Mellanox MLNX-OS® User Manual for IBM 90Y3474

Rev 3.20

Software Version 3.4.0000

www.mellanox.com

NOTE:
THIS HARDWARE, SOFTWARE OR TEST SUITE PRODUCT (“PRODUCT(S)”) AND ITS RELATED DOCUMENTATION ARE PROVIDED BY MELLANOX TECHNOLOGIES “AS-IS” WITH ALL FAULTS OF ANY KIND AND SOLELY FOR THE PURPOSE OF AIDING THE CUSTOMER IN TESTING APPLICATIONS THAT USE THE PRODUCTS IN DESIGNATED SOLUTIONS. THE CUSTOMER'S MANUFACTURING TEST ENVIRONMENT HAS NOT MET THE STANDARDS SET BY MELLANOX TECHNOLOGIES TO FULLY QUALIFY THE PRODUCTO(S) AND/OR THE SYSTEM USING IT. THEREFORE, MELLANOX TECHNOLOGIES CANNOT AND DOES NOT GUARANTEE OR WARRANT THAT THE PRODUCTS WILL OPERATE WITH THE HIGHEST QUALITY. ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL MELLANOX BE LIABLE TO CUSTOMER OR ANY THIRD PARTIES FOR ANY DIRECT, INDIRECT, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING, BUT NOT LIMITED TO, PAYMENT FOR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY FROM THE USE OF THE PRODUCT(S) AND RELATED DOCUMENTATION EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Mellanox Technologies
350 Oakmead Parkway Suite 100
Sunnyvale, CA 94085
U.S.A.
www.mellanox.com
Tel: (408) 970-3400
Fax: (408) 970-3403

Mellanox Technologies, Ltd.
Beit Mellanox
PO Box 586 Yokneam 20692
Israel
www.mellanox.com
Tel: +972 (0)74 723 7200
Fax: +972 (0)4 959 3245

Table of Contents

Document Revision History

Table 1 - Document Revision History

Document Revision	Date	Description
Rev 3.20	12 October, 2014	• Added: • Section 5.5.2, “MAC Learning Considerations,” on page 421 • the command “mac-learning disable” on page 424 Updated: • Section 1.2, “Ethernet Features,” on page 15 • Section 3.2, “Web Interface Overview,” on page 32 • the command “interface port-channel” on page 376 • the command “show lacp interfaces neighbor” on page 384 Replaced: • the command “show lacp interfaces port-channel” with the command “show lacp” on page 386 • the command “show lacp system-identifier” with the command “show lacp interfaces system-identifier” on page 387
Rev 3.10	20 July, 2014	Added: • Section 5.14, “Transport Applications,” on page 554 • Updated: • Section 4.13.1, “XML API,” on page 340 • MAC addresses note in Section 5.3, “MLAG,” on page 389
Rev 3.00	05 June, 2014	• N/A
Rev 2.90	19 May, 2014	• Updated: • the command “show configuration” on page 174 • the command “show uboot” on page 323 • the command “show voltage” on page 332
Rev 2.80	08 May, 2014	Added: • supported versions note in Section 5.8, “IGMP Snooping,” on page 461
Rev 2.60	10 April, 2014	N/A •
Rev 2.50	April 2014	Updated: • Section 3.1.7, “Command Output Filtering,” on page 31 • the command “show protocols” on page 338 • Section 5.1.1, “Break-Out Cables,” on page 356 • the command “show mac-address-table” on page 426 • the command “deny/permit (MAC ACL rule)” on page 516 • the command “show mac/ipv4 access-lists” on page 522

Table 1 - Document Revision History

Document Revision	Date	Description
Rev 2.40	February, 2014	Updated: • Section 4.3.5.2, "Importing Firmware and Changing the Default Firmware," on page 138 – updated Step 1 • Command "show running-config" on page 175 • Command "show log" on page 194 • Section 4.10, "Cryptographic (X.509, IPSec)," on page 274 • Section 5.2.1, "Configuring Static Link Aggregation Group (LAG)," on page 374 – removed unnecessary step • Command "lldp tlv-select" on page 488 • Command "show lldp interface" on page 491 Added: • Section 3.1.7, "Command Output Filtering," on page 31
Rev 2.30	January, 2014	• Updated: • command "crypto certificate generation" on page 279 • command "crypto certificate name" on page 280
Rev 2.20	January, 2014	• N/A
Rev 2.10	January, 2014	Added: • Section 4.12.2.1, "Width Reduction Power Saving," on page 313 Updated: • Section 2.2, "Starting the Command Line (CLI)," on page 17 • Section 2.3, "Starting the Web User Interface," on page 18 • Section 4.3.2, "Upgrading MLNX-OS Software," on page 130 with EULA note • Section 5.7, "OpenFlow," on page 452 • command "openflow description" on page 455 • command "show openflow" on page 460 • command "deny/permit (IPv4 ACL rule)" on page 517 • command "load-interval" on page 366 with Config Interface Port Channel • command "switchport {hybrid, trunk} allowed-vlan" on page 419 with Config Interface Port Channel • command "spanning-tree port-priority" on page 435 with Config Interface Port Channel • command "spanning-tree cost" on page 436 with Config Interface Port Channel • command "spanning-tree port type" on page 437 with Config Interface Port Channel • command "spanning-tree guard" on page 438 with Config Interface Port Channel • the command "spanning-tree bpdufilter" on page 439 with Config Interface Port Channel • command "sflow enable (interface)" on page 552 with Config Interface Port Channel • Section 6.2, "OSPF," on page 592 • command "router-id" on page 599

Table 1 - Document Revision History

Document Revision	Date	Description
Rev 2.00	December 2013	Added Section 5.1.2, “Transceiver Information,” on page 359 Updated Section 4.3.2, “Upgrading MLNX-OS Software,” on page 130 Updated Section 4.3.3, “Deleting Unused Images,” on page 133 Updated Section 4.6, “Debugging,” on page 195 Updated the example of the command “show cpld” on page 324 Updated “Notification Indicator” column in Section 8.4.2, “Standalone Proxy-ARP Configuration,” on page 1111 Updated the command “lldp tlv-select” on page 488 Moved Section 4.5.3, “Switch Power-On Self-Test,” on page 176 from 4.11.1 Moved Section 3.3, “Secure Shell (SSH),” on page 37 from 4.13.2 Removed mention of the MLNX-OS Command Reference Guide Removed the command “lldp tlv-select dcbx”
Rev 1.90	November 2013	Added Appendix A,“MEX6200 System,” on page 1162
Rev 1.80	October 2013	• Added: • Section 5.6.6, “MSTP,” on page 430 • Section 5.7, “OpenFlow,” on page 452 • Section 5.8.3, “IGMP Snooping Querier,” on page 463 • the command “ip igmp snooping querier” • the command “igmp snooping querier query-interval” • the command “show ip igmp snooping querier” • Section 5.9.2, “DCBX,” on page 480 • the command “lldp tlv-select dcbx” • the command “dcb application-priority” • the command “show dcb application-priority” • Updated • the command “show lldp interface” • the command “show lldp interfaces ethernet <inf> remote”
Rev 1.7.0	October 2013	Merged “MLNX-OS Command Reference Guide” Rev. 1.6.9 and “MLNX-OS User Manual” Rev. 1.6.9.

About this Manual

This manual provides general information concerning the scope and organization of this User's Manual.

Intended Audience

This manual is intended for network administrators who are responsible for configuring and managing Mellanox Technologies' SwitchX based Switch Platforms.

Related Documentation

The following table lists the documents referenced in this *User's Manual.*

Table 2 - Reference Documents

Document Name	Description
InfiniBand Architecture Specification, Vol. 1, Release 1.2.1	The InfiniBand Architecture Specification that is provided by IBTA.
Director switch Installation Guide	Each Mellanox Technologies' switch platform is shipped with an Installation Guide document to bring-up and initialize the switch platform.
System Hardware User Manual	This document contains hardware descriptions, LED assignments and hardware specifications among other things.
Switch Product Release Notes	Please look up the relevant SwitchX®-based switch system/series release note file
Mellanox Virtual Modular Switch Reference Guide	This reference architecture provides general information concerning Mellanox L2 and L3 Virtual Modular Switch (VMS) configuration and design.
Configuring Mellanox Hardware for VPI Operation Application Note	This manual provides information on basic configuration of the converged VPI networks.

All of these documents can be found on the Mellanox website. They are available either through the product pages or through the support page with a login and password.

Glossary

Table 3 - Glossary

AAA	Authentication, Authorization, and Accounting. Authentication - verifies user credentials (username and password). Authorization - grants or refuses privileges to a user/client for accessing specific services. Accounting - tracks network resources consumption by users.
ARP	Address Resolution Protocol. A protocol that translates IP addresses into MAC addresses for communication over a local area network (LAN).
CLI	Command Line Interface. A user interface in which you type commands at the prompt
DCB	Data Center Bridging
DCBX	DCBX protocol is an extension of the Link Layer Discovery Protocol (LLDP). DCBX end points exchange request and acknowledgment messages. For flexibility, parameters are coded in a type-length-value (TLV) format.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks.
DNS	Domain Name System. A hierarchical naming system for devices in a computer network
ETS	ETS provides a common management framework for assignment of bandwidth to traffic classes.
FTP/TFTP/sFTP	File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another over a TCP-based network, such as the Internet.
Gateway	A network node that interfaces with another network using a different network protocol
HA (High Availability)	A system design protocol that provides redundancy of system components, thus enables overcoming single or multiple failures in minimal downtime
Host	A computer platform executing an Operating System which may control one or more network adapters
LACP	Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).
LDAP	The Lightweight Directory Access Protocol is an application protocol for reading and editing directories over an IP network.
MAC	A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies including Ethernet.

Table 3 - Glossary

MTU (Maximum Transfer Unit)	The maximum size of a packet payload (not including headers) that can be sent /received from a port
Network Adapter	A hardware device that allows for communication between computers in a network
PFC/FC	Priority Based Flow Control applies pause functionality to traffic classes OR classes of service on the Ethernet link.
RADIUS	Remote Authentication Dial In User Service. A networking protocol that enables AAA centralized management for computers to connect and use a network service.
RDMA (Remote Direct Memory Access)	Accessing memory in a remote side without involvement of the remote CPU
RSTP	Rapid Spanning Tree Protocol. A spanning-tree protocol used to prevent loops in bridge configurations. RSTP is not aware of VLANs and blocks ports at the physical level.
SA (Subnet Administrator)	The interface for querying and manipulating subnet management data
SCP	Secure Copy or SCP is a means of securely transferring computer files between a local and a remote host or between two remote hosts. It is based on the Secure Shell (SSH) protocol.
SNMP	Simple Network Management Protocol. A network protocol for the management of a network and the monitoring of network devices and their functions
NTP	Network Time Protocol. A protocol for synchronizing computer clocks in a network
SSH	Secure Shell. A protocol (program) for securely logging in to and running programs on remote machines across a network. The program authenticates access to the remote machine and encrypts the transferred information through the connection.
syslog	A standard for forwarding log messages in an IP network
TACACS+	Terminal Access Controller Access-Control System Plus. A networking protocol that enables access to a network of devices via one or more centralized servers. TACACS+ provides separate AAA services.
XML Gateway	Extensible Markup Language Gateway. Provides an XML request-response protocol for setting and retrieving HW management information.

1 Introduction

Mellanox® Operating System (MLNX-OS®) enables the management and configuration of Mellanox Technologies' SwitchX® silicon based switch platforms. MLNX-OS supports the Virtual Protocol Interconnect (VPI) technology which enables it to be used for both Ethernet and InfiniBand technology providing the user with greater flexibility.

MLNX-OS provides a full suite of management options, including support for Mellanox's Unified Fabric Manager® (UFM), SNMP V1,2,3, and web user interface (WebUI). In addition, it incorporates a familiar industry-standard CLI, which enables administrators to easily configure and manage the system.

1.1 System Features

Table 4 - General System Features

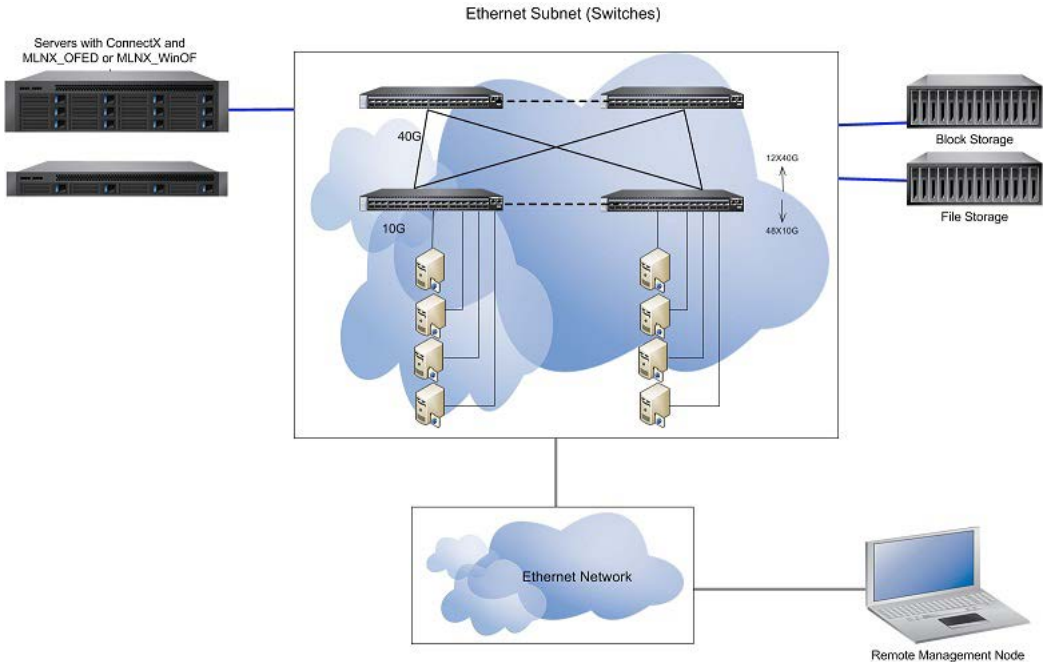
Feature	Description
Software Management	• Dual software image • Software and firmware updates
File management	• FTP • TFTP • SCP
Logging	• Event history log • SysLog support
Management Interface	• DHCP/Zeroconf • IPv6
Chassis Management	• Monitoring environmental controls
Network Management Interfaces	• SNMP v1,v2c,v3 • REST interfaces (XML Gateway) • Puppet Agent
Security	• SSH • Telnet • RADIUS • TACACS+
Date and Time	• NTP
Cables & Transceivers	• Transceiver info

1.2 Ethernet Features

Table 5 - Ethernet Features

Feature	Description
General	• ACL – 24K rules (permit/deny) • Breakout cables • Jumbo Frames (9K)
Ethernet support	• 48K Unicast MAC addresses • DCBX • DHCP Relay • ETS (802.1Qaz) • Flow control (802.3x) • IGMP snooping v1,2 • LAG/LACP (802.3ad), 16 links per LAG (64 LAGs) • LLDP • MLAG • MSTP • OpenFlow • PFC (802.1Qbb) • Rapid Spanning Tree (802.1w) • sFlow • VLAN (802.1Q) - 4K
IP routing	• BGP • DHCP Relay • ECMP • IGMP • OSPF • PIM • VLAN interface • VRRP

Figure 1: Managing an Ethernet Fabric Using MLNX-OS



2 Getting Started

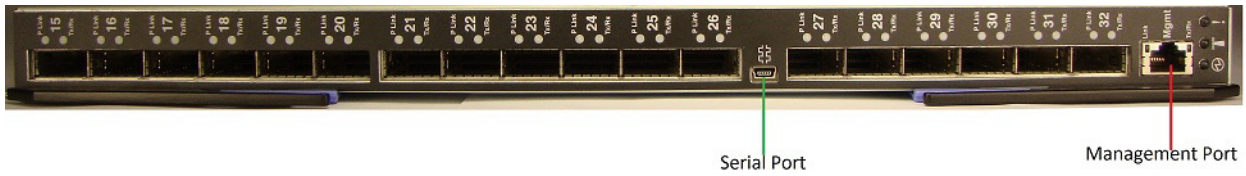
The procedures described in this chapter assume that you have already installed and powered on your switch according to the instructions in the *Hardware Installation Guide*, which was shipped with the product.

