-11)#

13.1.15 distribute-list

命令

distribute-list <acl-list> out <protocol>

no distribute-list <acl-list> out <protocol>

模式

ospf 配置模式。

参数

acl-list：访问控制列表名。

out：在向外通告路由时进行过滤。

protocol：指定过滤实施的目标协议。

描述

distribute-list 命令用来配置 ospf 通告路由时对引入的路由进行过滤。

no distribute-list 命令用来取消路由过滤。

举例

#配置 ospf 通告路由时对引入的 rip 路由使用名为 list123 的 acl 进行过滤：

Switch(config-ospf-11)# distribute-list list123 out rip

Switch(config-ospf-11)#

13.1.16 host

命令

host <host-address> area <area-id> [cost <cost>]

no host <host-address> area <area-id} [cost <cost>]

模式

ospf 配置模式。

参数

host-address：主机地址，32 位点分十进制。

area-id：区域 id，点分十进制 0.0.0.0～255.255.255.255 或数字 0～4294927695。

cost：路由花销，取值范围 0～65535。

描述

host 命令用来在一个区域内配置一条主机路由，在 router lsa 中以 stub 类型的 link 广播出去。

no host 命令用来取消主机路由及相关配置。

举例

#配置 ospf 11 的区域 1 中通告一条 172.20.1.1 的主机路由，cost 为 5：

Switch(config-ospf-11)#host 172.20.1.1 area 1 cost 5

Switch(config-ospf-11)#

13.1.17 ip ospf authentication

命令

ip ospf authentication [message-digest] [null]

no ip ospf authentication

模式

接口配置模式。

参数

缺省：使用简单文本验证。

message-digest：使用密文验证。

null：不使用验证。

描述

ip ospf authentication 命令用来配置配置接口的验证模式。

no ip ospf authentication 命令用来取消接口验证。

举例

#配置接口 vlan5 使用简单文本验证：

Switch(config-vlan5)#ip ospf authentication

Switch(config-vlan5)

13.1.18 ip ospf authentication-key

命令

ip ospf authentication-key <key-string>

no ip ospf authentication-key

模式

接口配置模式。

参数

key-string：简单文本验证的密码。

描述

ip ospf authentication-key 命令用来配置简单文本验证的密码。

no ip ospf authentication-key 命令用来删除简单文本验证的密码。

举例

#配置接口 vlan5 使用简单文本验证密码“pass123”：

Switch(config-vlan5)#ip ospf authentication-key pass123

Switch(config-vlan5)

13.1.19 ip ospf cost

命令

ip ospf cost <cost>

no ip ospf cost

模式

接口配置模式。

参数

cost：接口的链路花销，取值范围 1～65535。

描述

ip ospf cost 命令用来配置接口的链路花销，该值对出接口路由有效。

no ip ospf cost 命令用来恢复接口的链路花销到缺省值。

举例

#配置接口 vlan5 的链路花销为 23：

Switch(config-vlan5)#ip ospf cost 23

Switch(config-vlan5)

13.1.20 ip ospf database-filter

命令

ip ospf database-filter all out

no ip ospf database-filter

模式

接口配置模式。

参数

all：所有的路由信息。

out：出方向阻塞。

描述

ip ospf database-filter 命令用来配置接口阻塞泛洪。

no ip ospf database-filter 命令用来恢复接口的泛洪功能。

举例

#配置接口 vlan5 不发送 ospf 的 LSA 信息：

Switch(config-vlan5)# ip ospf database-filter all out

Switch(config-vlan5)

13.1.21 ip ospf dead-interval

命令

ip ospf dead-interval <interval>

no ip ospf dead-interval

模式

接口配置模式。

参数

interval：该接口上 dead 定时器的时间，取值范围 1～65535，广播网上缺省为 40，单位为秒。

描述

ip ospf dead-interval 命令用来配置接口的 dead 定时器值。

no ip ospf dead-interval 命令用来恢复接口 dead 定时器到缺省值。

举例

#配置接口 vlan5 上 ospf 邻居 dead 时间为 20s：

Switch(config-vlan5)# ip ospf dead-interval 20

Switch(config-vlan5)

13.1.22 ip ospf disable all

命令

ip ospf disable all

no ip ospf disable all

模式

接口配置模式。

参数

无。

描述

ip ospf disable 禁止该接口所有的功能，不再处理包；该命令优先于 network 命令。该命令只对三层接口有效。

no ip ospf disable 命令用来恢复接口的 ospf 功能。

举例

#配置接口 vlan5 上禁止 ospf 功能：

Switch(config-vlan5)# ip ospf disable all

Switch(config-vlan5)

13.1.23 ip ospf hello-interval

命令

ip ospf hello-interval <interval>

no ip ospf hello-interval

模式

接口配置模式。

参数

interval：该接口上 hello 定时器的时间间隔，取值范围 1～65535，缺省为

10，单位为秒。

描述

ip ospf hello-interval 命令用来配置接口的 hello 定时器时间间隔。

no ip ospf hello-interval 命令用来恢复接口 hello 定时器到缺省值。

举例

#配置接口 vlan5 上 ospf 邻居 hello 定时器时间间隔为 5s：

Switch(config-vlan5)# ip ospf hello-interval 5

Switch(config-vlan5)

13.1.24 ip ospf message-digest-key

命令

ip ospf message-digest-key <key-id> md5 <key-string>

no ip ospf message-digest-key <key-id>

模式

接口配置模式。

参数

key-id：密文认证的 id 号，取值范围 1～255。

key-string：密文认证的字符串。

描述

ip ospf message-digest-key 命令用来配置接口密文认证的字符串。

no ip ospf message-digest-key 命令用来删除接口密文认证的字符串。

举例

#配置接口 vlan5 上 ospf 的密文认证字 id 为 10，字符串为“123pass”：

Switch(config-vlan5)#ip ospf message-digest-key 10 md5 123pass

Switch(config-vlan5)#

13.1.25 ip ospf mtu

命令

ip ospf mtu <mtu>

no ip ospf mtu

模式

接口配置模式。

参数

mtu：就口最大传输单元，取值范围 576-65535。

描述

ip ospf mtu 命令用来配置接口的最大传输单元。

no ip ospf mtu 命令用来恢复 mtu 到缺省值。

举例

#配置接口 vlan5 上最大传输单元为 1000：

Switch(config-vlan5)# ip ospf mtu 1000

Switch(config-vlan5)#

13.1.26 ip ospf mtu-ignore

命令

ip ospf mtu-ignore

no ip ospf mtu-ignore

模式

接口配置模式。

参数

无。

描述

ip ospf mtu-ignore 命令用来配置接口接收到 DD 报文时的 mtu 忽略功能，接受到报文时不检查 mtu 位。

no ip ospf mtu-ignore 命令用来恢复接口对 mtu 的检查。

举例

#配置接口 vlan5 上不检查 mtu：

Switch(config-vlan5)# ip ospf mtu-ignore

Switch(config-vlan5)#

13.1.27 ip ospf network

命令

ip ospf network {broadcast | non-broadcast | point-to-multipoint [non-broadcast] | point-to-point}

no ip ospf network

模式

接口配置模式。

参数

broadcast:广播网类型。

non-broadcast：非广播网类型。

point-to-multipoint：点到多点网络类型。

point-to-point：点到点网络类型。

描述

ip ospf network 命令用来指定接口所在的网络类型，ospf 根据不同的网络类型运行对应的 ospf 处理机制。

no ip ospf network 命令用来恢复接口到缺省的网络类型。

举例

#配置接口 vlan5 的网络类型为点到点：

Switch(config-vlan5)# ip ospf network point-to-point

Switch(config-vlan5)#

13.1.28 ip ospf priority

命令

ip ospf priority <priority>

no ip ospf priority

模式

接口配置模式。

参数

priority：接口优先级，取值范围 0～255，默认值为 1。

描述

ip ospf priority 命令用来指定接口优先级。

no ip ospf priority 命令用来恢复接口默认优先级。

举例

#配置接口 vlan5 的优先级为 10：

Switch(config-vlan5)# ip ospf priority 10

Switch(config-vlan5)#

13.1.29 ip ospf retransmit-interval

命令

ip ospf retransmit-interval <interval>

no ip ospf retransmit-interval

模式

接口配置模式。

参数

interval：该接口上 retransmit 定时器的时间，取值范围 1～65535，缺省为 5，单位为秒。

描述

ip ospf retransmit-interval 命令用来配置接口的重传定时器值。

no ip ospf retransmit-interval 命令用来恢复接口重传定时器到缺省值。

举例

#配置接口 vlan5 上 ospf 的 retransmi 周期时间为 15s：

Switch(config-vlan5)# ip ospf retransmit-interval 15

Switch(config-vlan5)

13.1.30 ip ospf transmit-delay

命令

ip ospf transmit-delay <interval>

no ip ospf transmit-delay

模式

接口配置模式。

参数

interval：该接口上传输延迟时间，取值范围 1～65535，缺省为 40，单位为秒。

描述

ip ospf transmit-delay 命令用来配置接口的传输延迟值。

no ip ospf transmit-delay 命令用来恢复接口传输延迟到缺省值。

举例

#配置接口 vlan5 上 ospf 的传输延迟时间为 25s：

Switch(config-vlan5)# ip ospf transmit-interval 25

Switch(config-vlan5)

13.1.31 max-concurrent-dd

命令

max-concurrent-dd <number>

no max-concurrent-dd

模式

ospf 配置模式。

参数

number：DD 报文数，取值范围为 1～65535，缺省为 5。

描述

max-concurrent-dd 命令用来控制 DD 挂起列表的最大个数。若在 DD 交换过程中出错，邻居会被放入这个挂起列表。

no max-concurrent-dd 命令用来恢复到缺省值。

举例

#配置 ospf 11 的 DD 报文挂起最大数为 100：

Switch(config-ospf-11)# max-concurrent-dd 100

Switch(config-ospf-11)#

13.1.32 neighbor

命令

neighbor <router-id> [cost <cost>] [poll-interval <interval>] [priority <priority>]

no neighbor <router-id> [cost <cost>] [poll-interval <interval>] [priority <priority>]

模式

ospf 配置模式。

参数

router-id：邻居 router-id，32 位点分十进制。

cost：链路的花销，取值范围 1～65535。

interval：认为邻居 dead 的时间，取值范围 1～65535，单位为秒。

priority：DR 选举时的优先级，取值范围 0～255。

描述

neighbor 命令用来在 NBMA 网络上指定一个邻居，并配置相关参数。

no neighbor 命令用来取消 NBMA 网络上指定的一个邻居。

举例

#配置 NBMA 网络上的邻居 1.1.1.2，协商优先级为 10：

Switch(config-ospf-11)# neighbor 1.1.1.2 priority 10

Switch(config-ospf-11)#

13.1.33 network

命令

network <network> area <area-id>

no network <network> area <area-id>

模式

ospf 配置模式。

参数

network：使能 ospf 的网络，网络/掩码或网络＋反向掩码形式。

area-id：区域 id，32 位点分十进制或数字形式。

描述

network 命令用来使能一个网络并指定加入的区域。

no network 命令用来取消一个网络的使能。

举例

#配置使能网络 172.20.1.0/24 到 ospf 11 的区域 0 中：

Switch(config-ospf-11)# network 172.20.1.0/24 area 0

Switch(config-ospf-11)#

13.1.34 passive-interface

命令

passive-interface <if-name> <if-address>

no passive-interface <if-name> <if-address>

模式

ospf 配置模式。

参数

if-name：接口名。

if-address：接口地址，32 位点分十进制形式。

描述

passive-interface 命令用来配置接口为被动接口，配置后接口能够收 ospf 报文，但不能发送 ospf 报文。

no passive-interface 命令用来恢复接口为可收发状态。

举例

#将接口 vlan55 配置为被动接口：

Switch(config-ospf-11)#passive-interface vlan55 172.20.10.1

Switch(config-ospf-11)#

13.1.35 redistribute

命令

redistribute <protocol> [metric <metric>] [metric-type <type>] [route-map <route-map>] [tag <tag>]

no redistribute <protocol> [metric <metric>] [metric-type <type>] [route-map <route-map>] [tag <tag>]

模式

ospf 配置模式。

参数

protocol:需要引入到 ospf 中的路由协议类型。

metric：指定引入路由的 metric 值。

type：引入的路由类型，取值为 1 或 2，缺省为 2。

route-map：引入路由时需要引用的 route-map 名。

tag：引入路由标记。

描述

redistribute 用来引入其他协议的路由到 ospf 中。

no redistribute 用来取消对其他协议路由的引入。缺省情况下不做路由引入。

举例

#引入直连路由到 ospf 路由表中，并通过 route-map 规则“list123”规则，指定引入路由的 metric 值为 9。

Switch(config-ospf-11)#redistribute connected metric 9 route-map list123

Switch(config-ospf-11)#

13.1.36 router ospf

命令

router ospf [<process-id>]

no router ospf [<process-id>]

模式

全局配置模式。

参数

process-id：ospf 进程号，取值范围为 1～65535，缺省取值为 0。

描述

router ospf 命令用来创建 ospf 进程，并进入该进程的配置模式下。

no router ospf 命令用来删除一个 ospf 进程及该进程下的配置。

举例

#创建 ospf 进程 11：

Switch(config)#router ospf 11

Switch(config-ospf-11)#

13.1.37 router-id

命令

router-id <router-id>

no router-id [<router-id>]

模式

ospf 配置模式。

参数

router-id：路由器 id，点分十进制格式。

描述

router-id 命令用来配置 ospf 进程的 router-id，系统在与邻居协商 ospf 时需要一个 AS 中惟一的身份标识。不配置时使用最大的接口 ip 地址作为 router-id。

no router-id 命令用来删除配置的 router-id，使用默认方式选择。

举例

#配置 ospf 进程使用 router-id 1.1.1.10：

Switch(config-ospf-11)# router-id 1.1.1.10

Switch(config-ospf-11)#

13.1.38 summary-address

命令

summary-address <ip-prefix> [not-advertise] [tag <tag>]

no summary-address <ip-prefix> [not-advertise] [tag <tag>]

模式

ospf 配置模式。

参数

ip-prefix：需要聚合的路由范围，network/mask 形式。

not-advertise：聚合后不通告详细路由。

tag：指定聚合路由的 tag 值。

描述

summary-address 命令用来抑制或聚合外部引入的路由。从其他协议引入的路由，可以使用该命令聚合一定的范围。聚合后，在这个 prefix 覆盖范围内的路由将被抑制，只有聚合后的一条路由被广播。prefix 仅表示一个路由范围，引入的外部路由无需在这个范围内连续

no summary-address 命令用来删除配置的路由聚合。

举例

#配置 ospf 进程使用路由聚合：

Switch(config-ospf-11)#summary-address 1.1.0.0/20

Switch(config-ospf-11)#

13.1.39 timers spf

命令

timers spf <delay> <hold>

no timers spf <delay> <hold>

模式

ospf 配置模式。

参数

delay：延时时间，缺省为 5s。

hold：抑制时间，缺省为 10s。

描述

timers spf 命令用来配置 spf 计算计时器的延时时间和抑制时间。每次启动 spf 计算时，会计算上次 spf 计算到现在的抑制时间，若已经超过了配置的抑制时间则直接使用配置的延时时间启动计时器；若尚未超过配置的抑制时间，则使用配置的抑制时间计算出还需要延时的时间，若这个延时时间太小，小于配置的延时时间，则使用配置的延时时间，否则则使用计算出的延时时间启动计时器。

no timers spf 命令用来恢复 spf 计算定时器到默认值。

举例

#配置 ospf 进行 spf 计算的延时时间为 10s，抑制时间为 15s：

```
Switch(config-ospf-11)#timers spf 10 15
Switch(config-ospf-11)#
```

13.2 查看命令

13.2.1 show ip ospf

命令

show ip ospf [<process-id>]

模式

特权模式/普通模式。

参数

process-id：进程号，指定要查看的进程，取值范围 0～65535。

描述

show ip ospf 命令用来显示指定 ospf 进程相关的信息。不指定进程号时显示所有当前存在的进程的相关信息。

举例

#显示 ospf 进程 10 的相关信息：

```
Switch#show ip ospf 10
 Routing Process "ospf 10" with ID 192.168.0.1
 Process uptime is 1 day 7 hours 52 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
```

This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 1. Checksum 0x007741
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 69
Number of LSA received 192
Number of areas attached to this router: 2
Area 0 (BACKBONE)
Number of interfaces in this area is 17(17)
Number of fully adjacent neighbors in this area is 1
Area has no authentication
SPF algorithm last executed 31:09:58.285 ago
SPF algorithm executed 10 times
Number of LSA 5. Checksum 0x023ca6
Area 1
Number of interfaces in this area is 2(2)
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 31:52:10.025 ago
SPF algorithm executed 4 times
Number of LSA 20. Checksum 0x09f53d

Switch#

13.2.2 show ip ospf database

命令

show ip ospf [<process-id>] database [adv-router | asbr-summary | external | max-age | network | nssa-external | opaque-area | opaque-as | opaque-link | router | self-originate | summary]

模式

特权模式/普通模式。

参数

process-id：进程号，指定要查看的进程，取值范围 0～65535。

adv-router：通告路由链路状态信息。

asbr-summary：asbr 的 summary 链路状态信息。

external：外部路由链路状态信息。

max-age：age 列表中的链路状态信息。

network：Network 类型的链路状态信息。

nssa-external：NSSA 区域引入的链路状态信息。

router：路由器链路状态信息

self-originate：自己产生的链路状态信息。

summary：网络汇聚链路状态信息。

描述

show ip ospf [<process-id>] database 命令用来显示指定 ospf 进程的链路状态数据库信息。

举例

#显示 ospf 进程 10 的链路状态数据库中 networks 类型的信息：

Switch#show ip ospf 10 database network

OSPF Router with ID (192.168.0.1) (Process ID 10)

Net Link States (Area 0.0.0.0)

LS age: 531
Options: 0x22 (*|-|DC|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 172.20.5.3 (address of Designated Router)
Advertising Router: 192.168.130.2
LS Seq Number: 8000003e
Checksum: 0xe30a
Length: 32
Network Mask: /24
Attached Router: 192.168.130.2
Attached Router: 192.168.0.1

Switch#

13.2.3 show ip ospf interface

命令

show ip ospf interface [<if-name>]

模式

特权模式/普通模式。

参数

if-name：需要显示 ospf 接口信息的接口名。

描述

show ip ospf interface 命令用来显示接口的 ospf 相关信息。

举例

#显示启动了 ospf 协议的接口的相关信息：

```
Switch# show ip ospf interface
vlan5 is up, line protocol is up
  Internet Address 172.20.22.225/27, Area 0.0.0.1, MTU 1500
  Process ID 10, Router ID 172.20.22.225, Network Type BROADCAST,
Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.20.22.225, Interface Address 172.20.22.225
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 0, Adjacent neighbor count is 0
  Crypt Sequence Number is 3774326953
  Hello received 0 sent 5, 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
vlan6 is down, line protocol is down
  OSPF is enabled, but not running on this interface
vlan51 is up, line protocol is up
  Internet Address 172.20.6.2/24, Area 0.0.0.0, MTU 1500
  Process ID 10, Router ID 172.20.22.225, Network Type BROADCAST,
Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
```

Designated Router (ID) 172.20.22.225, Interface Address 172.20.6.2
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Neighbor Count is 0, Adjacent neighbor count is 0
Crypt Sequence Number is 3774326953
Hello received 0 sent 5, 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

Switch#

13.2.4 show ip ospf neighbor

命令

show ip ospf [<process-id>] neighbor [<neighbor-id>] | [all | detail | interface <if-address>]

模式

特权模式/普通模式。

参数

process-id：进程号，指定要查看的进程，取值范围 0～65535。

neighbor-id：邻居路由器 ID。

all：显示所有的邻居，包括 down 状态的。

detail：显示邻居的详细信息。

interface if-address：查看指定接口上的邻居信息。

描述

show ip ospf [<process-id>] neighbor 命令用来显示 ospf 的邻居信息。

举例

#显示 ospf 进程 10 的接口地址为 172.20.5.2 上的邻居信息：

Switch#show ip ospf nei inter 172.20.5.2

OSPF process 10

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.130.2	1	Full/DR	00:00:34	172.20.5.3	vlan10

Switch#

13.2.5 show ip ospf route

命令

show ip ospf [<process-id>] route [count]

模式

特权模式/普通模式。

参数

process-id：进程号，指定要查看的进程，取值范围 0～65535。

count：显示 ospf 路由条数。

描述

show ip ospf [process-id] route 命令用来显示 ospf 路由表。

举例

#显示 ospf 进程 10 的 ospf 路由条数：

```
Switch#show ip ospf 10 route    coun
total routes: 21

Switch#
```

13.2.6 show ip ospf virtual-links

命令

show ip ospf [<process-id>] virtual-links

模式

特权模式/普通模式。

参数

process-id：进程号，指定要查看的进程，取值范围 0～65535。

描述

show ip ospf [<process-id>] virtual-links 命令用来查看虚连接的相关信息。

举例

#显示 ospf 进程 10 的 ospf 路由条数：

```
Switch#show ip ospf virtual-links
Virtual Link VLINK0 to router 1.1.1.10 is down
  Transit area 0.0.0.1 via interface *
  Local address *
```

```
  Remote address *
  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

Switch#
```

13.2.7 show running ospf

命令

show running ospf

模式

特权模式/普通模式。

参数

无。

描述

show running ospf 命令用来查看当前系统中的 ospf 配置信息。

举例

#显示当前系统中 ospf 配置信息：

```
Switch#show running-config ospf
!
router ospf
!
router ospf 1
!
router ospf 10
 network 172.20.5.0/24 area 0
 network 172.20.6.0/24 area 0
 network 172.20.7.0/24 area 0
 network 172.20.11.0/24 area 0
 network 172.20.22.192/27 area 1
 network 172.20.22.224/27 area 1
 area 1 virtual-link 1.1.1.10
!
router ospf 11
```

```
 area 1 authentication message-digest
 area 1 nssa default-information-originate no-summary
!
Switch#
```

13.3 调试命令

13.3.1 debug ospf

`命令

debug ospf

no debug ospf

模式

特权模式。

参数

无。

描述

debug ospf 命令用来打开 ospf 相关调试开关，使用户能够看到 ospf 相关的协商过程和报文收发情况。

no debug ospf 命令用来关闭 ospf 调试开关

举例

#打开调试开关，显示 ospf 调试信息

```
Switch#debug ospf
Switch#
```

13.3.2 debug ospf all

`命令

debug ospf all

no debug ospf all

模式

特权模式。

参数

无。

描述

debug ospf all 命令用来打开 ospf 相关的所有调试开关，使用户能够看到 ospf 相关的协商过程和报文收发情况。

no debug ospf all 命令用来关闭 ospf 相关的所有调试开关。

举例

#打开调试开关，显示出 ospf 所有调试信息

Switch#debug ospf all

Switch#

13.3.3 debug ospf events

`命令

debug ospf events

no debug ospf events

模式

特权模式。

参数

无。

描述

debug ospf events 命令用来打开 ospf 事件调试开关，使用户能够看到 ospf 相关事件信息。

no debug ospf events 命令用来关闭 ospf 事件调试开关。

举例

#打开调试开关，显示 ospf 事件信息

Switch#debug ospf events

Switch#

13.3.4 debug ospf ifsm

`命令

debug ospf ifsm

no debug ospf ifsm

模式

特权模式。

参数

无。

描述

debug ospf ifsm 命令用来打开 ospf 接口状态调试开关，使用户能够看到 ospf 接口状态机变迁信息。

no debug ospf ifsm 命令用来关闭接口状态机调试开关。

举例

#打开调试开关，显示出 ospf 接口状态变迁信息

Switch#debug ospf ifsm

Switch#

13.3.5 debug ospf lsa

`命令

debug ospf lsa

no debug ospf lsa

模式

特权模式。

参数

无。

描述

debug ospf lsa 命令用来打开 ospf lsa 相关调试开关，使用户能够看到 lsa 收发信息。

no debug ospf lsa 命令用来关闭 ospf lsa 调试开关。

举例

#打开调试开关，显示出 ospf lsa 信息

Switch#debug ospf lsa

Switch#

13.3.6 debug ospf nfsm

`命令

debug ospf nfsm

no debug ospf nfsm

模式

特权模式。

参数

无。

描述

debug ospf nfsm 命令用来打开 ospf 邻居状态调试开关，使用户能够看到 ospf 邻居状态变迁情况。

no debug ospf nfsm 命令用来关闭 ospf 邻居状态调试开关。

举例

#打开调试开关，显示 ospf 邻居状态变迁信息

Switch#debug ospf nfsm

Switch#

13.3.7 debug ospf packet

`命令

debug ospf packet [recv | send] [detail]

no debug ospf packet [recv | send] [detail]

模式

特权模式。

参数

recv：接收报文信息。

send：发送报文信息。

detail：详细信息。

描述

debug ospf packet 命令用来打开 ospf 报文调试开关，使用户能够看到 ospf 报文的收发情况。

no debug ospf packet 命令用来关闭 ospf 报文调试开关。

举例

#打开调试开关，显示出 hello 报文的详细信息

Switch#debug ospf packet hello detail

Switch#

13.3.8 debug ospf route

`命令

debug ospf route

no debug ospf route

模式

特权模式。

参数

无。

描述

debug ospf route 命令用来打开 ospf 路由调试开关，使用户能够看到 ospf 路由调试信息。

no debug ospf route 命令用来关闭 ospf 路由调试开关。

举例

#打开调试开关，显示 ospf 路由调试信息

Switch#debug ospf route

Switch#

第 14 章 VRRP 命令

14.1 配置命令

14.1.1 disable/enable

命令

disable vrrp

enable vrrp

模式

vrrp 配置模式。

参数

无

描述

disable vrrp 命令用来禁止当前虚拟路由器的 vrrp 功能。

enable vrrp 命令用来使能当前虚拟路由器的 vrrp 功能。

举例

#使能 vlan10 下 id 为 10 的虚拟路由器的 vrrp 功能。

Switch(config)#router vrrp vlan10 10

Switch(config-vrrp)#enable vrrp

Switch(config-vrrp)

#禁止 vlan10 下 id 为 10 的虚拟路由器的 vrrp 功能。

Switch(config)#router vrrp vlan10 10

Switch(config-vrrp)#disable vrrp

Switch(config-vrrp)

14.1.2 router vrrp

命令

router vrrp <if-name> <vr-id>

no router vrrp <if-name> [<vr-id>]