2.1 Configuring the Switch for the First Time

➢ ***To configure the switch:***

Step 1. Connect the host PC to the console (mini USB) port of the switch system using the supplied cable.

Figure 2: IBM System Console Ports



No remote IP connection is available at this stage via the external management port. The internal management port can be accessed currently by the chassis management.

Step 2. Configure a serial terminal with the settings described below.

Table 6 - Serial Terminal Program Configuration for PPC Based Systems

Parameter	Setting
Baud Rate	9600
Data bits	8
Stop bits	1
Parity	None
Flow Control	None

Step 3. Login as *admin* and use *admin* as password.

2.2 Starting the Command Line (CLI)

Step 1. Set up an Ethernet connection between the switch and a local network machine using a standard RJ-45 connector.

Step 2. Start a remote secured shell (SSH) to the switch using the command “ssh -l <username> <switch ip address>.”

```
rem_mach1 >  ssh -l <username> <ip address>
```

Step 3. Login to the switch (default username is *admin*, password *admin*)

Step 4. Read and accept the EULA when prompted.

Step 5. Once you get the prompt, you are ready to use the system.

```
Mellanox MLNX-OS Switch Management

Password:
Last login: <time> from <ip-address>

Mellanox Switch
Please read and accept the Mellanox End User License Agreement located at:
http://www.mellanox.com/related-docs/prod_management_software/MLNX-OS_EULA.pdf

switch >
```

2.3 Starting the Web User Interface

➢ ***To start a WebUI connection to the switch platform:***

Step 1. Set up an Ethernet connection between the switch and a local network machine using a standard RJ-45 connector.

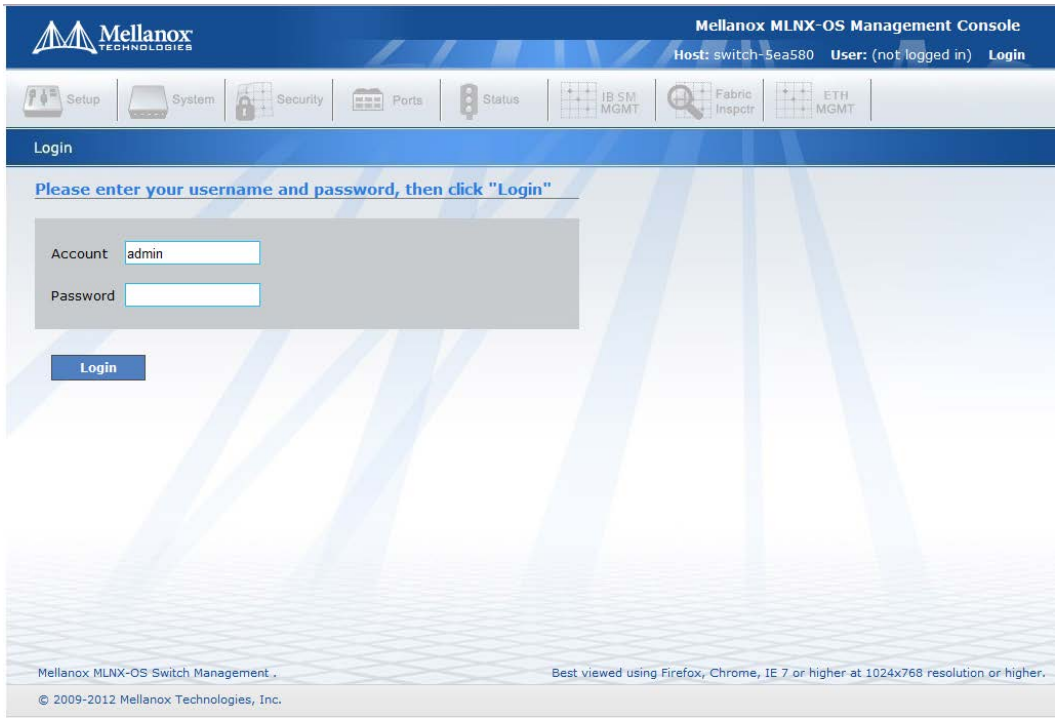
Step 2. Open a web browser – Firefox 12, Chrome 18, IE 8, Safari 5 or higher.

Note: Make sure the screen resolution is set to 1024*768 or higher.

Step 3. Type in the IP address of the switch or its DNS name in the format: https://<switch_IP_address>.

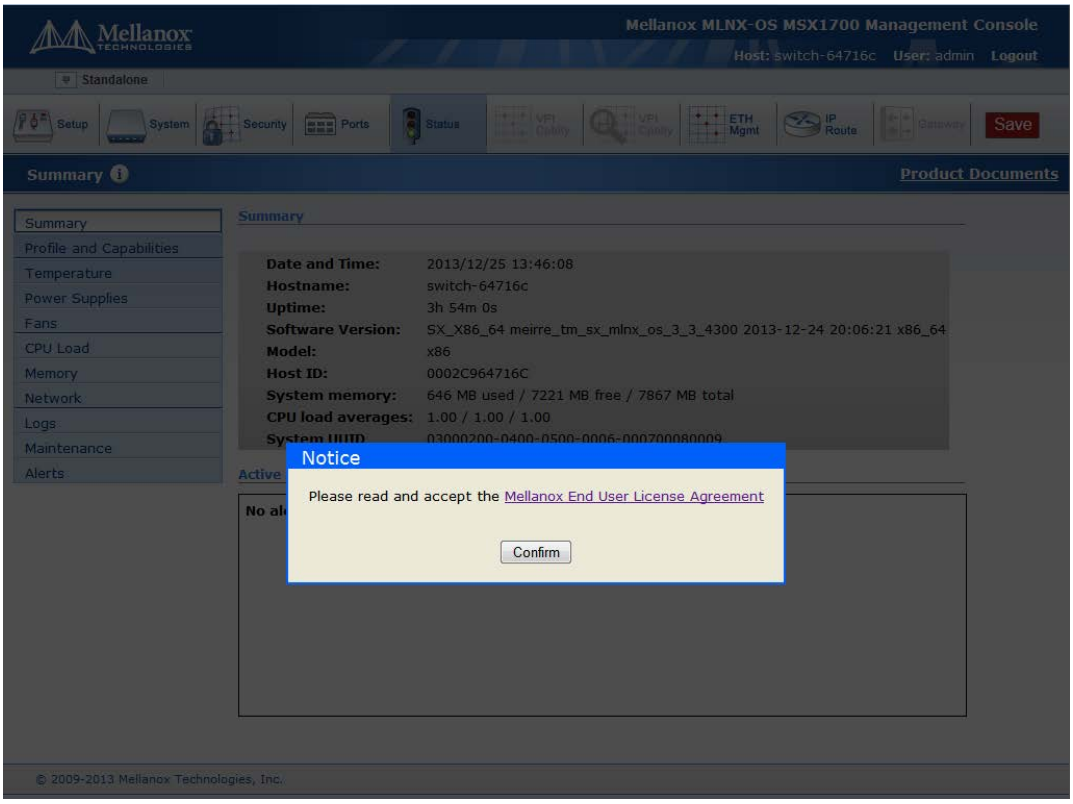
Step 4. Login to the switch (default user name is *admin*, password *admin*).

Figure 3: MLNX-OS Login Window



Step 5. Read and accept the EULA if prompted.
You are only prompted if you have not accessed the switch via CLI before.

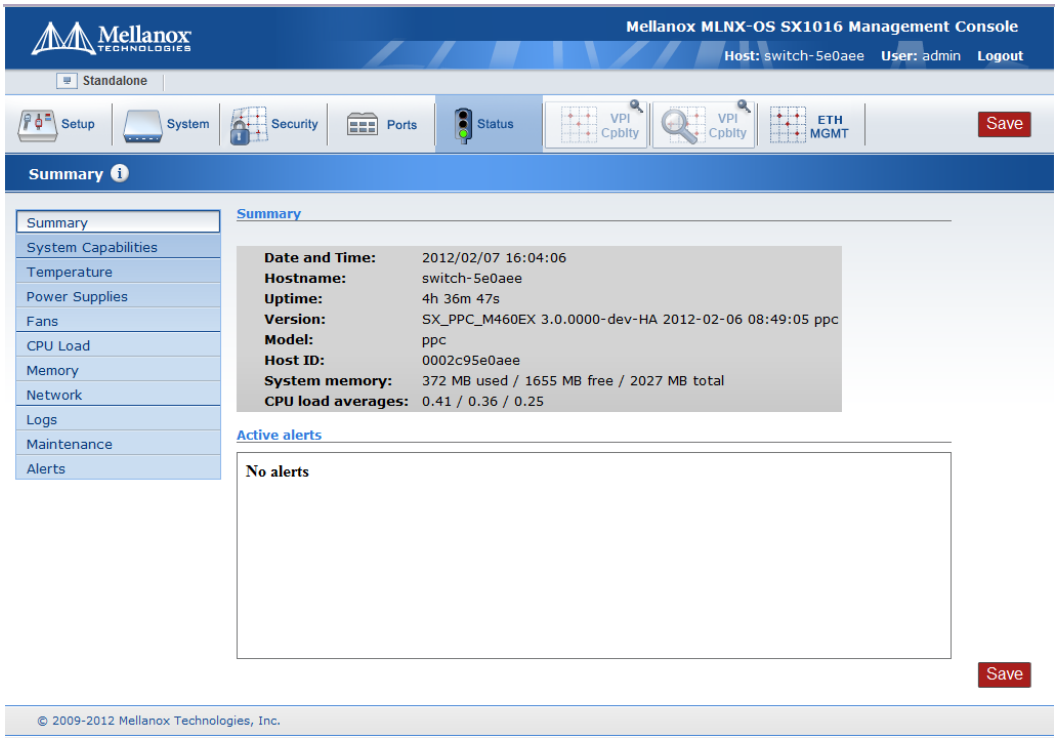
Figure 4: EULA Prompt



The following figure shows an example of the login window for remote management of the switch.

After you log in to MLNX-OS, a (default) status summary window is displayed as shown in Figure 5.

Figure 5: Display After Login



2.4 Licenses

MLNX-OS software package can be extended with premium features. Installing a license allows you to access the specified premium features.

This section is relevant only to switch systems with an internal management capability.

The following licenses are offered with MLNX-OS software:

2.4.1 Installing MLNX-OS® License (CLI)

➢ ***To install an MLNX-OS license via CLI:***

Step 1. Login as *admin* and change to *Config* mode.

```
switch > enable
switch # config terminal
```

Step 2. Install the license using the key. Run:

```
switch (config) # license install <license key>
```

Step 3. Display the installed license(s) using the following command.

```
switch (config) # show licenses
License 1: <license key>
Feature: EFM_SX
Valid: yes
Active: yes
switch (config) #
```

Make sure that the “Valid” and “Active” fields both indicate “yes”.

Step 4. Save the configuration to complete the license installation. Run:

```
switch (config) # configuration write
```

If you do not save the installation session, you will lose the license at the next system start up.

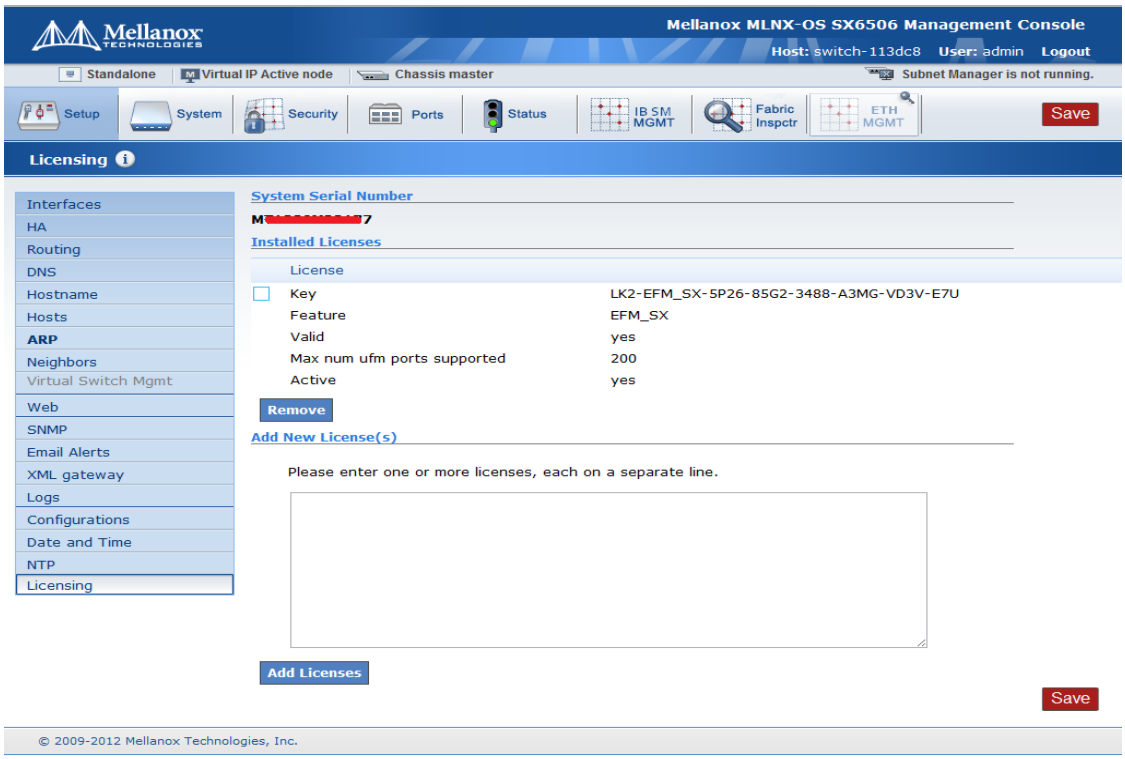
2.4.2 Installing MLNX-OS License (Web)

➢ ***To install an MLNX-OS license via CLI:***

Step 1. Log in as *admin*.