模式

全局配置模式。

参数

if-name：接口名。

vr-id：虚拟路由器 ID，取值范围：1～255。

描述

router vrrp 命令用来使能一个接口 vrrp 功能，创建一个虚拟路由器并进入 vrrp 配置模式。

no router vrrp 命令用来删除一个 vrrp 虚拟路由器。

举例

#配置接口 vlan10 上使能 vrrp 功能，创建一个 ID 为 10 的虚拟路由器，并进入 vrrp 配置模式。

Switch(config)#router vrrp vlan10 10

Switch(config-vrrp)#

#删除接口 vlan10 上 ID 为 10 的虚拟路由器

Switch(config)#no router vrrp vlan10 10

Switch(config)#

14.1.3 vrrp ip-address

命令

vrrp ip-address <ip-address>

no vrrp ip-address

模式

vrrp 配置模式。

参数

ip-address：虚拟路由器的 ip 地址，点分十进制格式。

注：该地址必须与接口实际地址在同一网段。

描述

vrrp ip-address 命令用来为虚拟路由器配置 ip 地址。

no vrrp ip-address 命令用来删除虚拟路由器配置的 ip 地址。

举例

#配置 vlan10 下 ID 为 10 的虚拟路由器的虚拟 ip 地址为 192.168.1.1：

Switch(config)#router vrrp vlan10 10

Switch(config-vrrp)#vrrp ip-address 192.168.1.1

Switch(config-vrrp)

#删除 vlan10 下 ID 为 10 的虚拟路由器的虚拟 ip 地址

Switch(config)#router vrrp vlan10 10

Switch(config-vrrp)#no vrrp ip-address
Switch(config-vrrp)

14.1.4 vrrp advertisement-interval

命令

vrrp advertisement-interval <interval>

模式

vrrp 配置模式。

参数

interval：虚拟路由器发送周期性消息的时间间隔，单位为秒，取值范围：1～255。缺省为 1 秒。

描述

vrrp advertisement-interval 命令用来配置作为 master 的虚拟路由器发送周期性消息的时间间隔。

举例

#配置 vlan10 下 ID 为 10 的虚拟路由器周期性消息的时间间隔为 10 秒：
Switch(config)#router vrrp vlan10 10
Switch(config-vrrp)#vrrp advertisement-interval 10
Switch(config-vrrp)

14.1.5 vrrp authentication

命令

vrrp authentication {none | simple-password <password>}

模式

vrrp 配置模式。

参数

none：指定 vrrp 报文不使用验证。
simple-password <password>：指定 vrrp 使用简单文本验证，配置验证码。

描述

vrrp authentication 命令用来指定 vrrp 报文的验证方式和验证密码。

举例

#配置 vlan10 下 ID 为 10 的虚拟路由器使用简单文本验证，验证密码为

“pass123”：

```
Switch(config)#router vrrp vlan10 10
Switch(config-vrrp)#authentication simple-password pass123
Switch(config-vrrp)
```

14.1.6 vrrp preempt

命令

vrrp preempt {false | true}

模式

vrrp 配置模式。

参数

false：不使用抢占模式。

true：使用抢占模式。

描述

vrrp preempt 命令用来指定 vrrp 虚拟路由器是否使用抢占模式，当抢占模式为真时，同等情况下，使用抢占模式的一方将作为 master。缺省情况下为 true。

举例

#配置 vlan10 下 ID 为 10 的虚拟路由器不使用抢占模式：

```
Switch(config)#router vrrp vlan10 10
Switch(config-vrrp)#vrrp preempt false
Switch(config-vrrp)
```

14.1.7 vrrp priority

命令

vrrp priority <priority-number>

模式

vrrp 配置模式。

参数

priority-number：优先级值。取值范围为 3～254，1～2 为保留值，缺省为 100。

描述

vrrp priority 命令用来指定 vrrp 虚拟路由器发送协商报文的优先级。同等条件下，优先级高的一方成为 master。

举例

#配置 vlan10 下 ID 为 10 的虚拟路由器的优先级为 70：

Switch(config)#router vrrp vlan10 10
Switch(config-vrrp)#vrrp priority 70
Switch(config-vrrp)

14.1.8 vrrp tracking

命令

vrrp tracking interface <if-name>
no vrrp tracking interface [<if-name>]

模式

vrrp 配置模式。

参数

if-name：配置 vrrp tracking 监控的接口名；可以是二层接口，也可以是三层接口。接口的 UP/DOWN 将触发 vrrp 的周期性通告报文的优先级变化。

描述

vrrp tracking interface：命令用来配置 vrrp tracking 功能的监视端口。vrrp 的 tracking 功能用来监控指定接口的接口状态，以实现动态的调整 vrrp 交换机的主备关系。监控接口 down 后，本地 vrrp 接口发送优先级为 1 的通告消息。接口 UP 时通告消息使用配置优先级，通过优先级变化实现 vrrp 主备的动态切换。监控接口可以有多个。

no vrrp tracking interface：命令用来删除监控端口的配置。

举例

配置 vlan3 上 vrid 为 2 的虚拟路由器监控接口为 ge2/3 和 vlan10：

Switch(config)#router vrrp vlan3 2
Switch(config-vrrp)#vrrp tracking interface ge2/3
Switch(config-vrrp)#vrrp tracking interface vlan10
Switch(config-vrrp)#end
Switch#show vrrp

Vlan: 3 Vrid: 2
Virtual Router: Disabled

State: INITIALIZE
Virtual Ip Address:
Ip Address Owner: FALSE
Advertisement Interval: 1s
Protocol Priority: 100
Config Priority: 100
Preempt Mode: TRUE
Authentication Type: No Authentication
Interface Tracking: ge2/3 vlan10
Switch#

14.2 查看命令

14.2.1 show vrrp

命令

show vrrp [<if-name>]

模式

特权模式/普通模式。

参数

if-name：接口名。

描述

show vrrp 命令用来显示接口下当前已经配置的 vrrp 及其工作情况。缺省显示所有接口下的配置的所有 vrrp 信息。

举例

#查看 vlan10 接口下的 vrrp 配置：

Switch#show vrrp vlan10

Vlan: 10 Vrid: 10
Virtual Router: Disabled
State: INITIALIZE
Virtual Ip Address:
Ip Address Owner: FALSE
Advertisement Interval: 10s
Protocol Priority: 100

Config Priority: 100
Preempt Mode: TRUE
Authentication Type: Simple Text Password
Authentication Password: pass123

Switch#

14.3 调试命令

14.3.1 debug vrrp

命令

debug vrrp
no debug vrrp

模式

特权模式。

参数

无。

描述

debug vrrp 命令用来打开当前 vrrp 的调试开关，使用户能够看到 vrrp 的协商过程和报文收发情况。

no debug vrrp 命令用来关闭 vrrp 的调试开关。

举例

#打开 vrrp 的调试开关：
Switch#debug vrrp
Switch#

14.3.2 debug vrrp all

命令

debug vrrp all
no debug vrrp all

模式

特权模式。

参数

无。

描述

debug vrrp all 命令用来打开所有 vrrp 相关的调试开关，使用户能够看到 vrrp 的协商过程和报文收发情况。

no debug vrrp all 命令用来关闭所有 vrrp 相关的调试开关。

举例

#打开 vrrp 相关的所有调试开关：

Switch#debug vrrp packet all

Switch#

14.3.3 debug vrrp events

命令

debug vrrp events

no debug vrrp events

模式

特权模式。

参数

无。

描述

debug vrrp events 命令用来打开 vrrp 的事件调试开关，使用户能够看到 vrrp 的协商过程。

no debug vrrp events 命令用来关闭 vrrp 的事件调试开关。

举例

#打开 vrrp 的事件信息调试开关：

Switch#debug vrrp events

Switch#

14.3.4 debug vrrp packet

命令

debug vrrp packet [recv | send] [detail]

no debug vrrp packet [recv | send] [detail]

模式

特权模式。

参数

recv：打开接收报文调试开关。

send：打开发送报文调试开关。

detail：打开 vrrp 报文的详细信息调试开关。

描述

debug vrrp 命令用来打开当前 vrrp 的调试开关，使用户能够看到 vrrp 的协商过程和报文收发情况。

no debug vrrp 命令用来关闭 vrrp 的调试开关。

举例

#打开 vrrp 的接收报文详细信息调试开关：

Switch#debug vrrp packet recv detail

Switch#

第 15 章 VLLP 命令

15.1 配置命令

15.1.1 router vllp

router vllp <if-name>

no router vllp <if-name>

模式

全局配置模式

参数

If-name：接口名，在该接口上启动 vllp 协议，该接口只能是三层 vlan 接口。

描述

router vllp 命令用来创建一个 vlan 相关的 vllp 进程并进入 vllp 配置模式；

no router vllp 命令用删除指定 vlan 的 vllp 进程。

举例

#在 vlan8 上启动 vllp 进程：

Switch(config)#router vllp vlan8

Switch(config-vllp)#

15.1.2 vllp disable/enable

vllp {enable | disable}

模式

vllp 配置模式

参数

无。

描述

vllp enable 命令用来使能 vllp 协议；

vllp disable 命令用来禁止 vllp 协议。

举例

#在 vlan8 上启动 vllp 协议：

Switch(config)#router vllp vlan8

Switch(config-vllp)#vllp enable

Switch(config-vllp)#

15.1.3 vllp port

vllp port <if-name>

no vllp port <if-name>

模式

vllp 配置模式

参数

If-name：二层接口名，可以是 Trunk 组。该接口必须在当前配置的 vllp vlan 内。

描述

vllp port 命令用来增加一个参加 vllp 环路计算的端口，缺省为空；

no vllp port 命令用来指定一个端口不再参与 vllp 环路计算。

举例

#指定 vlan4 中有两个端口 ge4/9 和 ge4/11 参与环路计算：

```
Switch#show vlan 4
 VLAN     Name       State        Member ports ([u]-Untagged, [t]-Tagged)
 ----     --------   ---------    ------------------------------------------------
 4        vlan4      active       [t]ge4/4 [t]ge4/9 [t]ge4/11
Switch#config terminal
Switch(config)#router vllp vlan4
Switch(config-vllp)#vllp port ge4/9
Switch(config-vllp)#vllp port ge4/11
Switch(config-vllp)#
```

15.1.4 vllp priority

vllp priority <priority-value>

no vllp priority [<priority-value >]

模式

vllp 配置模式

参数

priority-value：优先级值，取值范围是 1～255，缺省值为 100。

描述

vllp priority 命令用来配置 vlan 与其他交换机进行 vllp 协商时的优先级；

no vllp priority 命令用来删除 vlan 进行 vllp 协商的优先级配置，恢复到缺省值。

举例

#配置 vlan4 的 vllp 优先级为 108：

Switch(config)#router vllp vlan4

Switch(config-vllp)#vllp priority 108

Switch(config-vllp)#

15.1.5 vllp query-interval

vllp query-interval <interval-value>

no vllp query-interval [<interval -value >]

模式

vllp 配置模式

参数

interval-value：vllp 协议查询报文发送的时间间隔，取值范围是 1～255，缺省值为 5 秒。

描述

vllp query-interval 命令用来配置本端为发送端时发送 vllp 查询报文的时间间隔；

no vllp query-interval 命令用来删除本端发送 vllp 查询报文的时间间隔配置，恢复到缺省值。

举例

#配置 vlan4 在作为发送端时发送 vllp 查询报文的时间间隔为 10 秒：

Switch(config)#router vllp vlan4

Switch(config-vllp)#vllp query-interval 10

Switch(config-vllp)#

15.2 查看命令

15.2.1 show vllp

show vllp [<if-name>]

模式

普通模式/特权模式

参数

If-name：三层 vlan 接口名。

描述

show vllp 命令用来显示配置了 vllp 协议的接口，包括该接口的 vllp 状态和参数。在显示指定 vlan 的 vllp 信息时还包含加入 vllp 端口列表的 vllp 端口的链路状态、STP 状态及端口映射情况。

举例

#查看当前交换机上配置了 vllp 的接口信息：

```
Switch#show vllp
VLLP Equipment List:

IF: vlan8 Index: 6
Instance: 1
Status: Sender
Priority: 100
Main port: 0
Timer interval:
        local query: 5s
        remote query: 5s
        protocol query: 5s
        interrupt: 25s
Query timer: 00:00:04


IF: vlan3 Index: 4
Instance: 2
Status: Sender
Priority: 100
Main port: 0
Timer interval:
        local query: 5s
        remote query: 5s
        protocol query: 5s
        interrupt: 25s
```

Query timer: 00:00:00

Switch#

#查看 vlan4 的 vllp 配置情况和当前状态：

Switch#show vllp vlan4

IF: vlan4 Index: 5
Instance: 3
Status: Sender
Priority: 100
Main port: 0
Timer interval: query 5s/5s interrupt 25s
Query timer: 00:00:04
Port List:
IF: ge4/4 Index: 2196
Vlan flag: INVALID
Link status: UP
STP status: Forward
Mapping port: 0

IF: ge4/9 Index: 2201
Vlan flag: INVALID
Link status: UP
STP status: Forward
Mapping port: 0

IF: ge4/11 Index: 2203
Vlan flag: INVALID
Link status: UP
STP status: Forward
Mapping port: 0

Switch#

15.2.2 show vllp map

show vllp map

模式

普通模式/特权模式

参数

无。

描述

show vllp map 命令用来显示当前配置了 vllp 协议的各 vlan 中 vllp 端口的映射情况。

举例

#查看当前交换机上各 vllp 接口的映射情况：

```
Switch#show vllp map
Mapping table:
vlan8   name        pid      status        map
        ge5/5       2261     Forward       2197
        ge5/4       2260     Forward       2196
vlan3   name        pid      status        map
        ge5/11      2267     Forward       2201
        ge5/9       2265     Forward       2203
vlan4   name        pid      status        map
        ge5/11      2267     Forward       2201
        ge5/9       2265     Block         2203
        ge5/4       2260     Block         2196
Switch#
```

15.2.3 show debugging vllp

show debugging vllp

模式

普通模式/特权模式

参数

无。

描述

show debugging vllp 命令用来显示当前 vllp 调试开关的打开情况。

举例

#查看当前打开了哪些 vllp 调试开关：

```
Switch>show debugging vllp
```

VLLP debugging status:
  VLLP efsm debugging is on
Switch>

15.3 调试命令

15.3.1 debug vllp

debug vllp
no debug vllp

模式

特权模式

参数

无。

描述

debug vllp 命令用来打开所有 vllp 相关的调试开关，使用户能够观察到 vllp 协商中的状态变迁、报文收发等情况；

no debug vll 命令用来关闭所有 vllp 相关的调试开关。

举例

#打开 vllp 调试开关：
Switch#debug vllp
Switch#show debug vllp
VLLP debugging status:
  VLLP packet receive debugging is on
  VLLP packet send debugging is on
  VLLP event debugging is on
  VLLP efsm debugging is on
  VLLP pfsm debugging is on
Switch#

15.3.2 debug vllp all

debug vllp all
no debug vllp all

模式

特权模式

参数

无。

描述

debug vllp all 命令用来打开所有 vllp 相关的调试开关，与命令 debug vllp 相同；

no debug vllp all 命令用来关闭所有 vllp 相关的调试开关，与命令 no debug vllp 相同。

举例

#打开 vllp 相关的所有调试开关：

```
Switch#debug vllp all
Switch#show debug vllp
VLLP debugging status:
  VLLP packet receive debugging is on
  VLLP packet send debugging is on
  VLLP event debugging is on
  VLLP efsm debugging is on
  VLLP pfsm debugging is on
Switch#
```

15.3.3 debug vllp events

debug vllp events

no debug vllp events

模式

特权模式

参数

无。

描述

debug vllp event：用来打开 vllp 事件调试开关；

no debug vllp events：用来关闭 vllp 事件调试开关。

举例

#打开 vllp 相关的事件调试开关：

```
Switch#debug vllp events
Switch#log dis
```

Switch#

2007/04/12 18:55:03 Informational: VLLP:EVENT: QT expires

2007/04/12 18:55:08 Informational: VLLP:EVENT: QT expires

Switch#

15.3.4 debug vllp packet

debug vllp packet [recv | send]

no debug vllp packet [recv | send]

模式

特权模式

参数

recv：接收的报文，跟此参数只显示接收报文的调试信息；

send：发送的报文，跟此参数只显示发送报文的调试信息。

描述

debug vllp packet 命令用来打开 vllp 报文收发调试开关，用户可以观察到本机收发 vllp 协议报文的情况；

no debug vllp packet 命令用来关闭 vllp 报文收发调试开关。

举例

#打开 vllp 协议发送报文调试开关,观察协议报文发送情况：

Switch#debug vllp pack send

Switch#log dis

Switch#

2006/12/03 19:21:30 Informational: VLLP:SEND: ge4/11 send lq

2006/12/03 19:21:30 Informational: VLLP:SEND:

Ver: 1

Type: 1

Port1: 2203

Prio: 100

QT: 5

Main: 2203

Reserved: 0

Port2: 2203

Link: 1

STP: 3

2006/12/03 19:21:30 Informational: VLLP:EVENT: send packet

2006/12/03 19:21:30 Informational: VLLP:SEND:
des_mac: 00:09:ca:ff:ff:ff
src_mac: 00:00:00:00:00:02
port_id: 2203
vlan_id: 3
data: 01 01 08 9b 64 05 08 9b 00 00 00 00 08 9b 01 03

2006/12/03 19:21:30 Informational: VLLP:SEND: ge4/9 send lq

2006/12/03 19:21:30 Informational: VLLP:SEND:
Ver: 1
Type: 1
Port1: 2201
Prio: 100
QT: 5
Main: 2203
Reserved: 0
Port2: 2201
Link: 1
STP: 2

2006/12/03 19:21:30 Informational: VLLP:EVENT: send packet

2006/12/03 19:21:30 Informational: VLLP:SEND:
des_mac: 00:09:ca:ff:ff:ff
src_mac: 00:00:00:00:00:02
port_id: 2201
vlan_id: 3
data: 01 01 08 99 64 05 08 9b 00 00 00 00 08 99 01 02

Switch#

15.3.5 debug vllp efsm

debug vllp efsm [detail]

no debug vllp efsm

模式

特权模式

参数

detail：加该参数将显示 efsm 相关的详细调试信息。

描述

debug vllp efsm 命令用来打开设备 vllp 状态机调试开关，能够观察到设备 vllp 状态变迁信息；

no debug vllp efsm 命令用来关闭 vllp 设备状态调试开关。

举例

#打开 vllp：

Switch#debug vllp efsm detail

Switch#log dis

Switch#

2006/12/03 19:24:10 Informational: VLLP:EFSM:vlan3:Sender-QueryTimer

2006/12/03 19:24:10 Informational: VLLP:EFSM: Update QT 5s

2006/12/03 19:24:10 Informational: VLLP:EFSM: Update IT 25s

2006/12/03 19:24:10 Informational: VLLP:EFSM: Query timer re-on 5s

2006/12/03 19:24:10 Informational: VLLP:EFSM: PFSM event: SendLQ

2006/12/03 19:24:10 Informational: VLLP:EFSM:vlan3:Sender-RecvLA

2006/12/03 19:24:10 Informational: VLLP:EFSM:vlan3:Sender-RecvLA

Switch#

15.3.6 debug vllp pfsm

debug vllp pfsm [detail]

no debug vllp pfsm

模式

特权模式

参数

detail：加该参数将显示 pfsm 相关的详细调试信息。

描述

debug vllp pfsm 命令用来打开 vllp 端口状态机调试开关;

no debug vllp pfsm 命令用来关闭 vllp 端口状态机调试开关。

举例

#打开 vllp：

Switch#debug vllp pfsm detail

Switch#log dis

Switch#

2006/12/03 19:23:10 Informational: VLLP:PFSM:ge4/11:Forward-SendLQ[Sender]

2006/12/03 19:23:10 Informational: VLLP:PFSM: Send LQ

2006/12/03 19:23:10 Informational: VLLP:PFSM:ge4/9:Block-SendLQ[Sender]

2006/12/03 19:23:10 Informational: VLLP:PFSM: Send LQ

2006/12/03 19:23:10 Informational: VLLP:PFSM:ge4/11:Forward-RecvLA[Sender]

2006/12/03 19:23:10 Informational: VLLP:PFSM: Set mapping port 2265

2006/12/03 19:23:10 Informational: VLLP:PFSM: Port interrupt timer on 25s

2006/12/03 19:23:10 Informational: VLLP:PFSM:ge4/9:Block-RecvLA[Sender]

2006/12/03 19:23:10 Informational: VLLP:PFSM: Set mapping port 2267

2006/12/03 19:23:10 Informational: VLLP:PFSM: Port interrupt timer re-on 25s

Switch#

第 16 章 DHCP-RELAY 命令

16.1 配置命令

16.1.1 dhcp relay

命令

dhcp relay

no dhcp relay

模式

接口配置模式。

参数

无。

描述

dhcp relay 命令用来使能接口的 dhcp-relay 功能，缺省不使能接口的 dhcp-relay 功能。

no dhcp relay 命令用来关闭接口的 dhcp-relay 功能。

举例

#使能接口 vlan10 的 dhcp-relay 功能：

Switch(config-vlan10)#dhcp relay

Switch(config-vlan10)#

16.1.2 dhcp server

命令

dhcp server <ip-address>

no dhcp server <ip-address>

模式

接口配置模式。

参数

ip-address：DHCP 服务器的 ip 地址，点分十进制格式。

描述

dhcp server 命令用来指定一个 DHCP 服务器，交换机在收到 ip 地址请求报文时将报文转发到指定的服务器请求地址（需启动 DHCP-Relay 功能）。该配

置在入接口有效，即收到客户机 IP 地址请求的接口。

no dhcp server 命令用来删除接口上的 dhcp server 相关配置。

举例

#配置接口 vlan10 上请求 ip 地址的报文发向 DHCP 服务器：172.20.3.3：

Switch(config-vlan10)#dhcp relay

Switch(config-vlan10)# dhcp server 172.20.3.3

Switch(config-vlan10)#

16.1.3 dhcp snooping

命令

dhcp snooping

no dhcp snooping

模式

全局配置模式

参数

无。

描述

dhcp snooping 命令用来启动 dhcp snooping 功能，该功能记录客户获取地址时的信息来完成 IP 地址，MAC 地址和二层接口的对应关系，记录后只能被新的 DHCP 报文或手动静态配置更改，以此避免 arp 欺骗；

no dhcp snooping 命令用来禁止 dhcp snooping 功能。

举例

#在本地交换机上启动 dhcp snooping 功能：

Switch(config)#dhcp snooping

Switch(config)#

16.2 查看命令

16.2.1 show debugging dhcp-relay

命令

show debugging dhcp-relay

模式

特权模式/普通模式。

参数

无

描述

show debugging dhcp-relay命令用来查看当前的dhcp-relay调试开关的打开情况。

举例

#查看 dhcp-relay 的调试开关打开情况：

Switch#show debugging dhcp-relay

DHCP-relay debugging status:

DHCPr packet debugging is on

Switch#

16.3 调试命令

16.3.1 debug dhcp-relay

命令

debug dhcp-relay

no debug dhcp-relay

模式

特权模式。

参数

无。

描述

debug dhcp-relay 命令用来打开当前 dhcp-relay 的调试开关，使用户能够看到 dhcp-relay 的协商过程和报文收发情况。

no debug dhcp-relay 命令用来关闭 dhcp-relay 的调试开关。

举例

#打开 dhcp-relay 的调试开关：

Switch#debug dhcp-relay

Switch#

16.3.2 debug dhcp-relay all

命令

debug dhcp-relay all

no debug dhcp-relay all

模式

特权模式。

参数

无。

描述

debug dhcp-relay all 命令用来打开所有 dhcp-relay 相关的调试开关，使用户能够看到 dhcp-relay 的协商过程和报文收发情况。

no debug dhcp-relay all 命令用来关闭所有 dhcp-relay 相关的调试开关。

举例

#打开 dhcp-relay 相关的所有调试开关：

Switch#debug dhcp-relay packet all

Switch#

16.3.3 debug dhcp-relay events

命令

debug dhcp-relay events

no debug dhcp-relay events

模式

特权模式。

参数

无。

描述

debug dhcp-relay events 命令用来打开 dhcp-relay 的事件调试开关，使用户能够看到 dhcp-relay 的协商过程。

no debug dhcp-relay events 命令用来关闭 dhcp-relay 的事件调试开关。

举例

#打开 dhcp-relay 的事件信息调试开关：

Switch#debug dhcp-relay events

Switch#

16.3.4 debug dhcp-relay packet

命令

debug dhcp-relay packet [recv | send] [detail]

no debug dhcp-relay packet [recv | send] [detail]

模式

特权模式。

参数

recv：打开接收报文调试开关。

send：打开发送报文调试开关。

detail：打开 dhcp-relay 报文的详细信息调试开关。

描述

debug dhcp-relay packet 命令用来打开当前 dhcp-relay 的报文调试开关，使用户能够看到 dhcp-relay 报文的接收/发送情况。

no debug dhcp-relay packet 命令用来关闭 dhcp-relay 的报文调试开关。

举例

#打开 dhcp-relay 的接收报文详细信息调试开关：

Switch#debug dhcp-relay packet recv detail

Switch#

第 17 章 IGMP 命令

17.1 IGMP 配置命令

17.1.1 ip igmp

命令

ip igmp

no ip igmp

模式

接口配置模式

参数

无。

描述

ip igmp 命令是启动该 vlan 的 igmp 功能。

no ip igmp 命令是关闭该 vlan 的 igmp 功能。

举例

#在 VLAN1 中打开 IGMP 功能

Switch(config-vlan1)#ip igmp

#在 VLAN1 中关闭 IGMP 功能。

Switch(config-vlan1)#no ip igmp

17.1.2 ip igmp access-group

命令

ip igmp access-group {<acl-num> | <acl-name>}

no ip igmp access-group

模式

接口配置模式

参数

acl-num：访问控制列表号，必须是<1-99>的标准访问控制列表。

acl-name；访问控制列表名。

描述

ip igmp access-group 命令是按照 access-list 规则打开 IGMP 接口组过滤功

能。

no ip igmp access-group 命令关闭 IGMP 接口组过滤功能。

举例

#启动 vlan1 的 IGMP 过滤功能，过滤条目按照 access-list 1：

Switch(config-vlan1)#ip igmp access-group 1

#关闭 vlan1 的 IGMP 组过滤功能：

Switch(config-vlan1)#no ip igmp access-group

17.1.3 ip igmp immediate-leave group-list

命令

ip igmp immediate-leave group-list {<acl-num1> | <acl-num2> | <acl-name>}

no ip igmp immediate-leave

模式

接口配置模式

参数

acl-num1：访问控制列编号，是编号<1-99>的标准访问控制列表。

acl-num2：访问控制列扩展编号，是编号<1300-1999>的标准访问控制扩展列表。

acl-name；访问控制列表名称。

描述

ip igmp immediate-leave group-list 命令是配置过滤该接口接收到版本 2 和版本 3 的离开报文时过滤的组播地址 no ip igmp immediate-leave 命令是关闭过滤离开报文组播地址的功能