Step 2. Click the **Setup** tab and then **Licensing** in the left side navigation pane.

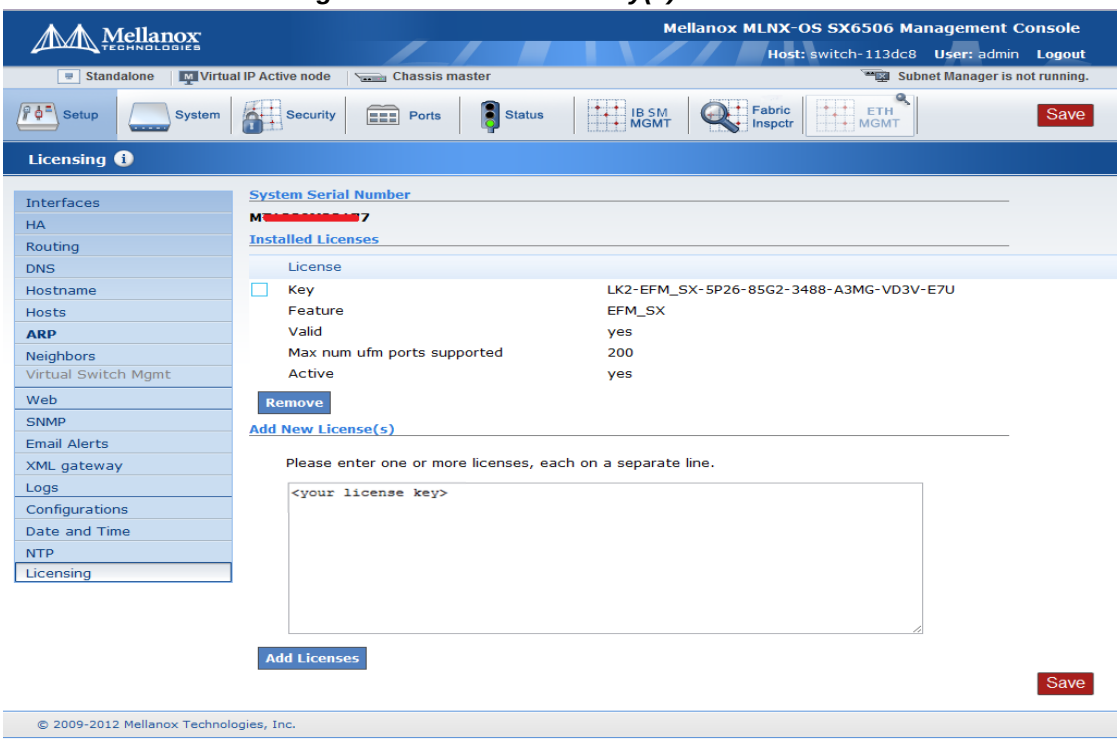
Figure 6: No Licenses Installed



Step 3. Enter your license key(s) in the text box. If you have more than one license, please enter each license in a separate line. Click “Add Licenses” after entering the last license key to install them.

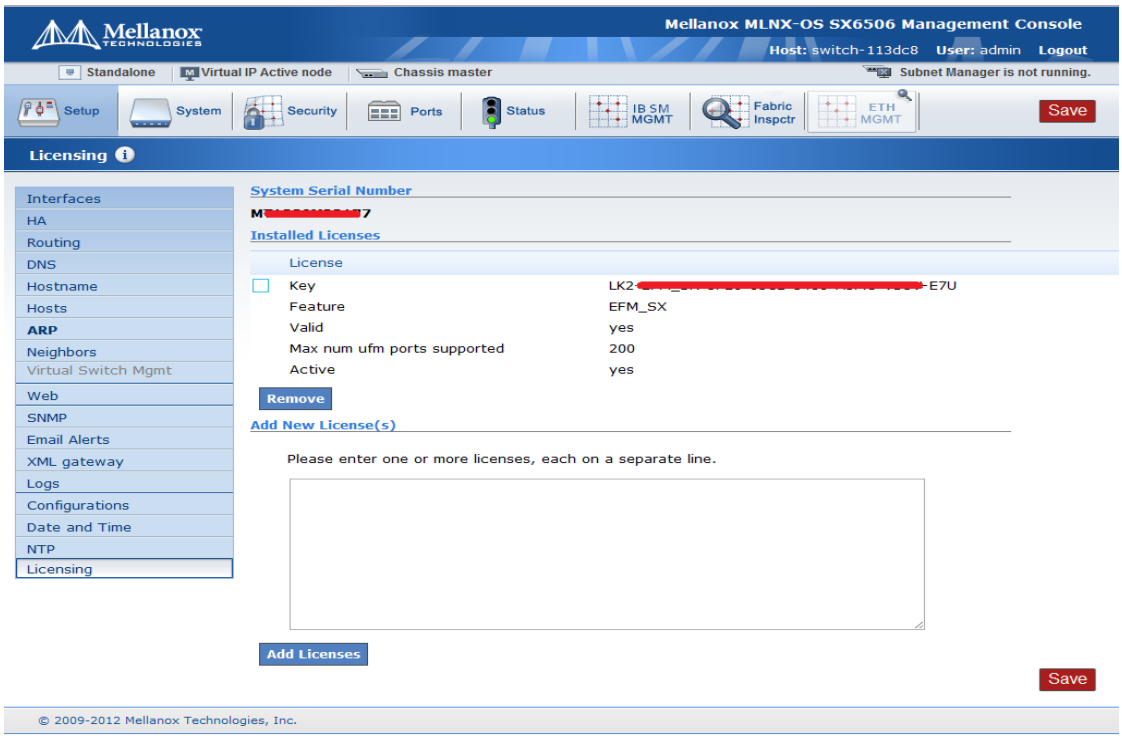
If you wish to add another license key in the future, you can simply enter it in the text box and click “Add Licenses” to install it.

Figure 7: Enter Licence Key(s) in Text Box



All installed licenses should now be displayed.

Figure 8: Installed License



Step 4. Save the configuration to complete the license installation.

If you do not save the installation session, you will lose the installed licenses at the next system boot.

2.4.3 Retrieving a Lost License Key

In case of a lost MLNX-OS® license key, contact your authorized Mellanox reseller and provide the switch's *chassis serial number.*

➢ ***To obtain the switch's chassis serial number:***

Step 1. Login to the switch.

Step 2. Retrieve the switch's *chassis serial number* using the command "show inventory".

```
switch (config) # show inventory
================================================================================
Module               Type                Part number          Serial Number

================================================================================
CHASSIS              SX1035              MSX6036F-1BFR        MT1121X02692
MGMT                 SX1035              MSX6036F-1BFR        MT1121X02692
FAN                  SXX0XX_FAN          MSX60-FF             MT1121X02722
PS1                  SXX0XX_PS           N/A                  N/A
CPU                  CPU                 SA000103             MT1120X01027
switch (config) #
```

Step 3. Send your Mellanox reseller the following information to obtain the license key:

- The chassis serial number
- The type of license you need to retrieve. Refer to “Licenses” on page 20.

Step 4. Once you receive the license key, you can install the license as described in the sections above.

2.4.4 Commands

show licenses

show licenses

Displays a list of all installed licenses. For each license, the following is displayed:
- a unique ID which is a small integer
- the text of the license key as it was added
- whether or not it is valid and active
- which feature(s) it is activating
- a list of all licensable features specifying whether or not it is currently activated by a license

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	monitor/admin

Example	`switch (config) # show licenses`
	`License 1: <license key>`
	`Feature: SX_CONFIG`
	`Valid: yes`
	`Active: yes`
	`switch (config) #`

Related Commands	license
Note	

3 User Interfaces

3.1 Command Line Interface (CLI) Overview

MLNX-OS® is equipped with an industry-standard CLI. The CLI is accessed through SSH or Telnet sessions, or directly via the console port on the front panel (if it exists).

3.1.1 CLI Modes

The CLI can be in one of following modes, and each mode makes available a certain group (or level) of commands for execution. The different CLI configuration modes are:

Table 7 - CLI Modes and Config Context

Mode/Context	Description
Standard	When the CLI is launched, it begins in Standard mode. This is the most restrictive mode and only has commands to query a restricted set of state information. Users cannot take any actions that directly affect the system, nor can they change any configuration.
Enable	The `enable` command moves the user to Enable mode. This mode offers commands to view all state information and take actions like rebooting the system, but it does not allow any configurations to be changed. Its commands are a superset of those in Standard mode.
Config	The `configure terminal` command moves the user from Enable mode to Config mode. Config mode is allowed only for user accounts in the “admin” role (or capabilities). This mode has a full unrestricted set of commands to view anything, take any action, and change any configuration. Its commands are a superset of those in Enable mode. To return to Enable mode, enter `exit` or `no configure`. Note that moving directly from/to Standard mode to/from Config mode is not possible.
Config Interface Management	Configuration mode for management interface mgmt0, mgmt1 and loopback.
Config Interface Ethernet	Configuration mode for Ethernet interface.
Config Interface Port Channel	Configuration mode for Port channel (LAG).
Config VLAN	Configuration mode for VLAN.
Any Command Mode	Several commands such as “show” can be applied within any context.

3.1.2 Syntax Conventions

To help you identify the parts of a CLI command, this section explains conventions of presenting the syntax of commands.

Table 8 - Syntax Conventions

Syntax Convention	Description	Example
< > Angled brackets	Indicate a value/variable that must be replaced.	<1...65535> or <switch interface>
[ ] Square brackets	Enclose optional parameters. However, only one parameter out of the list of parameters listed can be used. The user cannot have a combination of the parameters unless stated otherwise.	[destination-ip | destination-port | destination-mac]
{ } Braces	Enclose alternatives or variables that are required for the parameter in square brackets.	[mode {active | on | passive}]
| Vertical bars	Identify mutually exclusive choices.	active | on | passive

Do not type the angled or square brackets, vertical bar, or braces in command lines. This guide uses these symbols only to show the types of entries.

CLI commands and options are in lowercase and are case-sensitive.

For example, when you enter the `enable` command, enter it all in lowercase. It cannot be ENABLE or Enable. Text entries you create are also case-sensitive.

3.1.3 Getting Help

You may request context-sensitive help at any time by pressing “?” on the command line. This will show a list of choices for the word you are on, or a list of top-level commands if you have not typed anything yet.

For example, if you are in Standard mode and you type “?” at the command line, then you will get the following list of available commands.

```
switch > ?
cli              Configure CLI shell options
enable           Enter enable mode
exit             Log out of the CLI
help             View description of the interactive help system
no               Negate or clear certain configuration options
show             Display system configuration or statistics
```

```
slogin          Log into another system securely using ssh
switch          Configure switch on system
telnet          Log into another system using telnet
terminal        Set terminal parameters
traceroute      Trace the route packets take to a destination
switch-11a596 [standalone: master] >
```

If you type a legal string and then press "?" *without* a space character before it, then you will either get a description of the command that you have typed so far or the possible command/parameter completions. If you press "?" *after* a space character and "<cr>" is shown, this means that what you have entered so far is a complete command, and that you may press Enter (carriage return) to execute it.

Try the following to get started:

```
?
show ?
show c?
show clock?
show clock ?
show interfaces ?     (from enable mode)
```

You can also enter "help" to view a description of the interactive help system.

Note also that the CLI supports command and/or parameter tab-completions and their shortened forms. For example, you can enter "en" instead of the "enable" command, or "cli cl" instead of "cli clear-history". In case of ambiguity (more than one completion option is available, that is), then you can hit double tabs to obtain the disambiguation options. Thus, if you are in Enable mode and wish to learn which commands start with the letter "c", type "c" and click twice on the tab key to get the following:

```
switch # c<tab>
clear       cli       configure
switch # c
```

(There are three commands that start with the letter "c": `clear`, `cli` and `configure`.)

3.1.4 Prompt and Response Conventions

The prompt always begins with the hostname of the system. What follows depends on what command mode the user is in. To demonstrate by example, assuming the machine name is "`switch`", the prompts for each of the modes are:

```
switch >              (Standard mode)
switch #              (Enable mode)
switch (config) #     (Config mode)
```

The following session shows how to move between command modes: \

```
switch >   (You start in Standard mode)
switch > enable   (Move to Enable mode)
switch #   (You are in Enable mode)
switch # configure terminal                          (Move to Config mode)
switch (config) #   (You are in Config mode)
switch (config) # exit   (Exit Config mode)
switch #   (You are back in Enable mode)
switch # disable   (Exit Enable mode)
switch >   (You are back in Standard mode)
```

Commands entered do not print any response and simply show the command prompt after you press <Enter>.

If an error is encountered in executing a command, the response will begin with “%”, followed by some text describing the error.

3.1.5 Using the “no” Form

Several Config mode commands offer the negation form using the keyword “no”. This no form can be used to disable a function, to cancel certain command parameters or options, or to reset a parameter value to its default. To re-enable a function or to set cancelled command parameters or options, enter the command without the “no” keyword (with parameter values if necessary).

The following example performs the following:

1. Displays the current CLI session options.
2. Disables auto-logout.
3. Displays the new CLI session options (auto-logout is disabled).
4. Re-enables auto-logout (after 15 minutes).
5. Displays the final CLI session options (auto-logout is enabled)

```
// 1. Display the current CLI session options
switch (config) # show cli
CLI current session settings:
  Maximum line size:        8192
  Terminal width:           157 columns
  Terminal length:          60 rows
  Terminal type:            xterm
  Auto-logout:              15 minutes
  Paging:                   enabled
  Progress tracking:        enabled
  Prefix modes:             enabled
  ...
// 2. Disable auto-logout
switch (config) # no cli session auto-logout
// 3. Display the new CLI session options
switch-1 [standalone: master] (config) # show cli
CLI current session settings:
  Maximum line size:        8192
  Terminal width:           157 columns
  Terminal length:          60 rows
  Terminal type:            xterm
  Auto-logout:              disabled
  Paging:                   enabled
  Progress tracking:        enabled
  Prefix modes:             enabled
  ...
// 4. Re-enable auto-logout after 15 minutes
switch (config) # cli session auto-logout 15
```

```
// 5. Display the final CLI session options
switch (config) # show cli
CLI current session settings:
  Maximum line size:        8192
  Terminal width:           157 columns
  Terminal length:          60 rows
  Terminal type:            xterm
  Auto-logout:              15 minutes
  Paging:                   enabled
  Progress tracking:        enabled
  Prefix modes:             enabled
  ...
```

3.1.6 Parameter Key

This section provides a key to the meaning and format of all of the angle-bracketed parameters in all the commands that are listed in this document.