举例

#配置 VLAN1 的接口过滤符合规则 1 的离开报文的组播地址

Switch(config-vlan1)#ip igmp immediate-leave group-list 1

#关闭 VLAN1 的过滤离开报文组播地址功能

Switch(config-vlan1)#no ip igmp immediate-leave

17.1.4 ip igmp last-member-query-count

命令

ip igmp last-member-query-count <L-M-Q-Count-value>

no ip igmp last-member-query-count

模式

接口配置模式

参数

L-M-Q-Count-value：特定组查询次数。默认值：2，取值范围为：2~7。

描述

ip igmp last-member-query-count 命令是配置特定组查询次数的值

no ip igmp last-member-query-count 命令是恢复该次数的值为默认值。

举例

#设置 VLAN1 内的 IGMP 特定组查询次数值为 7：

Switch(config-vlan1)#ip igmp last-member-query-count 7

#恢复 VLAN1 内的 IGMP 特定组查询次数值为默认值

Switch(config-vlan1)#no ip igmp last-member-query-count

17.1.5 ip igmp last-member-query-interval

命令

ip igmp last-member-query-interval <L-M-Q-Interval-value >

no ip igmp last-member-query-interval

模式

接口配置模式

参数

L-M-Query-Interval-value：特定组查询间隔时间。默认值：1000ms，取值范围为：1000~25500ms。

描述

ip igmp last-member-query-interval 命令是配置当发送特定组查询报文的间隔时间

no ip igmp last-member-query-interval 命令是恢复该间隔时间为默认值

举例

#配置发送特定组查询报文的间隔时间为 2000ms

Switch(config-vlan1)#ip igmp last-member-query-interval 2000

#恢复该间隔时间为默认值

Switch(config-vlan1)#no ip igmp last-member-query-interval

17.1.6 ip igmp querier-timeout

命令

ip igmp querier-timeout <timeout-value >

no ip igmp querier-timeout

模式

接口配置模式

参数

timeout-value ：非查询者计时器时间。默认值：255s，取值范围为：60~300s。

描述

ip igmp querier-timeout 命令是配置非查询者计时器时间。

no ip igmp querier-timeout 命令是恢复默认值。

举例

#配置 vlan1 的非查询者计时器时间为 60s：

Switch(config-vlan1)#ip igmp querier-timeout 60

#恢复 vlan1 的非查询者计时器时间为默认值：

Switch(config-vlan1)#no ip igmp querier-timeout

17.1.7 ip igmp query-interval

命令

ip igmp query-interval <Interval-value>

no ip igmp query-interval

模式

接口配置模式

参数

Interval-value：发送查询报文间隔时间。默认值：125s，取值范围为：1~18000s。

描述

ip igmp query-interval 命令是配置发送查询报文的间隔时间。

no ip igmp query-interval 命令是恢复间隔时间为默认值

举例

#设置 VLAN1 发送查询报文的间隔时间为 100s：

Switch(config-vlan1)#ip igmp query-interval 100

#恢复间隔时间为默认值

Switch(config-vlan1)#no ip igmp query-interval

17.1.8 ip igmp query-max-response-time

命令

ip igmp query-max-response-time <respone-time>

no ip igmp query-max-response-time

模式

接口配置模式

参数

respone-time：IGMP 查询报文中的最大响应时间。默认值：10s，取值范围为 1~240s。

描述

ip igmp query-max-response-time 命令是配置 IGMP 查询报文中的最大响应时间。

no ip igmp query-max-response-time 命令是恢复最大响应时间为默认值

举例

#设置 VLAN1 的 IGMP 查询报文中的最大响应时间为 20s：

Switch(config-vlan1)#ip igmp query-max-response-time 20

#恢复查询报文中的最大响应时间为默认值

Switch(config-vlan1)#no ip igmp query-max-response-time

17.1.9 ip igmp robustness-variable

命令

ip igmp robustness-variable <Robust-value>

no ip igmp robust-variable

模式

接口配置模式

参数

Robust-value：IGMP 健壮系数，当 IGMP 收到离开报文时，发送 IGMP 特定组查询报文的重传次数。默认值：2，取值范围为 2~7。

描述

ip igmp robustness-variable 命令是配置当 IGMP 收到离开报文时，发送

IGMP 特定组查询报文的次数。

no ip igmp robustness-variable 命令是恢复发送次数为默认值

举例

#设置 VLAN1 的 IGMP 发送特定组查询次数为 4：

Switch(config-vlan1)#ip igmp robustness-variable 4

#恢复 VLAN1 的 IGMP 发送特定组查询次数为默认值

Switch(config-vlan1)#no ip igmp robustness-variable

17.1.10 ip igmp version

命令

ip igmp version <Version Number>

no ip igmp version

模式

接口配置模式

参数

Version Number：IGMP 版本号。默认值：3，取值范围为 1~3。

描述

ip igmp version 命令是配置运行 IGMP 的版本。

no ip igmp version 命令是恢复发送查询报文版本为默认值

举例

#设置 VLAN1 的 IGMP 发送查询报文的版本为 2：

Switch(config-vlan1)#ip igmp version 2

#恢复 VLAN1 的 IGMP 发送查询报文的版本为默认值

Switch(config-vlan1)#no ip igmp version

17.2 IGMP 查看命令

17.2.1 show ip igmp groups

命令

show ip igmp groups [<A.B.C.D> [detail] | <interface-name> [<A.B.C.D> [detail] | detail] | detail]

模式

普通模式/特权模式

参数

A.B.C.D：组播组地址

interface：指定接口。这里指的是 VLAN 接口。

描述

show igmp group 命令是显示相关的组播组信息。

举例

#显示存在的 igmp group 信息：

Switch#show ip igmp groups

17.2.2 show ip igmp interface

命令

show ip igmp interface [<if-name>]

模式

普通模式/特权模式

参数

if-name：指定接口。这里指定的是 VLAN 接口。

描述

show ip igmp interface 命令是显示 IGMP 接口配置信息。

举例

#显示 vlan3 的 IGMP 配置信息：

Switch#show ip igmp interface vlan3

Switch#

17.3 IGMP 调试命令

17.3.1 debug igmp

命令

debug igmp [all] | [events] | [fsm] | [packet] | [tib]

no debug igmp [all] | [events] | [fsm] | [packet] | [tib]

模式

特权模式。

参数

all：打开 igmp 所有得调试开关。

events：打开 igmp 事件调试开关。

fsm：IGMP 接口有限状态机

packet：打开 igmp 报文调试开关。

tib：IGMP 信息状态表

描述

debug igmp 命令用来打开 igmp 相关调试开关，使用户能够看到 igmp 的相关事件和报文收发情况。

no debug igmp 命令关闭对应的 igmp 调试开关。

举例

#打开 igmp 报文调试开关：

Switch#debug igmp packet

Switch#

17.3.2 show debug igmp

命令

show debug igmp

模式

普通模式/特权模式

参数

无。

描述

Show debug igmp 命令用来显示 igmp 相关调试开关的状态。

举例

#显示 igmp 报文调试开关状态：

Switch#show debug igmp

Switch#

第 18 章 PIM-SM 命令

18.1 系统配置命令

18.1.1 ip mroute

ip mroute <source-address> <group-address> <iif-name> <oif-name> {add | remove} <L2-port>

模式

全局配置模式

参数

source-address：组播路由（S,G）中对应的源 IP 地址；

group-address：组播组地址，用于指定一个组播组，取值范围是 224.0.0.0~239.255.255.255;

iif-name：组播路由的入接口名，必须是三层 vlan 接口；

oif-name：组播路由的出接口名，必须是三层 vlan 接口；

L2-port：需要加入或移出转发端口列表的二层端口，可以是 Trunk 端口组，但不能是某个 Trunk 组的成员端口。

描述

在 iSpirit8800 系列交换机上，存在一条激活的组播路由时是将一个三层接口内所有的二层端口全部置为转发状态。ip mroute 命令用来手动配置三层接口内哪些二层端口是组播的有效端口。source-address、group-address 和 iif-name 唯一确定一条组播路由。当 oif-name 包含多个二层端口时，ip mroute 命令用来将指定的二层端口加入或移出转发列表中。

举例

#有接口 vlan3，包含二层端口 ge2/4、ge4/5 和 ge4/6，对于从 vlan2 进入的组(192.168.1.12,224.1.1.10)的数据流，在 vlan3 为出接口时只允许从 ge2/4 转发：

Switch(config)#ip mroute 192.168.1.12 224.1.1.10 vlan2 vlan3 remove ge4/5

Switch(config)#ip mroute 192.168.1.12 224.1.1.10 vlan2 vlan3 remove ge4/6

Switch(config)#

#上述条件下，ge4/5 的用户通过申请允许接收该数据流：

Switch(config)#ip mroute 192.168.1.12 224.1.1.10 vlan2 vlan3 add ge4/5
Switch(config)#

18.1.2 ip multicast route-limit

命令

ip multicast route-limit <max-num> [<alarm-num>]
no ip multicast route-limit

模式

配置模式。

参数

max-num：组播路由的上限值；取值范围 1～2147483647；
alarm-num：发出告警的组播路由数，取值范围 1～2147483647。

描述

ip ip multicast route-limit 命令用来配置组播路由上限和发出告警的数目；超出上限后不再增加组播路由，达到告警值时发出告警信息。
no ip ip multicast route-limit 命令用来取消对组播路由条数的限制。

举例

#配置系统允许最多 300 条组播路由，达到 250 条时发出告警：
Switch(config)#ip multicast route-limit 300 250
Switch(config)#

18.1.3 ip multicast-routing

命令

ip multicast-routing
no ip multicast-routing

模式

配置模式。

参数

无

描述

ip multicast-routing 命令用来启动系统的组播路由功能；
no ip multicast-routing 命令用来禁止组播路由功能。

举例

#启动系统的组播路由功能：

Switch(config)#ip multicast-routing

Switch(config)#

18.1.4 ip pim accept-register

命令

ip pim accept-register {list} {<acl-num> | <acl-name>}

no ip pim accept-register

模式

配置模式。

参数

acl-num：访问控制列表号，必须是<100-199>或<2000-2699>的扩展访问控制列表。

acl-name；访问控制列表名。

描述

ip pim accept-register 命令用来配置注册过滤器，只有注册消息包含的源地址通过了 ACL 过滤才会被处理。

no ip pim accept-register 命令用来取消注册者过滤配置。

举例

#调用名为 reg-filter 的访问控制列表，对注册者进行过滤：

Switch(config)#ip pim accept-register list reg-filter

Switch(config)#access-list reg-filter permit 192.168.10.1/32

Switch(config)#access-list reg-filter deny any

Switch(config)#end

Switch#show access-list

String IP access list reg-filter,

permit 192.168.10.1/32

deny any

Switch#

18.1.5 ip pim bsr-candidate

命令

ip pim bsr-candidate {<if-name>} [<mask-len>]

no ip pim bsr-candidate

模式

配置模式。

参数

if-name：指定需要参与 BSR 选举的接口名；

mask-len：进行 bsr 计算时使用的掩码长度，取值范围 0～32；

描述

ip pim bsr-candidate 命令用来配置接口使用其 ip 地址作为 C-BSR，参与 BSR 的选举。

no ip pim bsr-candidate 命令用来取消接口的 C-BSR 指定

举例

#配置本地接口 vlan4 的地址参与 BSR 的选举

Switch(config)#ip pim bsr-candidate vlan4

Switch(config)#

18.1.6 ip pim cisco-register-checksum

命令

ip pim cisco-register-checksum [group-list <acl-num> | <acl-name>]

no ip pim cisco-register-checksum [group-list <acl-num> | <acl-name>]

模式

配置模式。

参数

acl-num：访问控制列表号，必须是<1-99>或<1300-1999>的标准访问控制列表。

acl-name；访问控制列表名。

描述

ip pim cisco-register-checksum 命令用来配置系统对通过了 ACL 过滤的组能够兼容 Cisco 的报文校验和检查功能。不使用 ACL 规则时该命令对所有组有效。

No ip pim cisco-register-checksum 命令用来删除系统兼容 Cisco 的报文校验和检查功能的配置。

举例

#配置对所有组兼容 Cisco 的注册校验和机制：

Switch(config)#ip pim cisco-register-checksum

Switch(config)#

18.1.7 ip pim crp-cisco-prefix

命令

ip pim crp-cisco-prefix

no ip pim crp-cisco-prefix

模式

配置模式。

参数

无。

描述

ip pim crp-cisco-prefix 命令用来配置启动 C-RP 的接口能够与 Cisco 的 BSR 兼容。

no ip pim crp-cisco-prefix 命令用来取消兼容 Cisco 设备作为 BSR。

举例

#配置系统兼容 Cisco 设备作为 BSR：

Switch(config)#ip pim crp-cisco-prefix

Switch(config)#

18.1.8 ip pim ignore-rp-set-priority

命令

ip pim ignore-rp-set-priority

no ip pim ignore-rp-set-priority

模式

配置模式。

参数

无。

描述

ip pim ignore-rp-set-priority 命令用来配置系统接收 RP-Set 时忽略 RP 的优先级。

no ip pim ignore-rp-set-priority 用来删除忽略 RP-Set 优先级的配置，恢复到默认配置，检查 RP 的优先级。

举例

#配置系统忽略 RP-Set 的优先级：

Switch(config)#ip pim ignore-rp-set-priority

Switch(config)#

18.1.9 ip pim jp-timer

命令

ip pim jp-timer <jp-interval>

no ip pim jp-timer [<jp-interval>]

模式

配置模式。

参数

jp-interval：发送加入/剪枝消息的时间间隔；取值范围 1～65535；默认值为 60 秒。

描述

ip pim jp-timer 命令用来配置系统周期性加入/剪枝消息定时器的时间间隔。

no ip pim jp-timer 命令用来恢复系统周期性加入/剪枝消息定时器时间间隔到缺省值。

举例

#配置系统发送加入/剪枝消息的时间间隔为 75 秒：

Switch(config)#ip pim jp-timer 75

Switch(config)#

18.1.10 ip pim register-rate-limit

命令

ip pim register-rate-limit <rate-value>

no ip pim register-rate-limit

模式

配置模式。

参数

rate-value：接收注册报文的速率上限，超出设置值时丢弃报文；取值范围 1～65535；缺省不做限制。

描述

ip pim register-rate-limit 命令用来配置系统接收注册消息的上限速率，配置一个较小的值能够一定程度上减少 CPU 的负担。

no ip pim register-rate-limit 命令用来恢复到缺省情况，不对注册消息速率做限制。

举例

#配置接收注册消息的速率上限为 1000pkt/s

Switch(config)#ip pim register-rate-limit 1000

Switch(config)#

18.1.11 ip pim register-rp-reachability

命令

ip pim register-rp-reachability

no ip pim register-rp-reachability

模式

配置模式。

参数

无。

描述

ip pim register-rp-reachability 命令用来配置系统启动 RP 可达性检查。

no ip pim register-rp-reachability 命令用来恢复到缺省情况，不检查 RP 的可达性。

举例

#配置系统启动 RP 可达性检查功能：

Switch(config)#ip pim register-rp-reachability

Switch(config)#

18.1.12 ip pim register-source

命令

ip pim register-source {<ip-address> | <if-name>}

no ip pim register-source

模式

配置模式。

参数

ip-address：32 位点分 10 进制 ip 地址。

if-name：接口名。

描述

ip pim register-source 命令用来指定一个 ip 地址（或指定接口的 ip 地址）作为发送注册消息时封装的原地址，缺省情况下使用发送注册消息的真实接口地址。

no ip pim register-source 命令用来恢复到缺省配置。

举例

#配置发送注册消息时，封装接口 vlan1024 的地址作为源地址：

Switch(config)#ip pim register-source vlan1024

Switch(config)#

18.1.13 ip pim register-suppression

命令

ip pim register-suppression <timer-value>

no ip pim register-suppression

模式

配置模式。

参数

timer-value：定时器的时间值，单位为秒，取值范围：1～65535；缺省值为 60 秒。

描述

ip pim register-suppression 命令用来配置注册抑制定时器的抑制时间。

no ip pim register-suppression 命令用来恢复注册抑制定时器的值到缺省配置。

举例

#配置注册抑制定时器的抑制时间为 300 秒：

Switch(config)#ip pim register-suppression 300

Switch(config)#

18.1.14 ip pim rp-address

命令

ip pim rp-address <ip-address> [<acl-num> | <acl-name>]

no ip pim rp-address <ip-address> [<acl-num> | <acl-name>]

模式

配置模式。

参数

acl-num：访问控制列表号，必须是<1-99>或<1300-1999>的标准访问控制列表。

acl-name；访问控制列表名。

描述

ip pim rp-address 命令为通过访问控制列表过滤的组静态配置 RP，不使用访问控制列表时该 RP 配置对所有组有效。

no ip pim rp-address 命令删除对应的静态 RP 配置。

举例

#配置所有组使用静态 RP192.168.93.3：

Switch(config)#ip pim rp-address 192.168.93.3

Switch(config)#

18.1.15 ip pim rp-candidate

命令

ip pim rp-candidate <if-name> [group-list <acl-num> | <acl-name>] [interval <adv-interval>] [priority <priority-value>]

no ip pim rp-candidate <if-name>

模式

配置模式。

参数

if-name：接口名。

acl-num：访问控制列表号，必须是 1-99 的标准访问控制列表。

acl-name；访问控制列表名。

adv-interval：C-RP-Adv 消息的通告周期，单位为秒，取值范围为 1～16383。

priority-value：优先级，取值范围 0～255。

描述

ip pim rp-candidate 命令用来配置一个接口作为 C-RP（候选 RP），同时指定 C-RP 的参数。

no ip pim rp-candidate 命令删除候选 RP 的配置。

举例

#配置 vlan4 使用缺省参数作为候选 RP：

Switch(config)#ip pim rp-candidate vlan4

Switch(config)#

18.1.16 ip pim rp-register-kat

命令

ip pim rp-register-kat <kat-value>

no ip pim rp-register-kat

模式

配置模式。

参数

kat-value：保活时间值，取值范围 1～65535。

描述

ip pim rp-register-kat 命令用来配置注册保活时间。

no ip pim rp-register-kat 命令用来恢复注册保活时间到缺省值。

举例

#配置注册者保活时间为 250 秒：

Switch(config)#ip pim rp-register-kat 250

Switch(config)#

18.1.17 ip pim spt-threshold

命令

ip pim spt-threshold [group-list <acl-num | acl-name>]

no ip pim spt-threshold [group-list <acl-num | acl-name>]

模式

配置模式。

参数

缺省：对所有组的组播路由实现切换；

acl-num：访问控制列表号，必须是<1-99>或<1300-1999>的标准访问控制列表。

acl-name；访问控制列表名。

描述

ip pim spt-threshold 命令用来配置 PIM-SM 从 RPT 向 SPT 的切换的门限值，缺省为无条件切换,即门限值为 0。默认情况下所有组无条件切换到 SPT。

no ip pim spt-threshold 命令用来删除切换配置。

举例

#配置通过 grp-list 控制只有组 234.1.1.1 向 SPT 切换：

Switch(config)#ip pim spt-threshold group-list grp-list

Switch(config)#access-list grp-list per 234.1.1.1/32

Switch(config)#

18.2 接口配置命令

18.2.1 ip pim dr-priority

命令

ip pim dr-priority <priority>

no ip pim dr-priority [<priority>]

模式

接口配置模式。

参数

priority：接口进行 DR 选举时使用的优先级值。取值范围：0～4294967294，缺省值为 1。

描述

ip pim dr-priority 命令用来配置该接口参与 DR 选举时使用的优先级值；

no ip pim dr-priority 命令用来恢复接口参与 DR 选举时使用缺省值 1。

举例

#配置接口 vlan10 的 DR 优先级为 123

Switch(config)#interface vlan100

```
Switch(config-vlan100)#ip pim dr-priority 123
Switch(config-vlan100)#end
Switch#show ip pim sparse-mode interface detail

vlan100 (vif 3):
  Address 192.168.100.1, DR 192.168.100.1
  Hello period 30 seconds, Next Hello in 13 seconds
  Triggered Hello period 5 seconds
  Neighbors:

Switch#
```

18.2.2 ip pim exclude-genid

命令

ip pim exclude-genid
no ip pim exclude-genid

模式

接口配置模式。

参数

无。

描述

ip pim exclude-genid 命令用来配置本地发出的 PIM-SM hello 报文中不包含 Gen-id，缺省时包含 Gen-id；

no ip pim exclude-genid 命令用来恢复到缺省配置，不在 hello 中包含 Gen-id。

举例

```
#使能 vlan10 上的
Switch(config-vlan10)#ip pim exclude-genid
Switch(config-vlan10)#
```

18.2.3 ip pim hello-holdtime

命令

ip pim hello-holdtime <holdtime>
no ip pim hello-holdtime

模式

接口配置模式。

参数

holdtime：接口上的 hello 报文有效定时器时间。单位为秒。取值范围：1～65535；默认值为 105 秒：

描述

ip pim hello-holdtime 命令用来配置 hello 报文的保持时间，自最后一次收到邻居的 hello 报文开始计时，超时还没有收到邻居的 hello 报文则认为邻居已经不存在；

no ip pim hello-holdtime 命令用来恢复 hello 报文保持时间到默认值。

举例

#配置接口 vlan100 的 hello-holdtime 时间为 123 秒

Switch(config)#interface vlan100

Switch(config-vlan100)#ip pim hello-holdtime 123

Switch(config-vlan100)#

18.2.4 ip pim hello-interval

命令

ip pim hello-interval <interval>

no ip pim hello-interval

模式

接口配置模式。

参数

interval：周期性发送 hello 报文的时间间隔，单位为秒。取值范围：1～65535；默认值：30 秒。

描述

ip pim hello-interval 命令用来配置接口上 hello 报文发送的时间间隔；

no ip pim hello-interval 命令用来删除接口上 hello 报文发送的时间配置，恢复到缺省值。

举例

#配置接口 vlan100 的 hello-interval 时间为 25 秒

Switch(config)#inter vlan100

Switch(config-vlan100)#ip pim hello-intervla 25

```
Switch(config-vlan100)#end
Switch# show ip pim sparse-mode interface detail
vlan100 (vif 3):
  Address 192.168.100.1, DR 192.168.100.1
  Hello period 25 seconds, Next Hello in 18 seconds
  Triggered Hello period 5 seconds
  Neighbors:

Switch#
```

18.2.5 ip pim neighbor-filter

命令

```
ip pim neighbor-filter {< acl-num> | <acl-name>}
no ip pim neighbor-filter {< acl-num> | <acl-name>}
```

模式

接口配置模式。

参数

acl-num：访问控制列表号，必须是<1-99>的标准访问控制列表。

acl-name；访问控制列表名。

描述

ip pim neighbor-filter 命令用来配置接口上的邻居过滤功能，通过了访问控制列表过滤的路由器才能成为本地邻居；

no ip pim neighbor-filter 命令用来恢删除邻居过滤配置，不对邻居进行过滤。

举例

#配置接口 vlan100 上调用名为 simple 的访问控制列表对邻居进行过滤，拒绝 ip 地址为 192.168.100.4～192.168.100.7 作为自己的邻居：

```
Switch(config)#access-list simple deny 192.168.100.4/30
Switch(config)#access-list simple permit any
Switch(config)#interface vlan100
Switch(config-vlan100)#ip pim neighbor-filter simple
Switch(config-vlan100)#
```

18.2.6 ip pim sparse-mode

命令

ip pim sparse-mode

no ip pim sparse-mode

模式

接口配置模式。

参数

无。

描述

ip pim sparse-mode 命令用来使能接口的 PIM-SM 功能；

no ip pim sparse-mode 命令用来禁止接口的 PIM-SM 功能。

举例

#在接口 vlan100 上使能 PIM-SM：

Switch(config-vlan100)#ip pim sparse-mode

Switch(config-vlan100)#

18.2.7 ip pim sparse-mode passive

命令

ip pim sparse-mode passive

no ip pim sparse-mode passive

模式

接口配置模式。

参数

无。

描述

ip pim sparse-mode passive 命令用来使能接口上的 PIM-SM 抑制功能,配置后该接口能够正常处理接收到的 PIM-SM 协议报文，但不发送 PIM-SM 协议报文；

no ip pim sparse-mode passive 命令用来禁止接口的 PIM-SM 抑制功能。

举例

#在接口 vlan100 上使能 PIM-SM 接口抑制功能：

Switch(config-vlan100)#ip pim sparse-mode passive

Switch(config-vlan100)#

18.2.8 ip multicast ttl-threshold

命令

ip multicast ttl-threshold <ttl-value>

no ip multicast ttl-threshold

模式

接口配置模式。

参数

ttl-value：指定组播路由输出接口列表的 ttl 值，取值范围：0～255；缺省值为 255。

描述

ip multicast ttl-threshold 命令用来配置接口上封装组播报文时 ip 包的 TTL 值，通过 TTL 值限制报文传递的范围。

no ip multicast ttl-threshold 命令用来恢复接口上组播报文封装的 TTL 值到默认值。

举例

#在接口 vlan100 上配置组播 ip 包 TTL 值为 10：

Switch(config-vlan100)# ip multicast ttl-threshold 10

Switch(config-vlan100)#

18.3 查看命令

18.3.1 show debugging pim sparse-mode

命令

show debugging pim sparse-mode

模式

普通模式/特权模式。

参数

无。

描述

show debugging pim sparse-mode 命令用来显示 PIM-SM 各个调试开关的打

开情况。

举例

#显示当前系统打开的 PIM-SM 调试开关：

Switch#show debugging pim sparse-mode

PIM-SM debugging status:

PIM event debugging is on

PIM packet debugging is on

Switch#

18.3.2 show ip mroute

命令

show ip mroute [<ip-address> | count | dense | sparse | summary]

模式

普通模式/特权模式。

参数

缺省：显示所有的组播路由信息

ip-address：组地址或源地址,32 位点分十进制；

count：统计出的组播路由条数；

dense：PIM 密集模式（PIM-DM）；

sparse：PIM 稀疏模式（PIM-SM）；

summary：简单摘要信息。

描述

show ip mroute 命令用来显示组播路由信息包含组播路由的源，组地址，入接口列表，出接口列表及相关的定时器信息。

举例

#显示当前稀疏模式的组播路由信息：

Switch#show ip mrout sparse

IP Multicast Routing Table

Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed

Timers: Uptime/Stat Expiry

Interface State: Interface (TTL)