Table 9 - Angled Brackets Parameter Description

Parameter	Description
<domain>	A domain name, e.g. “mellanox.com”.
<hostname>	A hostname, e.g. “`switch-1`”.
<ifname>	An interface name, e.g. “mgmt0”, “mgmt1”, “lo” (loopback), etc.
<index>	A number to be associated with aliased (secondary) IP addresses.
<IP address>	An IPv4 address, e.g. “192.168.0.1”.
<log level>	A syslog logging severity level. Possible values, from least to most severe, are: “debug”, “info”, “notice”, “warning”, “error”, “crit”, “alert”, “emerg”.
<GUID>	Globally Unique Identifier. A number that uniquely identifies a device or component.
<MAC address>	A MAC address. The segments may be 8 bits or 16 bits at a time, and may be delimited by “:” or “.”. So you could say “11:22:33:44:55:66”, “1122:3344:5566”, “11.22.33.44.55.66”, or “1122.3344.5566”.
<netmask>	A netmask (e.g. “255.255.255.0”) or mask length prefixed with a slash (e.g. “/24”). These two express the same information in different formats.
<network prefix>	An IPv4 network prefix specifying a network. Used in conjunction with a netmask to determine which bits are significant. e.g. “192.168.0.0”.
<regular expression>	An extended regular expression as defined by the “grep” in the man page. (The value you provide here is passed on to “grep -E”.)
<node id>	ID of a node belonging to a cluster. This is a numerical value greater than zero.
<cluster id>	A string specifying the name of a cluster.
<port>	TCP/UDP port number.

Table 9 - Angled Brackets Parameter Description

Parameter	Description
<TCP port>	A TCP port number in the full allowable range [0...65535].
<URL>	A normal URL, using any protocol that wget supports, including http, https, ftp, sftp, and tftp; or a pseudo-URL specifying an scp file transfer. The scp pseudo-URL format is scp://username:password@hostname/path/filename. Note that the path is an absolute path. Paths relative to the user's home directory are not currently supported. The implementation of ftp does not support authentication, so use scp or sftp for that. Note also that if you omit the ":password" part, you may be prompted for the password in a follow up prompt, where you can type it securely (without the characters being echoed). This prompt will occur if the "cli default prompt empty-password" setting is true; otherwise, the CLI will assume you do not want any password. If you include the ":" character, this will be taken as an explicit declaration that the password is empty, and you will not be prompted in any case.

3.1.7 Command Output Filtering

The MLNX-OS CLI supports filtering "show" commands to display lines containing or excluding certain phrases or characters. To filter the outputs of the "show" commands use the following format:

```
switch (config) # <show command> | [include | exclude] <extended regular expression>
[<ignore-case>] [next <lines>] [prev <lines>]
```

The filtering parameters are separated from the show command they filter by a pipe character (i.e. "|"). Quotation marks may be used to include or exclude a string including space, and multiple filters can be used simultaneously. For example:

```
switch (config) # <show command> | [include <extended regular expression> [<ignore-case>]
[next <lines>] [prev <lines>] | exclude <extended regular expression> [<ignore-case>]
[next <lines>] [prev <lines>]]
```

Examples:

```
switch (config) # switch (config) # switch (config) # show asic-version | include SX
SX module Version
SX 9.2.5440

arc-switch14 [standalone: master] (config) # show module | exclude PS==================
Module Type Present Power Is Fatal ==================================================
MGMT SX1036 1 N/A Not Fatal
FAN SXX0XX_FAN 1 N/A Not Fatal
CPU CPU 1 N/A Not Fatal

arc-switch14 [standalone: master] (config) # show interfaces | include "Eth|discard pac"
Eth1/1
0 discard packets
0 discard packets
Eth1/2
0 discard packets
0 discard packets
```

```
Eth1/3
0 discard packets
0 discard packets
Eth1/4
0 discard packets
0 discard packets
switch (config) # show interfaces | include "Tx" next 5 | exclude broad
Tx
0 packets
0 unicast packets
0 multicast packets
0 bytes
--
Tx
0 packets
0 unicast packets
0 multicast packets
0 bytes
```

3.2 Web Interface Overview

MLNX-OS® package equipped with web interface which is a web GUI that accept input and provide output by generating webpages which can be viewed by the user using a web browser.

The following web browsers are supported:

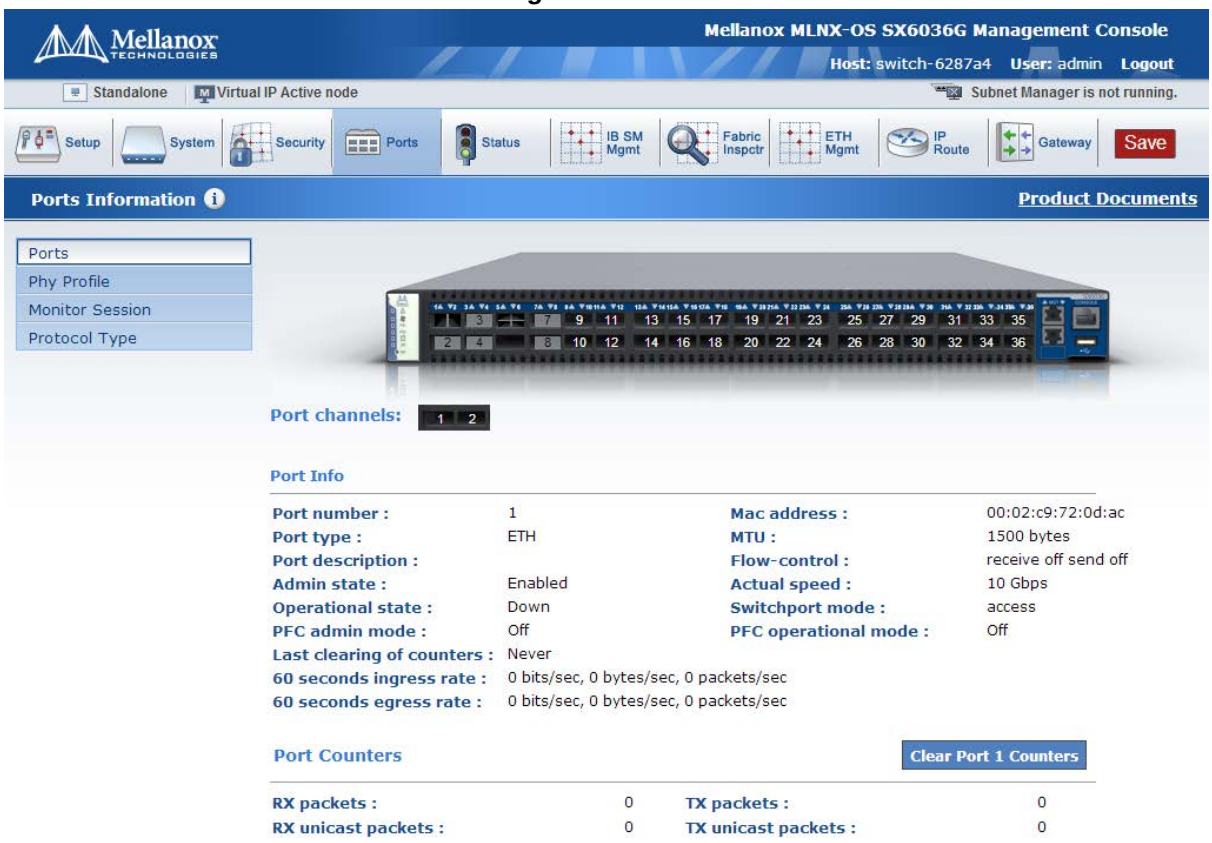
- Internet Explorer 8.0 or higher
- Chrome 18 or higher
- Mozilla Firefox 12 or higher
- Safari 5 or higher

The web interface makes available the following perspective tabs:

- Setup
- System
- Security
- Ports
- Status
- IB SM Management
- Fabric Inspector
- Ethernet Management
- IP Route
- Gateway

Make sure to save your changes before switching between menus or submenus. Click the “Save” button to the right of “Save Changes?”.

Figure 9: WebUI



3.2.1 Setup Menu

The **Setup** menu makes available the following submenus (listed in order of appearance from top to bottom):

Table 10 - Setup Submenus

Submenu Title	Description
Interfaces	Obtains the status of, configures, or disables interfaces to the InfiniBand fabric. Thus, you can: set or clear the IP address and netmask of an interface; enable DHCP to dynamically assign the IP address and netmask; and set interface attributes such as MTU, speed, duplex, etc.
HA	Creates, joins or modifies an InfiniBand subnet.
Routing	Configures, removes or displays the default gateway, and the static and dynamic routes.
Hostname	Configures or modifies the hostname. Configures or deletes static hosts. **Note:** Changing hostname stamps a new HTTPS certificate.
DNS	Configures, removes, modifies or displays static and dynamic name servers.
Login Messages	Edits the login messages: Message of the Day (MOTD), Remote Login message, and Local Login message.

Table 10 - Setup Submenus

Submenu Title	Description
Address Resolution	Adds static and dynamic ARP entries, and clears the dynamic ARP cache.
IPSec	Configures IPSec.
Neighbors	Displays IPv6 neighbor discovery protocol.
Virtualization	Manages the virtualization and virtual machines.
Virtual Switch Mgmt	Configures the system profile.
Web	Configures web user interface and proxy settings.
SNMP	Configures SNMP attributes, SNMP admin user, and trap sinks.
Email Alerts	Configures the destination of email alerts and the recipients to be notified.
XML gateway	Provides an XML request-response protocol to get and set hardware management information.
Logs	Sets up system log files, remote log sinks, and log formats.
Configurations	Manages, activates, saves, and imports MLNX-OS SwitchX configuration files, and executes CLI commands.
Date and Time	Configures the date, time, and time zone of the switch system.
NTP	Configures NTP (Network Time Protocol) and NTP servers.
Licensing	Manages MLNX-OS licenses.

3.2.2 System Menu

The **System** menu makes available the following sub-menus (listed in order of appearance from top to bottom):

Table 11 - System Submenus

Submenu Title	Description
Modules	Displays a graphic illustration of the system modules. By moving the mouse over the ports in the front view, a pop-up caption is displayed to indicate the status of the port. The port state (active/down) is differentiated by a color scheme (green for active, gray/black for down). By moving the mouse over the rear view, a pop-up caption is displayed to indicate the leaf part information.
Inventory	Displays a table with the following information about the system modules: module name, type, serial number, ordering part number and Asic firmware version.
Power Management	Displays a table with the following information about the system power supplies: power supply name, power, voltage level, current consumption, and status. A total power summary table is also displayed providing the power used, the power capacity, and the power available.
MLNX-OS Upgrade	Displays the installed MLNX-OS images (and the active partition), uploads a new image, and installs a new image.

Table 11 - System Submenus

Submenu Title	Description
Reboot	Reboots the system. Make sure that you save your configuration prior to clicking reboot.

3.2.3 Security Menu

The **Security** menu makes available the following sub-menus (listed in order of appearance from top to bottom):

Table 12 - Security Submenus

Submenu Title	Description
Users	Manages (setting up, removing, modifying) user accounts.
Admin Password	Modifies the system administrator password.
SSH	Displays and generate host keys.
AAA	Configures AAA (Authentication, Authorization, and Accounting) security services such as authentication methods and authorization.
Login Attempts	Manages login attempts
RADIUS	Manages Radius client.
TACACS+	Manages TACACS+ client.
LDAP	Manages LDAP client.
Certificate	Manages certificates.

3.2.4 Ports Menu

The Ports menu displays the port state and enables some configuration attributes of a selected port. It also enables modification of the port configuration. A graphical display of traffic over time (last hour or last day) through the port is also available.

Table 13 - Ports Submenus

Submenu Title	Description
Ports	Manages port attributes, counters, transceiver info and displays a graphical counters histogram.
Phy Profile	Provides the ability to manage phy profiles.
Monitor Session	Displays monitor session summary and enables configuration of a selected session.

3.2.5 Status Menu

The **Status** menu makes available the following sub-menus (listed in order of appearance from top to bottom):

Table 14 - Status Submenus

Submenu Title	Description
Summary	Displays general information about the switch system and the MLNX-OS image, including current date and time, hostname, uptime of system, system memory, CPU load averages, etc.
Profile and Capabilities	Displays general information about the switch system capabilities such as the enabled profiles (e.g IB/ETH) and their corresponding values.
Temperature	Provides a graphical display of the switch module sensors' temperature levels over time (1 hour). It is possible to display either the temperature level of one module's sensor or the temperature levels of all the module sensors' together.
Power Supplies	Provides a graphical display of one of the switch's power supplies voltage level over time (1 hour).
Fans	Provides a graphical display of fan speeds over time (1 hour). The display is per fan unit within a fan module.
CPU Load	Provides a graphical display of the management CPU load over time (1 hour).
Memory	Provides a graphical display of memory utilization over time (1 day).
Network	Provides a graphical display of network usage (transmitted and received packets) over time (1 day). It also provides per interface statistics.
Logs	Displays the system log messages. It is possible to display either the currently saved system log or a continuous system log.
Maintenance	Performs specific maintenance operations automatically on a predefined schedule.
Alerts	Displays a list of the recent health alerts and enables the user to configure health settings.

3.2.6 ETH Mgmt

The Eth Mgmt menu is not applicable when the switch profile is not Ethernet or VPI.

The **ETH Mgmt** menu makes available the following sub-menus (listed in order of appearance from top to bottom):

Table 15 - ETH Mgmt Submenus

Submenu Title	Description
Spanning Tree	Configures and monitors spanning tree protocol.

Table 15 - ETH Mgmt Submenus

Submenu Title	Description
MAC Table	Configures static mac addresses in the switch, and displays the MAC address table.
Link Aggregation	Configures and monitors aggregated Ethernet links (LAG) and configures LACP.
VLAN	Manages the switch VLAN table.
IGMP Snooping	Manages IGMP snooping in the switch.
ACL	Manages Access Control in the switch.
Priority Flow Control	Manages priority flow control.

3.2.7 IP Route

The **IP Route** menu makes available the following sub-menus (listed in order of appearance from top to bottom):

Table 16 - IP Route Submenus

Submenu Title	Description
Router Global	Enables/disables IP Routing protocol on the machine.
IP Route	Not implemented.
IP Interface	Not implemented.
Address Resolution	Not implemented.
IP Diagnostic	Not implemented.

3.3 Secure Shell (SSH)

It is recommended not to use more than 100 concurrent SSH sessions to the switch.

3.3.1 Adding a Host and Providing an SSH Key

➢ ***To add entries to the global known-hosts configuration file and its SSH value:***

Step 1. Change to Config mode Run:

```
switch [standalone: master] > enable
switch [standalone: master] # configure terminal
switch [standalone: master] (config) #
```

Step 2. Add an entry to the global known-hosts configuration file and its SSH value. Run:

```
switch [standalone: master] (config) # ssh client global known-host "myserver ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAsXeklqc8T0EN2mnMcVcfhueaRYzIVqt4rVsrERIjmlJh4mkYYIa8hGGikNa+
t5xw2dRrNxnHYLK51bUsSG1ZNwZT1Dpme3pAZeMY7G4ZMgGIW9xOuaXgAA3eBeoUjFdi6+1BqchWk0nTb+gMfI/
MK/heQNns7AtTrvqg/O5ryIc=″
switch [standalone: master] (config) #
```

Step 3. Verify what keys exist in the host. Run:

```
switch [standalone: master] (config) # show ssh client
SSH client Strict Hostkey Checking: ask

SSH Global Known Hosts:
    Entry 1: myserver
          Finger Print: d5:d7:be:d7:6c:b1:e4:16:df:61:25:2f:b1:53:a1:06

No SSH user identities configured.

No SSH authorized keys configured.

switch [standalone: master] (config) #
```

3.3.2 Retrieving Return Codes when Executing Remote Commands

➢ ***To stop the CLI and set the system to send return errors if some commands fail:***

Step 1. Connect to the system from the host SSH.