(192.168.77.3, 233.1.1.1), uptime 00:01:04, stat expires 00:03:24

```
Owner PIM-SM, Flags: TF
  Incoming interface: vlan400
  Outgoing interface list:
    vlan1024 (1)

(192.168.77.3, 233.1.1.2), uptime 00:01:04, stat expires 00:03:24
Owner PIM-SM, Flags: TF
  Incoming interface: vlan400
  Outgoing interface list:
    vlan1024 (1)

(192.168.77.3, 233.1.1.3), uptime 00:01:04, stat expires 00:03:24
Owner PIM-SM, Flags: TF
  Incoming interface: vlan400
  Outgoing interface list:
    vlan1024 (1)

Switch#
```

18.3.3 show ip mvif

命令

show ip mvif [<if-name>]

模式

普通模式/特权模式。

参数

if-name：接口名，指定需要显示的接口；

缺省：显示所有接口的信息；

描述

show ip mvif 命令用来显示组播接口索引，更新时间，接口地址等接口属性。

举例

#显示当前组播接口信息：

```
Switch#show ip mvif
Interface   Vif    Owner      TTL   Local          Remote         Uptime
            Idx    Module           Address        Address
vlan1024    0      PIM-SM     1     192.168.8.2    0.0.0.0        00:15:27
```

```
Register   1                1     192.168.8.2    0.0.0.0        00:15:27
vlan400    2     PIM-SM    1     192.168.77.2   0.0.0.0        00:06:28
Switch#
```

18.3.4 show ip pim sparse-mode bsr-router

命令

show ip pim sparse-mode bsr-router

模式

普通模式/特权模式。

参数

无

描述

show ip pim sparse-mode bsr-router 命令用来显示稀疏模式中的 BSR 路由器信息。

举例

#显示当 BSR 路由器信息：

```
Switch#show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 192.168.100.1
  Uptime:        00:00:11, BSR Priority: 0, Hash mask length: 10
  Expires:       00:01:59
  Role: Candidate BSR
  State: Pending BSR

  Candidate RP: 192.168.100.1(vlan100)
    Advertisement interval 60 seconds
    Next Cand_RP_advertisement in 00:00:40
Switch#
```

18.3.5 show ip pim sparse-mode interface

命令

show ip pim sparse-mode interface [detail]

模式

普通模式/特权模式。

参数

缺省：显示 PIM-SM 接口的摘要信息；

detail：显示 PIM-SM 接口的详细信息。

描述

show ip pim sparse-mode interface 命令用来显示系统启动了 PIM-SM 的接口信息,包括接口名，接口地址，邻居及 DR 状态等。

举例

#显示系统启动 PIM-SM 的接口信息：

```
Switch#show ip pim sparse-mode interface detail
vlan11 (vif 2):
   Address 192.168.11.4, DR 192.168.11.4
   Hello period 30 seconds, Next Hello in 20 seconds
   Triggered Hello period 5 seconds
   Neighbors:
    192.168.11.3

Switch#
```

#显示 PIM-SM 接口的摘要信息：

```
Switch#show ip pim sparse-mode interface
Address         Interface VIFindex    Ver/     Nbr      DR      DR
                                      ode      Count    Prior
192.168.11.4    vlan11    2           v2/S     1        1       192.168.11.4
Switch#
```

18.3.6 show ip pim sparse-mode local-members

命令

show ip pim sparse-mode local-members [ifname]

模式

普通模式/特权模式。

参数

缺省：显示系统当前所有 PIM-SM 本地成员信息；

ifname：指定接口名，显示该接口相关的本地成员。

描述

show ip pim sparse-mode local-members 命令用来显示系统启动了 PIM-SM 的接口信息,包括接口名，接口地址，邻居及 DR 状态等。

举例

#显示系统本地成员信息：

Switch#show ip pim sparse-mode local-members
PIM Local membership information

vlan1024:

vlan400:

Switch#

18.3.7 show ip pim sparse-mode mroute

命令

show ip pim sparse-mode mroute

模式

普通模式/特权模式。

参数

无。

描述

show ip pim sparse-mode mroute 命令用来显示 PIM-SM 的组播路由信息，包括（*,*,RP)，(*,G)，(S,G)，(S,G,RPT）等各种类型的组播路由项。

举例

#显示系统的 PIM-SM 组播路由信息：

Switch#show ip pim sp mrout
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 2
(S,G,rpt) Entries: 1
FCR Entries: 0

```
(*, 233.1.1.1)
RP: 192.168.8.4
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
  Local:       vlan93
  Joined:
  Asserted:
FCR:

(192.168.8.2, 233.1.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
  Local:
  Joined:     reg
  Asserted:
  Outgoing: vlan93 reg

(192.168.8.2, 233.1.1.1, rpt)
RP: 192.168.8.4
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: NOT PRUNED
  Local:
  Pruned:
  Outgoing: vlan93

Switch#
```

18.3.8 show ip pim sparse-mode neighbor

命令

show ip pim sparse-mode neighbor [detail]

模式

普通模式/特权模式。

参数

缺省：缺省显示邻居摘要信息。

detail：显示邻居的详细信息。

描述

show ip pim sparse-mode neighbor 命令用来显示 PIM-SM 组播邻居信息，包含邻居 ip 地址，发现时间和超时时间，与邻居连接的本地接口，邻居优先级等信息。

举例

#显示系统的 PIM-SM 组播路由信息：

```
Switch#show ip pim sparse-mode neighbor
Neighbor        Interface        Uptime/Expires       Ver     DR Priority/Mode
Address
192.168.11.3    vlan11           01d03h39m/00:01:44 v2      N /
Switch#
```

18.3.9 show ip pim sparse-mode nexthop

命令

show ip pim sparse-mode nexthop

模式

普通模式/特权模式。

参数

无。

描述

show ip pim sparse-mode nexthop 命令用来显示 PIM-SM 进行 RPF 计算出的下一跳地址。

举例

#显示当前系统中组播路由的下一跳信息：

```
Switch#show ip pim sp nex
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination Type Nexthop Nexthop    Nexthop Nexthop Metric Pref    Refcnt
                 Num      Addr       Ifindex  Name
_____________________________________________________________________
192.168.8.2    ..S.  1        0.0.0.0        4                0        0      4
192.168.10.3 .R..    1      192.168.101.3    7                2      120      8
```

Switch#

18.3.10 show ip pim sparse-mode rp

命令

show ip pim sparse-mode rp <mapping>

模式

普通模式/特权模式。

参数

mapping：RP 与组的映射。

描述

show ip pim sparse-mode rp mapping 命令用来显示当前 PIM-SM 中 RP 与组的映射关系，包括 RP 地址，RP 映射的组，正常运行的时间等。

举例

#显示当前系统的 RP 映射关系：

Switch#show ip pim sparse-mode rp mapping

PIM Group-to-RP Mappings

Group(s): 224.0.0.0/4, Static

RP: 192.168.11.4

Uptime: 01d06h33m

Switch#

18.3.11 show ip pim sparse-mode rp-hash

命令

show ip pim sparse-mode rp-hash <grp-address>

模式

普通模式/特权模式。

参数

grp-address：指定组地址。

描述

show ip pim sparse-mode rp-hash 命令用来显示指定的组通过 hash 算法映射的 RP。

举例

#显示组 234.1.1.1 在当前系统中的 RP 选择：

```
Switch#show ip pim sparse-mode rp-hash 234.1.1.1
    RP: 192.168.11.4
Switch#
```

18.4 诊断与调试命令

18.4.1 debug pim sparse-mode

命令

debug pim spare-mode

no debug pim sparse-mode

模式

特权模式。

参数

无。

描述

debug pim sparse-mode 命令用来打开 PIM-SM 相关的所有调试开关，能够在终端输出调试信息。

no debug pim sparse-mode 命令用来关闭 PIM-SM 的调试开关。

举例

#打开系统的 PIM-SM 调试开关：

```
Switch#debug pim sparse-mode
Switch#show debugging pim sparse-mode
PIM-SM debugging status:
  PIM event debugging is on
  PIM MFC debugging is on
  PIM state debugging is on
  PIM 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 nsm debugging is on
PIM nexthop debugging is on
Switch#

18.4.2 debug pim sparese-mode all

命令

debug pim spare-mode all
no debug pim sparse-mode all

模式

特权模式。

参数

无。

描述

debug pim sparse-mode all 命令用来打开 PIM-SM 相关的所有调试开关，能够在终端输出所有 PIM-SM 的调试信息。

no debug pim sparse-mode all 命令用来关闭 PIM-SM 的所有调试开关。

举例

#打开系统所有的 PIM-SM 调试开关：
Switch#debug pim sparse-mode all
Switch#

18.4.3 debug pim sparse-mode event

命令

debug pim spare-mode events
no debug pim sparse-mode events

模式

特权模式。

参数

无。

描述

debug pim sparse-mode events 命令用来打开 PIM-SM 的事件调试开关，能够在终端输出事件调试信息。

no debug pim sparse-mode events 命令用来关闭 PIM-SM 的事件调试开关。

举例

#打开 PIM-SM 事件调试开关：

Switch#debug pim sparse-mode events

Switch#log display

Switch#

2006/10/26 15:11:39 Informational: PIM-SM: WholePkt message: src 192.168.8.2 for 233.1.1.2 vif 1

2006/10/26 15:11:40 Informational: PIM-SM: Hello Timer expired on vlan100

2006/10/26 15:11:40 Informational: PIM-SM: Restarting Hello Timer on vlan100 with 30 secs timeout

2006/10/26 15:11:40 Informational: PIM-SM: Stopping Triggered Hello Timer on vlan100

Switch#no log display

Switch#

18.4.4 debug pim sparse-mode mfc

命令

debug pim spare-mode mfc

no debug pim sparse-mode mfc

模式

特权模式。

参数

无。

描述

debug pim sparse-mode mfc 命令用来打开 PIM-SM 的 MFC 调试开关，能够在终端输出组播路由写入和删除的相关调试信息。

no debug pim sparse-mode mfc 命令用来关闭 PIM-SM 的 MFC 调试开关。

举例

#打开 PIM-SM 的 MFC 调试开关：

```
Switch#debug pim sparse-mode mfc
Switch#show debugging pim sparse-mode
PIM-SM debugging status:
  PIM MFC debugging is on
Switch#log display
Switch#

 2006/10/26 15:16:51 Informational: PIM-SM: MFC add message to MRIB for (192.168.8.2, 233.1.1.2) iif:2 olist:0x00000002 succeeded

 2006/10/26 15:16:51 Informational: PIM-SM: MFC add message to MRIB for (192.168.8.2, 233.1.1.1) iif:2 olist:0x00000002 succeeded

 2006/10/26 15:16:51 Informational: PIM-SM: MRT ADD notification for (192.168.8.2, 233.1.1.2) status: 14 msg_id: 312

 2006/10/26 15:16:51 Informational: PIM-SM: MRIB MRT add for (192.168.8.2, 233.1.1.2) MRT succeeded

 2006/10/26 15:16:51 Informational: PIM-SM: MRT ADD notification for (192.168.8.2, 233.1.1.1) status: 14 msg_id: 313

 2006/10/26 15:16:51 Informational: PIM-SM: MRIB MRT add for (192.168.8.2, 233.1.1.1) MRT succeeded