Step 2. Add the `-h` parameter after the `cli` (as shown in the example below) to notify the system to halt on failure and pass through the exit code.

```
ssh <username>@<hostname> cli -h '"enable" "show interfaces brief"'
```

3.4 Commands

3.4.1 CLI Session

This chapter displays all the relevant commands used to manage CLI session terminal.

cli clear-history

cli clear-history

Clears the command history of the current user.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	`switch (config) # cli clear-history` `switch (config) #`
Related Commands	N/A
Note	

cli default

cli default {auto-logout <minutes> | paging enable | prefix-modes {enable | show-config} | progress enable | prompt {confirm-reload | confirm-reset | confirm-unsaved | empty-password}
no cli default {auto-logout | paging enable | prefix-modes {enable | show-config} | progress enable prompt {confirm-reload | confirm-reset | confirm-unsaved | empty-password}

Configures default CLI options for all future sessions.
The no form of the command deletes or disables the default CLI options.

Syntax Description	minutes	Configures keyboard inactivity timeout for automatic logout. Range is 0-35791 minutes. Setting the value to 0 or using the no form of the command disables the auto-logout.
	paging enable	Enables text viewing one screen at a time.
	prefix-modes {enable | show-config}	Configures the prefix modes feature of CLI. • "prefix-modes enable" enables prefix modes for current and all future sessions • "prefix-modes show-config" uses prefix modes in "show configuration" output for current and all future sessions
	progress enable	Enables progress updates.
	prompt confirm-reload	Prompts for confirmation before rebooting.
	prompt confirm-reset	Prompts for confirmation before resetting to factory state.
	prompt confirm-unsaved	Confirms whether or not to save unsaved changes before rebooting.
	prompt empty-password	Prompts for a password if none is specified in a pseudo-URL for SCP.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # cli default prefix-modes enable
switch (config) # show cli
CLI current session settings:
  Maximum line size:        8192
 Terminal width:           171 columns
  Terminal length:          38 rows
  Terminal type:            xterm
  X display setting:        (none)
  Auto-logout:              disabled
  Paging:                   enabled
  Progress tracking:        enabled
  Prefix modes:             disabled

CLI defaults for future sessions:
  Auto-logout:              disabled
  Paging:                   enabled
  Progress tracking:        enabled
  Prefix modes:             enabled (and use in 'show configuration')

Settings for both this session and future ones:
  Show hidden config:        yes
  Confirm losing changes:    yes
  Confirm reboot/shutdown:   no
  Confirm factory reset:     yes
  Prompt on empty password:  yes
switch (config) #
```

Related Commands show cli

Note

cli session

cli session {auto-logout <minutes> | paging enable | prefix-modes {enable | show-config} | progress enable | terminal {length <size> | resize | type <terminal-type> | width} | x-display full <display>}
no cli session {auto-logout | paging enable | prefix-modes {enable | show-config} | progress enable | terminal type | x-display}

Configures default CLI options for all future sessions.
The no form of the command deletes or disables the CLI sessions.

Syntax Description	minutes	Configures keyboard inactivity timeout for automatic logout. Range is 0-35791 minutes. Setting the value to 0 or using the no form of the command disables the auto logout.
	paging enable	Enables text viewing one screen at a time.
	prefix-modes enable | show-config	Configures the prefix modes feature of CLI. • "prefix-modes enable" enables prefix modes for current and all future sessions • "prefix-modes show-config" uses prefix modes in "show configuration" output for current and all future sessions
	progress enable	Enables progress updates.
	terminal length	Sets the number of lines for the current terminal. Valid range is 5-999.
	terminal resize	Resizes the CLI terminal settings (to match the actual terminal window).
	terminal-type	Sets the terminal type. Valid options are: • ansi • console • dumb • linux • unknown • vt52 • vt100 • vt102 • vt220 • vt320 • xterm
	terminal width	Sets the width of the terminal in characters. Valid range is 34-999.
	x-display full <display>	Specifies the display as a raw string, e.g localhost:0.0.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # cli session auto-logout` `switch (config) #`
Related Commands	show terminal
Note	

show cli

show cli

Displays the CLI configuration and status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # show cli`
	`CLI current session settings:`
	`  Maximum line size:  8192`
	`  Terminal width:  171 columns`
	`  Terminal length:  38 rows`
	`  Terminal type:  xterm`
	`  X display setting:  (none)`
	`  Auto-logout:  disabled`
	`  Paging:  enabled`
	`  Progress tracking:  enabled`
	`  Prefix modes:  disabled`
	
	`CLI defaults for future sessions:`
	`  Auto-logout:  disabled`
	`  Paging:  enabled`
	`  Progress tracking:  enabled`
	`  Prefix modes:  enabled (and use in 'show configuration')`
	
	`Settings for both this session and future ones:`
	`  Show hidden config:  yes`
	`  Confirm losing changes:  yes`
	`  Confirm reboot/shutdown:  no`
	`  Confirm factory reset:  yes`
	`  Prompt on empty password:  yes`
	`switch (config) #`

Related Commands	cli default
Note	

3.4.2 Banner

banner login

banner {login | login-remote | login-local} <string>
no banner login

Sets the CLI welcome banner message. The login-remote refers to the SSH connections banner, while the login-local refers to the serial connection banner.
The no form of the command resets the system login banner to its default.

Syntax Description	string Text string.
Default	“Mellanox MLNX-OS Switch Management”
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # banner login example`
	`switch (config) # show banner`
	`Banners:`
	`  MOTD:`
	`Mellanox Switch`
	
	`  Login: example`
	`switch (config) #`

Related Commands	show banner
Note	If more then one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).

banner login-local

banner login-local <string>
no banner login-local

Sets system login local banner.
The no form of the command resets the banner.

Syntax Description	string	Text string.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # banner login-local Testing` `switch (config) #`	
Related Commands	show banner	
Note	If more then one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).	

banner login-remote

banner login-remote <string>
no banner login-remote

Sets system login remote banner.
The no form of the command resets the banner.

Syntax Description	string	Text string.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # banner login-remote Testing` `switch (config) #`	
Related Commands	show banner	
Note	If more then one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).	

banner motd

banner motd <string>
no banner motd

Sets the message of the day banner.
The no form of the command resets the system Message of the Day banner.

Syntax Description	string	Text string.
Default	“Mellanox Switch”	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # banner motd “My Banner”`
	`switch (config) # show banner`
	`Banners:`
	`  MOTD: My-Banner`
	`  Login:`
	`Mellanox MLNX-OS Switch Management`
	`switch (config) #`	

Related Commands	show banner	
Note	• If more then one word is used (there is a space) quotation marks should be added (i.e. "xxxx xxxx"). • To insert a multi-line MotD, hit Ctrl-V (escape sequence) followed by Ctrl-J (new line sequence). The symbol “^J” should appear. Then, whatever is typed after it becomes the new line of the MotD. Remember to also include the string between quotation marks.	

show banner

show banner

Displays configured banners.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	unpriv/monitor/admin

Example	`switch (config) # show banner`
	`Banners:`
	`    MOTD: Testing`
	`    Login:`
	`Mellanox MLNX-OS Switch Management`
	`switch (config) #`

Related Commands	banner login banner motd
Note	

3.4.3 SSH

ssh server enable

ssh server enable
no ssh server enable

Enables the SSH server.
The no form of the command disables the SSH server.

Syntax Description	N/A
Default	SSH server is enabled
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # ssh server enable`
	`switch (config) # show ssh server`
	`SSH server configuration:`
	`  SSH server enabled:  yes`
	`  Server security strict mode: no`
	`  Minimum protocol version: 2`
	`  TCP forwarding enabled:  yes`
	`  X11 forwarding enabled:  no`
	`  SSH server ports:  22`
	
	`  Interface listen enabled: yes`
	`  No Listen Interfaces.`
	
	`Host Key Finger Prints:`
	`  RSA v1 host key: a0:63:db:96:e2:95:5a:5a:fd:a8:d0:f4:ab:e3:5f:f8`
	`  RSA v2 host key: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6`
	`  DSA v2 host key: 7c:4a:f7:72:51:67:b5:0b:cd:a2:d2:b9:f3:be:3e:68`
	`switch (config) #`

Related Commands	show ssh server
Note	Disabling SSH server does not terminate existing SSH sessions, it only prevents new ones from being established.

ssh server host-key

ssh server host-key {<key type> {private-key <private-key>| public-key <public-key>} | generate}

Manipulates host keys for SSH.

Syntax Description	key type	• rsa1 - RSAv1 • rsa2 - RSAv2 • dsa2 - DSAv2
	private-key	Sets new private-key for the host keys of the specified type.
	public-key	Sets new public-key for the host keys of the specified type.
	generate	Generates new RSA and DSA host keys for SSH.
Default	SSH keys are locally generated	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # ssh server host-key dsa2 private-key
Key: *********************************************
Confirm: *********************************************
switch (config) # show ssh server host-keys
SSH server configuration:
   SSH server enabled:       yes
   Minimum protocol version: 2
   X11 forwarding enabled:   no
   SSH server ports:         22

   Interface listen enabled: yes
   No Listen Interfaces.

Host Key Finger Prints:
    RSA v1 host key: a0:63:db:96:e2:95:5a:5a:fd:a8:d0:f4:ab:e3:5f:f8
    RSA v2 host key: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6
    DSA v2 host key: 7c:4a:f7:72:51:67:b5:0b:cd:a2:d2:b9:f3:be:3e:68

Host Keys:
    RSA v1 host key: "switch-5ea5d8 1024 35
124574979953740101054914168679199879767768820169843759428319155849627 96
993754065960858042722190424504565987058666581448544931321723650687895 17
135705094208643369518330467004513542694677583792888489626241653307245 12
160918999830386915710362193855779785962822146445334448137121056286541 58
302298222057602977129709 3"
    RSA v2 host key: "switch-5ea5d8 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEArB9i5OnukAHNUOkwpCmEl0m88kJgBzL22+F5tfaSn+S
0pVYxrceZeyuzXsoZ1VtFTk2Fydwy0YvMS0Kcv2PuCrPZV/
GYd31QEnn22rEmrlPrKCrMl1XlUy6DFlr3OgwWm1baobmDlG/gSziWz/
gc4Jgqf2CyXFq4pzaR1jar1Vk="
    DSA v2 host key: "switch-5ea5d8 ssh-dss
AAAAB3NzaC1kc3MAAACBAMeJ3S+nyaHhRbwv3tJqlWttDC35RZVC5iG4ZEvMMHp28VL94Oc
yyuGh39VCdM9pEVaI7hzZrsgHrNqakb/YLD/
7anGH3wpl9Fx8lfe0RH3bloJzG+mJ6R5momdoPCrKwEKiKABKE00jLzlVznpP0IHxjwF+Tb
R3dK5HwVzQYw/
bAAAAFQCBoDPqBZZa+2KylKlzUsbZ2pKhgQAAAIAJK+StiQdtORw1B5UCMzTrTef5L07DSf
VreMEYtTRnBBtgVSNqQFWpSQIYbVDHQr9T6qCM4VO39DuHUGQ1TMDIX7t+9mfbB87YyUu5a
/ndbf3GhNhxHWwbzlr9hgLL7FSHA7DYH7bVOZRlqxH64eQKGZqy1ps/
F4E31lyn7GC4EQAAAIA/2osHipXf+NRjplgfmHROVVf/mGE9Vzc9/
AMUxlJJn5VhvEJ5CZW9cI+LxMOJojhOj3YW3B1czGxROb DA9vUbKXTNc8bkgoUrxySAH1rH
N0PqJgeT4L009AItSp3m1mxHqdS7jixfTvOTEKWXrgpczlmTB8+zjhUah/YuuBl2H
g=="
switch (config) #
```

Related Commands show ssh server

Note

ssh server listen

ssh server listen {enable | interface <inf>}
no ssh server listen {enable | interface <inf>}

Enables the listen interface restricted list for SSH. If enabled, and at least one non-DHCP interface is specified in the list, the SSH connections are only accepted on those specified interfaces.
The no form of the command disables the listen interface restricted list for SSH. When disabled, SSH connections are not accepted on any interface.

Syntax Description	enable	Enables SSH interface restrictions on access to this system.
	interface <inf>	Adds interface to SSH server access restriction list. Possible interfaces are “lo”, and “mgmt0”.
Default	SSH listen is enabled	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ssh server listen enable`
	`switch (config) # show ssh server`
	`SSH server configuration:`
	`  SSH server enabled:  yes`
	`  Minimum protocol version: 2`
	`  X11 forwarding enabled:  no`
	`  SSH server ports:  22`
	
	`  Interface listen enabled: yes`
	`  No Listen Interfaces.`
	
	`Host Key Finger Prints:`
	`  RSA v1 host key: a0:63:db:96:e2:95:5a:5a:fd:a8:d0:f4:ab:e3:5f:f8`
	`  RSA v2 host key: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6`
	`  DSA v2 host key: 7c:4a:f7:72:51:67:b5:0b:cd:a2:d2:b9:f3:be:3e:68`
	`switch (config) #`	

Related Commands	show ssh server	
Note		

ssh server min-version

ssh server min-version <version>
no ssh server min-version

Sets the minimum version of the SSH protocol that the server supports.
The no form of the command resets the minimum version of SSH protocol supported.

Syntax Description	version	Possible versions are 1 and 2.
Default	2	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example		

```
switch (config) # ssh server min-version 2
switch (config) # show ssh server
SSH server configuration:
   SSH server enabled:       yes
   Minimum protocol version: 2
   X11 forwarding enabled:   no
   SSH server ports:         22

   Interface listen enabled: yes
   No Listen Interfaces.

Host Key Finger Prints:
    RSA v1 host key: a0:63:db:96:e2:95:5a:5a:fd:a8:d0:f4:ab:e3:5f:f8
    RSA v2 host key: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6
    DSA v2 host key: 7c:4a:f7:72:51:67:b5:0b:cd:a2:d2:b9:f3:be:3e:68
switch (config) #
```

Related Commands	show ssh server
Note	

ssh server ports

ssh server ports {<port1> [<port2>...]}

Specifies which ports the SSH server listens on.