Switch#no log display
```

18.4.5 debug pim sparse-mode mib

命令

debug pim spare-mode mib

no debug pim sparse-mode mib

模式

特权模式。

参数

无。

描述

debug pim sparse-mode mib 来打开 PIM-SM 的 mib 关,能够在终端输出 pim 组播路由发生变化的调试信息。

no debug pim sparse-mode mib 来关闭 PIM-SM 的 mib 调试开关。

举例

Switch#debug pim sparse-mode mib
Switch#

18.4.6 debug pim sparse-mode nexthop

命令

debug pim spare-mode nexthop
no debug pim sparse-mode nexthop

模式

特权模式。

参数

无。

描述

debug pim sparse-mode nexthop 来打开组播路由下一跳的相关调试信息。

no debug pim sparse-mode nexthop 来关闭组播下一跳调试信息。

举例

#打开下一跳检查调试开关，显示组播下一跳相关信息
Switch#debug pim sparse-mode nexthop
Switch#show debugging pim sparse-mode
PIM-SM debugging status:
  PIM nexthop debugging is on
Switch#log display
Switch#

2006/10/26 16:34:54 Informational: PIM-SM: Nexthop 192.168.8.4:

Increment refcnt 3

2006/10/26 16:34:54 Informational: PIM-SM: Nexthop 192.168.8.2: Increment refcnt 3

2006/10/26 16:34:54 Informational: PIM-SM: Nexthop 192.168.8.4: Increment refcnt 4

Switch#no log display

18.4.7 debug pim sparse-mode packets

命令

debug pim spare-mode packets [recv | send]

no debug pim sparse-mode packets [rec | send]

模式

特权模式。

参数

recv：接收到的报文。

send：发送的报文。

缺省时接收和发送都打开。

描述

debug pim sparse-mode packets 命令用来打开 PIM-SM 的报文调试开关，能够在终端输出收到和发送 pim 协议报文的相关信息。

no debug pim sparse-mode packets 来关闭 PIM-SM 的报文调试开关。

举例

#打开 pim-sm 接收报文调试开关

Switch#debug pim sp packets recv

Switch#show debugging pim sparse-mode

PIM-SM debugging status:

PIM packet receive debugging is on

Switch#

18.4.8 debug pim sparse-mode state

命令

debug pim spare-mode state

no debug pim sparse-mode state

模式

特权模式。

参数

无。

描述

debug pim sparse-mode state 命令用来打开组播路由状态调试开关。

no debug pim sparse-mode state 来关闭组播路由状态调试开关。

举例

#打开 pim-sm 路由状态调试开关，查看成员离开时组播路由的状态变化

Switch#debug pim sparse-mode state

Switch#log dis

Switch#

2006/10/26 17:01:16 Informational: PIM-SM: US (*, 233.1.1.1): JOINED to NOT JOINED, JoinDesired => FALSE

2006/10/26 17:01:16 Informational: PIM-SM: US (192.168.8.2, 233.1.1.1, rpt): NOT PRUNED to RPT NOT JOINED, RPTJoinDesired(G)=>FALSE

Switch#

18.4.9 debug pim sparse-mode timer

命令

debug pim spare-mode timer [assert [at] | bsr [bst | crp] | hello [ht | nlt | tht] | joinprune [et | jt | kat | ot | ppt] | register [rst]]

no debug pim sparse-mode timer [assert [at] | bsr [bst | crp] | hello [ht | nlt | tht] | joinprune [et | jt | kat | ot | ppt] | register [rst]]

模式

特权模式。

参数

assert [at]：断言定时器。

bsr [bst | crp]：自举路由器的自举定时器和候选 rp 定时器。

hello [ht | nlt | tht]：hello 定时器，包含 hello 定时器，邻居失效定时器和 hello 触发定时器。

joinprune [et | jt | kat | ot | ppt]：加入剪枝定时器，包括超时定时器，加入加入剪枝定时器，保活定时器，否决定时器和剪枝抑制定时器。

register [rst]：注册定时器。

描述

debug pim spare-mode timer 命令用来打开指定定时器的调试开关。

no debug pim sparse-mode timer 命令用来关闭指定定时器的调试开关。

举例

#打开 pim-sm hello 报文定时器的调试开关

Switch#debug pim sparse-mode timer hello

Switch#show debugging pim sparse-mode

PIM-SM debugging status:

PIM Hello HT timer debugging is on

PIM Hello NLT timer debugging is on

PIM Hello THT timer debugging is on

Switch#

第 19 章 SNMP 命令

19.1 SNMP 配置命令

19.1.1 snmp community

命令

snmp community <community-name> {ro | rw}

no snmp community <community-name>

模式

全局配置模式

参数

Community-name：SNMP 共用体名。字符长度：1~20。

ro：只读属性。

rw：读写属性。

描述

snmp community 命令是配置 SNMP 共用体名及该共用体的相关属性。

no snmp community 命令是删除指定的 SNMP 共用体名。

举例

#配置一个名为 private 的共用体且属性为读写属性：

Switch(config)#snmp community private rw

#删除一个名为 private 的共用体

Switch(config)#no snmp community private

19.1.2 snmp trap

命令

snmp trap <notify-name> host <ipaddress> version {1 | 2c | 3}

no snmp trap <notify-name>

模式

全局配置模式

参数

notify-name：SNMP trap 命名。字符长度：1~32。

Ipaddress：发送 trap 的目的 IP 地址。

1：SNMP 版本 1。

2：SNMP 版本 2。

3：SNMP 版本 3。

描述

snmp trap 命令是配置 SNMP trap 及该 trap 的相关属性。

no snmp trap 命令是删除指定的 SNMP trap。

举例

#配置一个名为 test 的 SNMP trap 且发送的目的 IP 为 192.168.0.10；使用的 SNMP 版本为 1。

Switch(config)#snmp trap test host 192.168.0.10 version 1

#删除一个名为 test 的 SNMP trap

Switch(config)#no snmp trap test

19.1.3 snmp system information contact

命令

snmp system information <contact | location | name > < information string >

no snmp system information <contact | location | name >

模式

全局配置模式

参数

information string：指定的内容。字符长度：1~255。

描述

snmp system information 命令是配置系统信息。

no snmp system information 命令是删除系统信息。

举例

#配置系统的 contact 的具体内容为：E-mail:networks@lenovo.com

Switch(config)#snmp system information contact E-mail:networks@lenovo.com

#配置系统的 location 具体内容为：ShennanRoad,Shenzhen,China

Switch(config)#snmp system information location ShennanRoad,Shenzhen,China

#配置系统的 name 具体内容为：iSpirit8812E

Switch(config)#snmp system information name iSpirit8812E

#删除系统的 name

Switch(config)#no snmp system information name

19.1.4 snmp engine-id local

命令

snmp engine-id local < engine-id>

模式

全局配置模式

参数

engine-id：SNMP 版本 3 所使用的 engine id。

描述

snmp engine-id local 命令是配置 SNMP 版本 3 所使用的 engine id。该 ID 为一个 24 位的十六进制数；且输入不足 24 位时，自动用 0 补齐。

举例

#配置 SNMP engineID 为：00002ffc0000226c7f000022

Switch(config)#snmp engine-id local 00002ffc0000226c7f000022

19.1.5 snmp user

命令

snmp user <user-name> <group-name> v3 [auth {md5 | sha} <auth-key>]

no snmp user <user-name> <group-name> v3

模式

全局配置模式

参数

user-name：设置 snmpv3 engine ID 所对应的某个用户名。字符长度：1~32。

group-name：设置该用户名所对应的组名。字符长度：1~32。

auth：使用该用户名的安全级别是可鉴别的。

md5：使用鉴别 hmac md5 鉴别协议

sha：使用鉴别 hmac sha 鉴别协议

auth-key：输入鉴别密码，md5 的为 16 字节长的 16 进制的数字字符串，sha

的为 20 字节长的 16 进制的数字字符串。

描述

snmp user命令是设置snmpv3本地的engine ID所对应的某个用户名。及该用户名对应的组名，如果该用户名支持鉴别，则需设置鉴别协议（md5或sha）及相应的鉴别密码。

no snmp user命令是删除snmpv3本地的engine ID所对应的某个用户名。

举例

#设置某支持 md5 鉴别的用户名 initialmd5，组名为 initia，鉴别密码为 047b473f93211a17813ce5fff290066b:

Switch(config)# snmp user initialmd5 initial v3 auth md5 047b473f93211a17813ce5fff290066b

#设置无需鉴别的用户名 initialnone，组名为 initial:

Switch(config)# snmp user initialnone initial v3

#删除用户名 initialmd5，组名为 initial 的用户。

Switch(config)# no snmp user initialmd5 initial v3

19.1.6 snmp group

命令

snmp group <group-name> v3 {auth | noauth} [notify <notify-view-name> | write <write-view-name> | read <read-view-name>]

no snmp group <group-name> v3 {auth | noauth}

模式

全局配置模式

参数

group-name：进行配置组名。字符长度：1~32。

auth：该访问控制是需要鉴别的。

noauth：该访问控制是不需要鉴别的。

notify：指定可产生通知的 mib 视图。

notify-view：指定可产生通知的 mib 视图的视图名。

write：指定可写的 mib 视图。

write-view：指定可写的 mib 视图的视图名。

read：指定可读的 mib 视图。

read-view：指定可读的 mib 视图的视图名。

描述

snmp group命令是设置snmp group命名及信息。

no snmp group命令是删除snmp group命名及信息。

举例

#设置组名为 initial，安全级别是（auth），安全模型（v3）所指定的通知，可写或可读的视图名分别为 internet，internet，internet:

Switch(config)# snmp group initial v3 auth read internet write internet notify internet

#删除组名为 initial 的组。

Switch(config)# no snmp group initial v3 auth

Switch(config)#

19.2 SNMP 查看命令

19.2.1 show snmp community

命令

show snmp community

模式

普通模式/特权模式

参数

无

描述

show snmp community命令是显示目前所有的公用体名。

举例

#显示所有的公用体名:

Switch# show snmp community

19.2.2 show snmp trap

命令

show snmp trap

模式

普通模式/特权模式

参数

无

描述

show snmp trap命令是用来显示目前所有的trap名。

举例

#显示所有的 trap 名:

Switch#show snmp trap

19.2.3 show snmp system information

命令

show snmp system information

模式

普通模式/特权模式

参数

无

描述

show snmp system information命令是显示SNMP设置的系统信息。

举例

#显示目前的系统信息:

Switch#show snmp system information

19.2.4 show snmp engine-id

命令

show snmp engine-id

模式

普通模式/特权模式

参数

无

描述

show snmp engine-id命令是显示SNMP所使用的engine-id。

举例

#显示 SNMP 使用的 engine-id：

Switch#show snmp engine-id

19.2.5 show snmp user

命令

show snmp user [specify-name-of-user]

模式

普通模式/特权模式

参数

无

描述

show snmp user命令是显示SNMP所使用的user及其属性。

举例

#显示 SNMP 使用的用户 initialnone 及其属性.:

Switch#show snmp user initialnone

19.2.6 show snmp group

命令

show snmp group

模式

普通模式/特权模式

参数

无

描述

show snmp group 命令是显示 SNMP 使用的所有的 group 信息

举例

#显示 SNMP 使用的所有的 group 信息

Switch#show snmp group

Switch#

第 20 章 系统日志命令

20.1 通用日志命令

20.1.1 debug ip

命令

debug ip [all | arp | icmp | tcp | udp]
no debug ip [all | arp | icmp | tcp | udp]

模式

特权模式。

参数

all：调试所有 ip、arp、icmp、udp、tcp 等协议包。解析 IP 包头的重要字段，包括协议类型、数据包长度和四层消息，如端口号等。

arp：调试 arp 协议包，可以解析是 ARP 请求还是响应，可以解析 ARP 内容，发送端 IP 和接收端 MAC 地址信息等等。

icmp：调试 icmp 协议数据报文的收发情况。该命令主要是通过解析包头的源和目的地址。

tcp：调试运输层协议TCP的收发包情况，可以看到收发包窗口大小，应用层端口和报文大小以及源和目的地址。

udp：调试运输层协议 udp 的收发包情况，可以看到应用层端口和报文大小以及收发包的源和目的地址。

描述

debug ip 命令用来打开以 ip 头封装的报文的相关调试开关，使用户能够看到指定类型的 ip 报文的报文收发情况。

no debug ip 命令关闭对应的 ip 报文调试开关。

举例

#打开 icmp 报文的调试开关：
Switch#debug ip icmp
Switch#

20.1.2 log display

命令

log display [critical | debugging | informational | warning]

no log display [critical | debugging | informational | warning]

模式

特权模式。

参数

critical：输出 critical 级的信息。

debugging：输出 debugging 级的调试信息。

informational：输出法 information 级的调试信息。

warning：输出 warning 级的调试信息。

举例

#输出所有打开调试开关调试信息：

Switch#log display

Switch#

20.1.3 no debug all

命令

no debug all

模式

特权模式。

参数

无。

描述

no debug all 命令用来关闭所有打开的调试开关。

举例

#关闭所有打开的调试开关：

Switch#no debug all

Switch#

20.1.4 show debugging

命令

show debugging [dhcp-relay | igmp | ip | mstp | ospf | pim | rip | vrrp]

模式

特权模式/普通模式。

参数

dhcp-relay：dhcp-relay 的相关调试开关。

igmp：igmp 的相关调试开关。

ip：ip 的相关调试开关。

mstp：mstp 的相关调试开关。

ospf：ospf 的相关调试开关。

pim：组播 pim 的相关调试开关。

rip：rip 的相关调试开关。

vrrp：vrrp 的相关调试开关。

描述

show debug 命令用来查看当前打开了那些调试开关。

举例

#查看调试开关信息：

```
Switch#show debug
IP debugging status:
  ICMP receive packets debugging is on.
  ICMP send packets debugging is on.

RIP debugging status:

OSPF debugging status:

VRRP debugging status:

DHCP-relay debugging status:

PIM-SM debugging status:

IGMP debugging status:

MSTP debugging status:

IGMP SNOOPING debugging status:

Switch#
```

20.1.5 show log

命令

show log [critical | debugging | informational | warning]

模式

特权模式/普通模式。

参数

critical：输出 critical 级的日志信息。

debugging：输出 debugging 级的日志信息。

informational：输出 information 级的日志信息。

warning：输出 warning 级的日志信息。

描述

show log 命令用来显示日志表中的日志信息。

举例

#显示 information 级的日志信息：

Switch#show log informational

2089/08/10 11:01:24 Informational: ICMP: SEND: Destination IP: 172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0

2089/08/10 11:01:21 Informational: ICMP: SEND: Destination IP: 172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0

2089/08/10 11:01:18 Informational: ICMP: SEND: Destination IP: 172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0

2089/08/10 11:00:13 Informational: ICMP: SEND: Destination IP: 172.20.3.3 Source IP: 172.20.14.2 ICMP Type: 3 ICMP Code: 3

2089/08/10 11:00:13 Informational: ICMP: SEND: Destination IP: 172.20.3.3 Source IP: 172.20.14.2 ICMP Type: 3 ICMP Code: 3

2089/08/10 10:59:38 Informational: ICMP: SEND: Destination IP: 172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0

2089/08/10 10:53:21 Informational: ICMP: SEND: Destination IP:

172.20.3.3 Source IP: 172.20.10.2 ICMP Type: 3 ICMP Code: 3

Switch#

20.1.6 show log display

命令

show log display [critical | debugging | informational | warning]

模式

特权模式/普通模式。

参数

critical：输出严重级的日志信息。

debugging：输出调试信息。

informational：输出一般性提示级的日志信息。

warning：输出一般警告级的日志信息。

描述

show log display 命令用来显示四个优先级的终端实时监测开关的配置（打开还是关闭）。

举例

#显示监控配置信息：

Switch#show log display

Log display configuration:

Critical log: OFF

Warning log: OFF

Informational log: OFF

Debugging log: OFF

Switch#