Syntax Description	port	Port number in [1...65535].
Default	22.	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ssh server ports 22`
	`switch (config) # show ssh server`
	`SSH server configuration:`
	`SSH server enabled: yes`
	`Minimum protocol version: 2`
	`X11 forwarding enabled: no`
	`SSH server ports: 22`
	
	`Interface listen enabled: yes`
	`No Listen Interfaces.`
	
	`Host Key Finger Prints:`
	`RSA v1 host key: a0:63:db:96:e2:95:5a:5a:fd:a8:d0:f4:ab:e3:5f:f8`
	`RSA v2 host key: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6`
	`DSA v2 host key: 7c:4a:f7:72:51:67:b5:0b:cd:a2:d2:b9:f3:be:3e:68`
	`switch (config) #`	

Related Commands	show ssh server	
Note	• Multiple ports can be specified by repeating the <port> parameter • The command will remove any previous ports if not listed in the command	

ssh server x11-forwarding

ssh server x11-forwarding enable
no ssh server x11-forwarding enable

Enables X11 forwarding on the SSH server.
The no form of the command disables X11 forwarding.

Syntax Description	N/A
Default	X11-forwarding is disabled.
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # ssh server x11-forwarding enable`
	`switch (config) # show ssh server`
	`SSH server configuration:`
	`   SSH server enabled:       yes`
	`   Minimum protocol version: 2`
	`   X11 forwarding enabled:   yes`
	`   SSH server ports:         22`
	
	`   Interface listen enabled: yes`
	`   No Listen Interfaces.`
	
	`Host Key Finger Prints:`
	`    RSA v1 host key: a0:63:db:96:e2:95:5a:5a:fd:a8:d0:f4:ab:e3:5f:f8`
	`    RSA v2 host key: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6`
	`    DSA v2 host key: 7c:4a:f7:72:51:67:b5:0b:cd:a2:d2:b9:f3:be:3e:68`
	`switch (config) #`

Related Commands	N/A
Note	

ssh client global

ssh client global {host-key-check <policy>} | known-host <known-host-entry>}
no ssh client global {host-key-check | known-host localhost}

Configures global SSH client settings.
The no form of the command negates global SSH client settings.

Syntax Description	host-key-check <policy>	Sets SSH client configuration to control how host key checking is performed. This parameter may be set in 3 ways. • If set to “no” it always permits connection, and accepts any new or changed host keys without checking • If set to “ask” it prompts user to accept new host keys, but does not permit a connection if there was already a known host entry that does not match the one presented by the host • If set to “yes” it only permits connection if a matching host key is already in the known hosts file
	known-host	Adds an entry to the global known-hosts configuration file.
	known-host-entry	Adds/removes an entry to/from the global known-hosts configuration file. The entry consist of “<IP> <key-type> <key>”.
Default	host-key-check - ask, no keys are configured by default	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # ssh client global host-key-check no
switch (config) # ssh client global known-host "72.30.2.2 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEArB9i5OnukAHNUOkwpCmEl0m88kJgBzL22+F5tfaSn+S
0pVYxrceZeyuzXsoZ1VtFTk2Fydwy0YvMS0Kcv2PuCrPZV/
GYd31QEnn22rEmrlPrKCrMl1XlUy6DFlr3OgwWm1baobmDlG/gSziWz/
gc4Jgqf2CyXFq4pzaR1jar1Vk="

switch (config) # show ssh client
SSH client Strict Hostkey Checking: ask

SSH Global Known Hosts:
    Entry 1: 72.30.2.2
          Finger Print: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6

No SSH user identities configured.

No SSH authorized keys configured.

switch (config) #
```

Related Commands	show ssh client
Note	

ssh client user

ssh client user <username> {authorized-key sshv2 <public key> | identity <key type> {generate | private-key [<private key>] | public-key [<public key>]} | known-host <known host> remove}
no ssh client user admin {authorized-key sshv2 <public key ID> | identity <key type>}

Adds an entry to the global known-hosts configuration file, either by generating new key, or by adding manually a public or private key.
The no form of the command removes a public key from the specified user's authorized key list, or changes the key type.

Syntax Description	username	The specified user must be a valid account on the system. Possible values for this parameter are “admin”, “monitor”, “xmladmin”, and “xmluser”.
	authorized-key sshv2 <public key>	Adds the specified key to the list of authorized SSHv2 RSA or DSA public keys for this user account. These keys can be used to log into the user's account.
	identity <key type>	Sets certain SSH client identity settings for a user, dsa2 or rsa2.
	generate	Generates SSH client identity keys for specified user.
	private-key	Sets private key SSH client identity settings for the user.
	public-key	Sets public key SSH client identity settings for the user.
	known-host <known host> remove	Removes host from user's known host file.
Default	No keys are created by default	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ssh client user admin known-host 172.30.1.116 remove` `switch (config) #`	
Related Commands	show ssh client	
Note	If a key is being pasted from a cut buffer and was displayed with a paging program, it is likely that newline characters have been inserted, even if the output was not long enough to require paging. One can specify “no cli session paging enable” before running the “show” command to prevent the newlines from being inserted.	

slogin

slogin [<slogin options>] <hostname>

Invokes the SSH client. The user is returned to the CLI when SSH finishes.

Syntax Description	slogin options	usage: slogin [-1246AaCfgkNnqsTtVvXxY] [-b bind_address] [-c cipher_spec] [-D port] [-e escape_char] [-F configfile] [-i identity_file] [-L port:host:hostport] [-l login_name] [-m mac_spec] [-o option] [-p port] [-R port:host:hostport] [user@]host-name [command]
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	monitor/admin	

Example	`switch (config) # slogin 192.168.10.70`
	`The authenticity of host '192.168.10.70 (192.168.10.70)' can't be estab-lished.`
	`RSA key fingerprint is 2e:ad:2d:23:45:4e:47:e0:2c:ae:8c:34:f0:1a:88:cb.`
	`Are you sure you want to continue connecting (yes/no)? yes`
	`Warning: Permanently added '192.168.10.70' (RSA) to the list of known hosts.`
	
	`Mellanox MLNX-OS Switch Management`
	
	`Last login: Sat Feb 28 22:55:17 2009 from 10.208.0.121`
	
	`Mellanox Switch`
	
	`switch (config) #`	

Related Commands	N/A	
Note		

show ssh client

show ssh client

Displays the client configuration of the SSH server.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # show ssh client`
	`SSH client Strict Hostkey Checking: ask`
	
	`SSH Global Known Hosts:`
	`  Entry 1: 72.30.2.2`
	`  Finger Print: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6`
	
	`No SSH user identities configured.`
	
	`No SSH authorized keys configured.`
	
	`switch (config) #`

Related Commands	N/A
Note	

show ssh server

show ssh server

Displays SSH server configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000 3.3.5050 Updated Example
Role	admin

Example	`switch (config) # show ssh server`
	`SSH server configuration:`
	`SSH server enabled: yes`
	`Server security strict mode: no`
	`Minimum protocol version: 2`
	`TCP forwarding enabled: yes`
	`X11 forwarding enabled: no`
	`SSH server ports: 22`
	
	`Interface listen enabled: yes`
	`No Listen Interfaces.`
	
	`Host Key Finger Prints and Key Lengths:`
	`RSA v1 host key: 5f:4e:5f:4a:81:bb:6a:b4:06:52:77:eb:d3:ad:78:92 (2048)`
	`RSA v2 host key: 15:e2:a8:45:1c:58:1b:00:cc:29:ec:00:38:83:49:00 (2048)`
	`DSA v2 host key: df:c0:ac:a6:3e:a5:52:a5:d1:f6:22:37:ef:f1:08:f9 (1024)`
	
	`switch (config) #`

Related Commands	ssh server
Note	

3.4.4 Remote Login

telnet-server enable

telnet-server enable
no telnet-server enable

Enables the telnet server.
The no form of the command disables the telnet server.

Syntax Description	N/A
Default	Telnet server is disabled
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # telnet-server enable`
	`switch (config) # show telnet-server`
	`Telnet server enabled: yes`

Related Commands	show telnet-server
Note	

show telnet-server

show telnet-server

Displays telnet server settings.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # show telnet-server`
	`Telnet server enabled:  yes`
	`switch (config) #`

Related Commands	telnet-server enable
Note	

3.4.5 Web Interface

web auto-logout

web auto-logout <number of minutes>
no web auto-logout <number of minutes>

Configures length of user inactivity before auto-logout of a web session.
The no form of the command disables the web auto-logout (web sessions will never logged out due to inactivity).

Syntax Description	number of minutes	The length of user inactivity in minutes. 0 will disable the inactivity timer (same as a “no web auto-logout” command).
Default	60 minutes	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # web auto-logout 60
switch (config) # show web

Web User Interface:
   Web interface enabled:  yes
   HTTP enabled:           yes
   HTTP port:              80
   HTTP redirect to HTTPS: no
   HTTPS enabled:          yes
   HTTPS port:             443
   HTTPS ssl-ciphers:      all
   HTTPS certificate name: default-cert
  Listen enabled:         yes
   No Listen Interfaces.

   Inactivity timeout:     1 hr
   Session timeout:        2 hr 30 min
   Session renewal:        30 min

Web file transfer proxy:
   Proxy enabled: no

Web file transfer certificate authority:
   HTTPS server cert verify: yes
   HTTPS supplemental CA list: default-ca-list
switch (config) #
```

Related Commands	show web
Note	The no form of the command does not automatically log users out due to inactivity.

web client cert-verify

web client cert-verify
no web client cert-verify

Enables verification of server certificates during HTTPS file transfers.
The no form of the command disables verification of server certificates during HTTPS file transfers.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.2.3000
Role	admin
Example	`switch (config) # web client cert-verify`
Related Commands	N/A
Note	

web client ca-list

web client ca-list {<ca-list-name> | default-ca-list | none}
no web client ca-list

Configures supplemental CA certificates for verification of server certificates during HTTPS file transfers.
The no form of the command uses no supplemental certificates.

Syntax Description	ca-list-name	Specifies CA list to configure.
	default-ca-list	Configures default supplemental CA certificate list.
	none	Uses no supplemental certificates.
Default	default-ca-list	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # web client ca-list default-ca-list`	
Related Commands	N/A	
Note		

web enable

web enable
no web enable

Enables the web-based management console.
The no form of the command disables the web-based management console.

Syntax Description	N/A
Default	enable
Configuration Mode	Config
History	3.1.0000 3.3.5050 Updated Example
Role	admin

Example	`switch (config) # web enable`
	`switch (config) # show web`
	
	`Web User Interface:`
	`  Web interface enabled:  yes`
	`  HTTP enabled:  yes`
	`  HTTP port:  80`
	`  HTTP redirect to HTTPS: no`
	`  HTTPS enabled:  yes`
	`  HTTPS port:  443`
	`  HTTPS ssl-ciphers:  all`
	`  HTTPS certificate name: default-cert`
	`  Listen enabled:  yes`
	`  No Listen Interfaces.`
	
	`  Inactivity timeout:  1 hr`
	`  Session timeout:  2 hr 30 min`
	`  Session renewal:  30 min`
	
	`Web file transfer proxy:`
	`  Proxy enabled: no`
	
	`Web file transfer certificate authority:`
	`  HTTPS server cert verify: yes`
	`  HTTPS supplemental CA list: default-ca-list`
	`switch (config) #`

Related Commands	show web
Note	

web http

web http {enable | port <port number> | redirect}
no web http {enable | port | redirect}

Configures HTTP access to the web-based management console.
The no form of the command negates HTTP settings for the web-based management console.

Syntax Description	enable	Enables HTTP access to the web-based management console.
	port number	Sets a port for HTTP access.
	redirect	Enables redirection to HTTPS. If HTTP access is enabled, this specifies whether a redirect from the HTTP port to the HTTPS port should be issued to mandate secure HTTPS access.
Default	HTTP is enabled HTTP TCP port is 80 HTTP redirect to HTTPS is disabled	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # web http enable
switch (config) # show web

Web User Interface:
   Web interface enabled:  yes
   HTTP enabled:           yes
   HTTP port:              80
   HTTP redirect to HTTPS: no
   HTTPS enabled:          yes
   HTTPS port:             443
   HTTPS ssl-ciphers:      all
   HTTPS certificate name: default-cert
  Listen enabled:         yes
   No Listen Interfaces.

   Inactivity timeout:     1 hr
   Session timeout:        2 hr 30 min
   Session renewal:        30 min

Web file transfer proxy:
   Proxy enabled: no

Web file transfer certificate authority:
   HTTPS server cert verify: yes
   HTTPS supplemental CA list: default-ca-list
switch (config) #
```

Related Commands	show web web enable
Note	Enabling HTTP is meaningful if the WebUI as a whole is enabled.

web httpd

web httpd listen {enable | interface <ifName> }
no web httpd listen {enable | interface <ifName> }

Enables the listen interface restricted list for HTTP and HTTPS.
The no form of the command disables the HTTP server listen ability.

Syntax Description	enable	Enables Web interface restrictions on access to this system.
	interface <ifName>	Adds interface to Web server access restriction list (i.e. mgmt0, mgmt1)
Default	Listening is enabled. all interfaces are permitted.	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # web httpd listen enable
switch (config) # show web

Web User Interface:
   Web interface enabled:  yes
   HTTP enabled:           yes
   HTTP port:              80
   HTTP redirect to HTTPS: no
   HTTPS enabled:          yes
   HTTPS port:             443
   HTTPS ssl-ciphers:      all
   HTTPS certificate name: default-cert
   Listen enabled:         yes
   No Listen Interfaces.

   Inactivity timeout:     1 hr
   Session timeout:        2 hr 30 min
   Session renewal:        30 min

Web file transfer proxy:
   Proxy enabled: no

Web file transfer certificate authority:
   HTTPS server cert verify: yes
   HTTPS supplemental CA list: default-ca-list
switch (config) #
```

Related Commands	N/A
Note	If enabled, and if at least one of the interfaces listed is eligible to be a listen interface, then HTTP/HTTPS requests will only be accepted on those interfaces. Otherwise, HTTP/HTTPS requests are accepted on any interface.

web https

web https {certificate {regenerate | name | default-cert} | enable | port <port number> | ssl ciphers {all | TLS1.2}}
no web https {enable | port <port number>}

Configures HTTPS access to the web-based management console.
The no form of the command negates HTTPS settings for the web-based management console.

Syntax Description	certificate regenerate	Re-generates certificate to use for HTTPS connections.
	certificate name	Configure the named certificate to be used for HTTPS connections
	certificate default-cert	Configure HTTPS to use the configured default certificate
	enable	Enables HTTPS access to the web-based management console.
	port	Sets a TCP port for HTTPS access.
	ssl ciphers {all | TLS1.2}	Sets SSL mode to be used for HTTPS.
Default	HTTPS is enabled Default port is 443	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Added “ssl ciphers” parameter
Role	admin	

Example

```
switch (config) # web https enable
switch (config) # show web

Web User Interface:
   Web interface enabled:  yes
   HTTP enabled:           yes
   HTTP port:              80
   HTTP redirect to HTTPS: no
   HTTPS enabled:          yes
   HTTPS port:             443
   HTTPS ssl-ciphers:      all
   HTTPS certificate name: default-cert
   Listen enabled:         yes
   No Listen Interfaces.

   Inactivity timeout:     1 hr
   Session timeout:        2 hr 30 min
   Session renewal:        30 min

Web file transfer proxy:
   Proxy enabled: no

Web file transfer certificate authority:
   HTTPS server cert verify: yes
   HTTPS supplemental CA list: default-ca-list
switch (config) #
```

Related Commands

show web
web enable

Note

- Enabling HTTPS is meaningful if the WebUI as a whole is enabled.
- See the command “crypto certificate default-cert name” for how to change the default certificate if inheriting the configured default certificate is preferred

web session

web session {renewal <minutes> | timeout <minutes>}
no web session {renewal | timeout}

Configures session settings.
The no form of the command resets session settings to default.

Syntax Description	renewal <minutes>	Configures time before expiration to renew a session.
	timeout <minutes>	Configures time after which a session expires.
Default	timeout - 2.5 hours renewal - 30 min	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # web session renewal 60
switch (config) # show web

Web User Interface:
   Web interface enabled:  yes
   HTTP enabled:           yes
   HTTP port:              80
   HTTP redirect to HTTPS: no
   HTTPS enabled:          yes
   HTTPS port:             443
   HTTPS ssl-ciphers:      all
   HTTPS certificate name: default-cert
   Listen enabled:         yes
   No Listen Interfaces.

   Inactivity timeout:     1 hr
   Session timeout:        2 hr 30 min
   Session renewal:        60 min

Web file transfer proxy:
   Proxy enabled: no

Web file transfer certificate authority:
   HTTPS server cert verify: yes
   HTTPS supplemental CA list: default-ca-list
switch (config) #
```

Related Commands	N/A
Note	

web proxy auth

web proxy auth {authtype <type>| basic [password <password> | username <username>]}
no web proxy auth {authtype | basic {password | username }

Configures authentication settings for web proxy authentication.
The no form of the command resets the attributes to their default values.

Syntax Description	type	Configures the type of authentication to use with web proxy. The possible values are: • basic - HTTP basic authentication • none - No authentication
	basic	Configures HTTP basic authentication settings for proxy. The password is accepted and stored in plaintext.
	password	A password used for HTTP basic authentication with the web proxy.
	username	A username used for HTTP basic authentication with the web proxy.
Default	Web proxy is disabled.	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # web proxy auth authtype basic
switch (config) # web proxy auth basic username web-user
switch (config) # web proxy auth basic password web-password
switch (config) # show web

Web User Interface:
   Web interface enabled:  yes
   HTTP enabled:           yes
   HTTP port:              80
   HTTP redirect to HTTPS: no
   HTTPS enabled:          yes
   HTTPS port:             443
   HTTPS ssl-ciphers:      all
   HTTPS certificate name: default-cert
   Listen enabled:         yes
   No Listen Interfaces.

   Inactivity timeout:     1 hr
   Session timeout:        2 hr 30 min
   Session renewal:        30 min

Web file transfer proxy:
   Proxy enabled: yes
   Proxy address:          10.10.10.11
   Proxy port:             40
   Authentication type:    basic
   Basic auth username:    web-user
   Basic auth password:    web-password

Web file transfer certificate authority:
   HTTPS server cert verify: yes
   HTTPS supplemental CA list: default-ca-list
switch (config) #
```

Related Commands

show web
web proxy host

Note

web proxy host

web proxy host <IP address> [port <port number>]
no web proxy

Adds and enables a proxy to be used for any HTTP or FTP downloads.
The no form of the command disables the web proxy.

Syntax Description	IP address	IPv4 or IPv6 address.
	port number	Sets the web proxy default port.
Default	1080	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # web proxy host 10.10.10.10 port 1080
switch (config) # show web

Web User Interface:
   Web interface enabled:  yes
   HTTP enabled:           yes
   HTTP port:              80
   HTTP redirect to HTTPS: no
   HTTPS enabled:          yes
   HTTPS port:             443
   HTTPS ssl-ciphers:      all
   HTTPS certificate name: default-cert
   Listen enabled:         yes
   No Listen Interfaces.

   Inactivity timeout:     1 hr
   Session timeout:        2 hr 30 min
   Session renewal:        30 min

Web file transfer proxy:
   Proxy enabled: yes
   Proxy address:          10.10.10.10
   Proxy port:             1080
   Authentication type:    basic
   Basic auth username:    web-user
   Basic auth password:    web-password

Web file transfer certificate authority:
   HTTPS server cert verify: yes
   HTTPS supplemental CA list: default-ca-list
switch (config) #
```

Related Commands	web proxy auth
Note	

show web

show web

Displays the web configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000 3.3.5050 Updated Example
Role	admin

Example	`switch (config) # show web`
	
	`Web User Interface:`
	`  Web interface enabled:  yes`
	`  HTTP enabled:  yes`
	`  HTTP port:  80`
	`  HTTP redirect to HTTPS: no`
	`  HTTPS enabled:  yes`
	`  HTTPS port:  443`
	`  HTTPS ssl-ciphers:  all`
	`  HTTPS certificate name: default-cert`
	`  Listen enabled:  yes`
	`  No Listen Interfaces.`
	
	`  Inactivity timeout:  1 hr`
	`  Session timeout:  2 hr 30 min`
	`  Session renewal:  30 min`
	
	`Web file transfer proxy:`
	`  Proxy enabled: yes`
	`  Proxy address:  10.10.10.11`
	`  Proxy port:  40`
	`  Authentication type:  basic`
	`  Basic auth username:  web-user`
	`  Basic auth password:  web-password`
	
	`Web file transfer certificate authority:`
	`  HTTPS server cert verify: yes`
	`  HTTPS supplemental CA list: default-ca-list`
	`switch (config) #`

Related Commands	show web web proxy auth
Note	

4 System Management

4.1 Management Interface

4.1.1 Configuring Management Interfaces with Static IP Addresses

If your switch system was set during initialization to obtain dynamic IP addresses through DHCP and you wish to switch to static assignments, perform the following steps:

Step 1. Enter Config mode. Run:

```
switch >
switch > enable
switch # configure terminal
```

Step 2. Disable setting IP addresses using the DHCP using the following command:

```
switch (config) # no interface <ifname> dhcp
```

Step 3. Define your interfaces statically using the following command:

```
switch (config) # interface <ifname> ip address <IP address> <netmask>
```

4.1.2 Configuring IPv6 Address on the Management Interface

Step 1. Enable IPv6 on this interface.

```
switch (config) # interface mgmt0 ipv6 enable
```

Step 2. Set the IPv6 address to be configured automatically.

```
switch (config) # interface mgmt0 ipv6 address autoconfig
```

Step 3. Verify the IPv6 address is configured correctly.

```
switch (config) # show interfaces mgmt0 brief
```

4.1.3 Dynamic Host Configuration Protocol (DHCP)

DHCP is used for automatic retrieval of management IP addresses.

For all other systems (and software versions) DHCP is disabled by default.

If a user connects through SSH, runs the wizard and turns off DHCP, the connection is immediately terminated as the management interface loses its IP address.

```
<localhost># ssh admin@<ip-address>
Mellanox MLNX-OS Switch Management
Password:
Mellanox Switch
Mellanox configuration wizard
Do you want to use the wizard for initial configuration? yes
Step 1: Hostname? [my-switch]
Step 2: Use DHCP on mgmt0 interface? [yes] no
<localhost>#
```

In such case the serial connection should be used.

4.1.4 Default Gateway

To configure manually the default gateway, use the “ip route” command, with “0.0.0.0” as prefix and mask. The next-hop address must be within the range of one of the IP interfaces on the system.

```
switch (config)# ip route 0.0.0.0 0.0.0.0 10.209.0.2
switch (config)# show ip route
Destination       Mask             Gateway           Interface   Source
default           0.0.0.0          10.209.0.2        mgmt0       static
10.209.0.0        255.255.254.0    0.0.0.0           mgmt0       direct
switch (config)#
```

4.1.5 In-Band Management

In-band management is a management path passing through the data ports. In-band management can be created over one of the VLANs in the systems.

The in-band management feature does not require any license. However, it works only for system profiles VPI and Ethernet. It cannot be enabled with IP Routing or IP Proxy-ARP.

➢ ***To set an in-band management channel:***

Step 1. Create a VLAN. Run:

```
switch (config) # vlan 10
switch (config vlan 10) #
```

Step 2. Create a VLAN interface. Run:

```
switch (config) # interface vlan 10 create
```

Step 3. Enter the VLAN interface configuration mode and configure L3 attributes. Run:

```
switch (config) # interface vlan10
switch (config interface vlan10)#ip address 10.10.10.10 /24
```

Step 4. (Optional) Verify in-band management configuration. Run:

```
switch (config) # show interfaces vlan10
Interface vlan10 status:
   Comment:
   Admin up:           yes
   Link up:            yes
   DHCP running:       no
   IP address:         10.10.10.10
   Netmask:            255.255.255.0
   IPv6 enabled:       no
```

```
   Speed:              N/A
   Duplex:             N/A
   Interface type:     ethernet
   Interface source:   vlan
   MTU:                1500
   HW address:         00:02:C9:7E:24:E8

   RX bytes:           0                   TX bytes:       250
   RX packets:         0                   TX packets:     3
   RX mcast packets:   0                   TX discards:    0
   RX discards:        0                   TX errors:      0
   RX errors:          0                   TX overruns:    0
   RX overruns:        0                   TX carrier:     0
   RX frame:           0                   TX collisions:  0
                                           TX queue len:   0
switch (config) #
```

4.1.6 Commands

4.1.6.1 Interface

This chapter describes the commands should be used to configure and monitor the management interface.

interface

interface {mgmt0 | mgmt1 | lo | vlan<id>}

Enters a management interface context.

Syntax Description	mgmt0	Management port 0 (out of band).
	mgmt1	Management port 1 (out of band).
	lo	Loopback interface.
	vlan<id>	In-band management interface (e.g. vlan10).
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # interface mgmt0` `switch (config interface mgmt0) #`	
Related Commands	show interfaces <ifname>	
Note		

interface vlan create

interface vlan <id> create
no interface vlan <id> create

Creates an in-band management interface.
The no form of the command deletes the in-band management interface.

Syntax Description	id	VLAN ID. Range is 1-4094.
Default	N/A	
Configuration Mode	Config	
History	3.3.3500	
Role	admin	
Example	`switch (config) # interface vlan 10 create` `switch (config) #`	
Related Commands	interface show interfaces <ifname>	
Note	• This command does not requires any license • If IP Proxy-ARP or IP Routing is enabled, the interface cannot be created • No more than 60 in-band management interfaces can be created • All management interface commands are applicable under this interface (ip address, mtu, dhcp, shutdown, zeroconf …) • To enter the interface VLAN configuration mode you need to use the command “interface vlan<id>” (e.g. interface vlan10)	

ip address

ip address <IP address> <netmask>
no ip address

Sets the IP address and netmask of this interface.
The no form of the command clears the IP address and netmask of this interface.

Syntax Description	IP address	IPv4 address
	netmask	Subnet mask of IP address
Default	0.0.0.0/0	
Configuration Mode	Config Interface Management	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # interface mgmt0
switch (config interface mgmt0) # ip address 10.10.10.10 255.255.255.0
switch (config interface mgmt0) # show interfaces mgmt0
Interface mgmt0 state
   Admin up:           yes
   Link up:            yes
   IP address:         10.10.10.10
   Netmask:            255.255.255.0
   IPv6 enabled:       yes
   Autoconf enabled:   no
   Autoconf route:     yes
   Autoconf privacy:   no
   IPv6 addresses:     1
   IPv6 address:       fe80:202:c9ff:fe5e:a5d8/64
   Speed:              1000Mb/s (auto)
   Duplex:             full (auto)
   Interface type:     ethernet
   Interface ifindex:  2
   Interface source:   physical
   MTU:                1500
   HW address:         00:02:C9:5E:A5:D8
   Comment:

   RX bytes:          2946769856          TX bytes:       467577486
   RX packets:        44866091            TX packets:     1385520
   RX mcast packets:  0                   TX discards:    0
   RX discards:       0                   TX errors:      0
   RX errors:         0                   TX overruns:    0
   RX overruns:       0                   TX carrier:     0
   RX frame:          0                   TX collisions:  0
                                          TX queue len:   1000
switch (config interface mgmt0) #
```

Related Commands	show interfaces <ifname>
Note	If DHCP is enabled on the specified interface, then the DHCP IP assignment will hold until DHCP is disabled.

alias

alias <index> ip address < IP address> <netmask>
no alias <index>

Adds an additional IP address to the specified interface. The secondary address will appear in the output of “show interface” under the data of the primary interface along with the alias.
The no form of the command removes the secondary address to the specified interface.

Syntax Description	index	A number that is to be aliased to (associated with) the secondary IP.
	IP address	Additional IP address.
	netmask	Subnet mask of the IP address.

Default	N/A
Configuration Mode	Config Interface Management
History	3.1.0000
Role	admin

Example

```
switch (config interface mgmt0) # alias 2 ip address 9.9.9.9
255.255.255.255
switch (config interface mgmt0) # show interfaces mgmt0
Interface mgmt0 state
   Admin up:           yes
   Link up:            yes
   IP address:         172.30.2.2
   Netmask:            255.255.0.0
   Secondary address:  9.9.9.9/32 (alias: 'mgmt0:2')
   IPv6 enabled:       yes
   Autoconf enabled:   no
   Autoconf route:     yes
   Autoconf privacy:   no
   IPv6 addresses:     1
   IPv6 address:       fe80::202:c9ff:fe5e:a5d8/64
   Speed:              1000Mb/s (auto)
   Duplex:             full (auto)
   Interface type:     ethernet
   Interface ifindex:  2
   Interface source:   physical
   MTU:                1500
   HW address:         00:02:C9:5E:A5:D8
   Comment:

   RX bytes:          2970074221          TX bytes:       468579522
   RX packets:        44983023            TX packets:     1390539
   RX mcast packets:  0                   TX discards:    0
   RX discards:       0                   TX errors:      0
   RX errors:         0                   TX overruns:    0
   RX overruns:       0                   TX carrier:     0
   RX frame:          0                   TX collisions:  0
                                          TX queue len:   1000
switch (config interface mgmt0) #
```

Related Commands	show interfaces <ifname>
Note	• If DHCP is enabled on the specified interface, then the DHCP IP assignment will hold until DHCP is disabled • More than one additional IP address can be added to the interface

mtu

mtu <bytes>
no mtu <bytes>

Sets the Maximum Transmission Unit (MTU) of this interface.
The no form of the command resets the MTU to its default.

Syntax Description	bytes The entry range is 68-1500.
Default	1500
Configuration Mode	Config Interface Management
History	3.1.0000
Role	admin
Example	

```
switch (config interface mgmt0) # mtu 1500
switch (config interface mgmt0) # show interfaces mgmt0
Interface mgmt0 state
   Admin up:           yes
   Link up:            yes
   IP address:         172.30.2.2
   Netmask:            255.255.0.0
   Secondary address:  9.9.9.9/32 (alias: 'mgmt0:2')
   IPv6 enabled:       yes
   Autoconf enabled:   no
   Autoconf route:     yes
   Autoconf privacy:   no
   IPv6 addresses:     1
   IPv6 address:       fe80:202:c9ff:fe5e:a5d8/64
   Speed:              1000Mb/s (auto)
   Duplex:             full (auto)
   Interface type:     ethernet
   Interface ifindex:  2
   Interface source:   physical
   MTU:                1500
   HW address:         00:02:C9:5E:A5:D8
   Comment:

   RX bytes:          2970074221          TX bytes:       468579522
   RX packets:        44983023            TX packets:     1390539
   RX mcast packets:  0                   TX discards:    0
   RX discards:       0                   TX errors:      0
   RX errors:         0                   TX overruns:    0
   RX overruns:       0                   TX carrier:     0
   RX frame:          0                   TX collisions:  0
                                          TX queue len:   1000
switch (config interface mgmt0) #
```

Related Commands	show interfaces <ifname>
Note	

duplex

duplex <duplex>
no duplex

Sets the interface duplex.
The no form of the command resets the duplex setting for this interface to its default value.

Syntax Description	duplex	Sets the duplex mode of the interface. The following are the possible values: • half - half duplex • full - full duplex • auto - auto duplex sensing (half or full)

Default	auto
Configuration Mode	Config Interface Management
History	3.1.0000
Role	admin

Example

```
switch (config interface mgmt0) # duplex auto
switch (config interface mgmt0) # show interfaces mgmt0
Interface mgmt0 state
   Admin up:           yes
   Link up:            yes
   IP address:         172.30.2.2
   Netmask:            255.255.0.0
   Secondary address:  9.9.9.9/32 (alias: 'mgmt0:2')
   IPv6 enabled:       yes
   Autoconf enabled:   no
   Autoconf route:     yes
   Autoconf privacy:   no
   IPv6 addresses:     1
   IPv6 address:       fe80::202:c9ff:fe5e:a5d8/64
   Speed:              1000Mb/s (auto)
   Duplex:             full (auto)
   Interface type:     ethernet
   Interface ifindex:  2
   Interface source:   physical
   MTU:                1500
   HW address:         00:02:C9:5E:A5:D8
   Comment:

   RX bytes:          2970074221          TX bytes:       468579522
   RX packets:        44983023            TX packets:     1390539
   RX mcast packets:  0                   TX discards:    0
   RX discards:       0                   TX errors:      0
   RX errors:         0                   TX overruns:    0
   RX overruns:       0                   TX carrier:     0
   RX frame:          0                   TX collisions:  0
                                          TX queue len:   1000
switch (config interface mgmt0) #
```

Related Commands	show interfaces <ifname>
Note	• Setting the duplex to “auto” also sets the speed to “auto” • Setting the duplex to one of the settings “half” or “full” also sets the speed to a manual setting which is determined by querying the interface to find out its current auto-detected state

speed

speed <speed>
no speed

Sets the interface speed.
The no form of the command resets the speed setting for this interface to its default value.

Syntax Description	speed	Sets the speed of the interface. The following are the possible values: • 10 - fixed to 10Mbps • 100 - fixed to 1000Mbps • 1000 - fixed to 1000Mbps • auto - auto speed sensing (10/100/1000Mbps)

Default	auto
Configuration Mode	Config Interface Management
History	3.1.0000
Role	admin

Example

```
switch (config interface mgmt0) # speed auto
switch (config interface mgmt0) # show interfaces mgmt0
Interface mgmt0 state
   Admin up:           yes
   Link up:            yes
   IP address:         172.30.2.2
   Netmask:            255.255.0.0
   Secondary address:  9.9.9.9/32 (alias: 'mgmt0:2')
   IPv6 enabled:       yes
   Autoconf enabled:   no
   Autoconf route:     yes
   Autoconf privacy:   no
   IPv6 addresses:     1
   IPv6 address:       fe80::202:c9ff:fe5e:a5d8/64
   Speed:              1000Mb/s (auto)
   Duplex:             full (auto)
   Interface type:     ethernet
   Interface ifindex:  2
   Interface source:   physical
   MTU:                1500
   HW address:         00:02:C9:5E:A5:D8
   Comment:

   RX bytes:          2970074221          TX bytes:       468579522
   RX packets:        44983023            TX packets:     1390539
   RX mcast packets:  0                   TX discards:    0
   RX discards:       0                   TX errors:      0
   RX errors:         0                   TX overruns:    0
   RX overruns:       0                   TX carrier:     0
   RX frame:          0                   TX collisions:  0
                                          TX queue len:   1000
switch (config interface mgmt0) #
```

Related Commands	show interfaces <ifname>
Note	• Setting the speed to “auto” also sets the duplex to “auto” • Setting the speed to one of the manual settings (generally “10”, “100”, or “1000”) also sets the duplex to a manual setting which is determined by querying the interface to find out its current auto-detected state

dhcp

dhcp [renew]
no dhcp

Enables DHCP on the specified interface.
The no form of the command disables DHCP on the specified interface.

Syntax Description	renew	Forces a renewal of the IP address. A restart on the DHCP client for the specified interface will be issued.
Default	Could be enabled or disabled (per part number) manufactured with 3.2.0500	
Configuration Mode	Config Interface Management	
History	3.1.0000	
Role	admin	

Example

```
switch (config interface mgmt0) # dhcp
switch (config) # show interfaces mgmt0 configured
Interface mgmt0 configuration
   Enabled:          yes
   DHCP:             yes
   Zeroconf:         no
   IP address:
   Netmask:
   IPv6 enabled:     yes
   Autoconf enabled: no
   Autoconf route:   yes
   Autoconf privacy: no
   IPv6 addresses:   0
   Speed:            auto
   Duplex:           auto
   MTU:              1500
   Comment:
```

Related Commands show interfaces <ifname> configured

Note

- When enabling DHCP, the IP address and netmask are received via DHCP hence, the static IP address configuration is ignored
- Enabling DHCP disables zeroconf and vice versa
- Setting a static IP address and netmask does not disable DHCP. DHCP is disabled by using the “no” form of this command, or by enabling zeroconf.

shutdown

shutdown
no shutdown

Disables the specified interface.
The no form of the command enables the specified interface.

Syntax Description	N/A
Default	no shutdown
Configuration Mode	Config Interface Management
History	3.1.0000
Role	admin

Example	`switch (config interface mgmt0) # no shutdown`
	`switch (config) # show interfaces mgmt0 configured`
	`Interface mgmt0 configuration`
	`Enabled: yes`
	`DHCP: yes`
	`Zeroconf: no`
	`IP address:`
	`Netmask:`
	`IPv6 enabled: yes`
	`Autoconf enabled: no`
	`Autoconf route: yes`
	`Autoconf privacy: no`
	`IPv6 addresses: 0`
	`Speed: auto`
	`Duplex: auto`
	`MTU: 1500`
	`Comment:`
	`switch (config) #`

Related Commands	show interfaces <ifname> configured
Note	

zeroconf

zeroconf
no zeroconf

Enables zeroconf on the specified interface. It randomly chooses a unique link-local IPv4 address from the 169.254.0.0/16 block. This command is an alternative to DHCP.
The no form of the command disables the use of zeroconf on the specified interface.

Syntax Description	N/A
Default	no zeroconf
Configuration Mode	Config Interface Management
History	3.1.0000
Role	admin

Example	`switch (config interface mgmt0) # zeroconf`
	`switch (config) # show interfaces mgmt0 configured`
	`Interface mgmt0 configuration`
	`Enabled: yes`
	`DHCP: no`
	`Zeroconf: yes`
	`IP address:`
	`Netmask:`
	`IPv6 enabled: yes`
	`Autoconf enabled: no`
	`Autoconf route: yes`
	`Autoconf privacy: no`
	`IPv6 addresses: 0`
	`Speed: auto`
	`Duplex: auto`
	`MTU: 1500`
	`Comment:`

Related Commands	show interfaces <ifname> configured
Note	Enabling zeroconf disables DHCP and vice versa.

comment

comment <comment>
no comment

Adds a comment for an interface.
The no form of the command removes a comment for an interface.

Syntax Description	comment	A free-form string that has no semantics other than being displayed when the interface records are listed.
Default	no comment	
Configuration Mode	Config Interface Management	
History	3.1.0000	
Role	admin	

Example

```
switch (config interface mgmt0) # comment my-interface
switch (config interface mgmt0) # show interfaces mgmt0
Interface mgmt0 state
   Admin up:           yes
   Link up:            yes
   IP address:         172.30.2.2
   Netmask:            255.255.0.0
   IPv6 enabled:       yes
   Autoconf enabled:   no
   Autoconf route:     yes
   Autoconf privacy:   no
   IPv6 addresses:     1
   IPv6 address:       fe80::202:c9ff:fe5e:a5d8/64
   Speed:              1000Mb/s (auto)
   Duplex:             full (auto)
   Interface type:     ethernet
   Interface ifindex:  2
   Interface source:   physical
   MTU:                1500
   HW address:         00:02:C9:5E:A5:D8
   Comment:            my-interface

   RX bytes:          962067812          TX bytes:       40658219
   RX packets:        3738865            TX packets:     142345
   RX mcast packets:  0                  TX discards:    0
   RX discards:       0                  TX errors:      0
   RX errors:         0                  TX overruns:    0
   RX overruns:       0                  TX carrier:     0
   RX frame:          0                  TX collisions:  0
                                         TX queue len:   1000
switch (config interface mgmt0) #
```

Related Commands	N/A
Note	

ipv6 address

ipv6 address {<IPv6 address/netmask> | autoconfig [default | privacy]}
no ipv6 {<IPv6 address/netmask> | autoconfig [default | privacy]}

Configures IPv6 address and netmask to this interface, static or autoconfig options are possible.
The no form of the command removes the given IPv6 address and netmask or disables the autoconfig options.

Syntax Description	IPv6 address/netmask	Configures a static IPv6 address and netmask. Format example: 2001:db8:1234::5678/64.
	autoconfig	Enables IPv6 stateless address auto configuration (SLAAC) for this interface. An address will be automatically added to the interface based on an IPv6 prefix learned from router advertisements, combined with an interface identifier.
	autoconfig default	Enables default learning routes. The default route will be discovered automatically, if the autoconfig is enabled.
	autoconfig privacy	Uses privacy extensions for SLAAC to construct the autoconfig address, if the autoconfig is enabled.
Default	No IP address available, auto config is enabled	
Configuration Mode	Config Interface Management	
History	3.1.0000	
Role	admin	

Example

```
switch (config interface mgmt0) # ipv6 fe80::202:c9ff:fe5e:a5d8/64
switch (config interface mgmt0) # show interfaces mgmt0
Interface mgmt0 state
   Admin up:           yes
   Link up:            yes
   IP address:         172.30.2.2
   Netmask:            255.255.0.0
   IPv6 enabled:       yes
   Autoconf enabled:   no
   Autoconf route:     yes
   Autoconf privacy:   no
   IPv6 addresses:     1
   IPv6 address:       fe80::202:c9ff:fe5e:a5d8/64
   Speed:              1000Mb/s (auto)
   Duplex:             full (auto)
   Interface type:     ethernet
   Interface ifindex:  2
   Interface source:   physical
   MTU:                1500
   HW address:         00:02:C9:5E:A5:D8
   Comment:            my-interface

   RX bytes:           962067812           TX bytes:       40658219
   RX packets:         3738865             TX packets:     142345
   RX mcast packets:   0                   TX discards:    0
   RX discards:        0                   TX errors:      0
   RX errors:          0                   TX overruns:    0
   RX overruns:        0                   TX carrier:     0
   RX frame:           0                   TX collisions:  0
                                           TX queue len:   1000
switch (config interface mgmt0) #
```

Related Commands

ipv6 enable
show interface <ifname>

Note

- Unlike IPv4, IPv6 can have multiple IPv6 addresses on a given interface
- For Ethernet, the default interface identifier is a 64-bit long modified EUI-64, which is based on the MAC address of the interface

show interface

show interface {<ifname> [configured | brief]}

Displays information about the specified interface, configuration status, and counters.

Syntax Description	ifname	The interface name e.g., “mgmt0”, “mgmt1”, “lo” (loopback), etc.
	configured	Displays the interface configuration.
	brief	Displays a brief info on the interface configuration and status.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example

```
switch (config) #show interfaces mgmt0 configured
Interface mgmt0 configuration
   Enabled:          yes
   DHCP:             yes
   Zeroconf:         no
   IP address:
   Netmask:
   IPv6 enabled:     yes
   Autoconf enabled: no
   Autoconf route:   yes
   Autoconf privacy: no
   IPv6 addresses:   0
   Speed:            auto
   Duplex:           auto
   MTU:              1500
   Comment:          my-interface
switch (config) # show interfaces mgmt0 brief
Interface mgmt0 state
   Admin up:           yes
   Link up:            yes
   IP address:         172.30.2.2
   Netmask:            255.255.0.0
   IPv6 enabled:       yes
   Autoconf enabled:   no
   Autoconf route:     yes
   Autoconf privacy:   no
   IPv6 addresses:     1
   IPv6 address:       fe80::202:c9ff:fe5e:a5d8/64
   Speed:              1000Mb/s (auto)
   Duplex:             full (auto)
   Interface type:     ethernet
   Interface ifindex:  2
   Interface source:   physical
   MTU:                1500
   HW address:         00:02:C9:5E:A5:D8
   Comment:            my-interface
switch (config) #
```

Related Commands	N/A
Note	

4.1.6.2 Hostname Resolution

hostname

hostname <hostname>
no hostname

Sets a static system hostname.
The no form of the command clears the system hostname.

Syntax Description	hostname	A free-form string.
Default	Default hostname	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # hostname my-switch-hostname` `my-switch-hostname (config) #`	
Related Commands	show hosts	
Note	• Hostname may contain letters, numbers, and hyphens ('-'), in any combination • Hostname may not contain other letters, such as '%', '_', '.'etc • Hostname may not begin with a hyphen • Hostname may be 1-63 characters long • Changing hostname stamps a new HTTPS certificate	

ip name-server

ip name-server <IPv4/IPv6 address>
no name-server <IPv4/IPv6 address>

Sets the static name server.
The no form of the command clears the name server.

Syntax Description	IPv4/v6 address	IPv4 or IPv6 address.
Default	No server name	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ip name-server 9.9.9.9`
	`switch (config) # show hosts`
	`Hostname: switch`
	`Name server: 9.9.9.9 (configured)`
	`Name server: 10.211.0.121 (dynamic)`
	`Name server: 172.30.0.126 (dynamic)`
	`Name server: 10.4.0.135 (dynamic)`
	`Domain name: lab.mtl.com (dynamic)`
	`Domain name: vmlab.mtl.com (dynamic)`
	`Domain name: yok.mtl.com (dynamic)`
	`Domain name: mtl.com (dynamic)`
	`IP 127.0.0.1 maps to hostname localhost`
	`IPv6 ::1 maps to hostname localhost6`
	`Automatically map hostname to loopback address: yes`
	`Automatically map hostname to IPv6 loopback address: no`
	`switch (config) #`	

Related Commands	show hosts	
Note		

ip domain-list

ip domain-list <domain-name>
no ip domain-list <domain-name>

Sets the static domain name.
The no form of the command clears the domain name.

Syntax Description	domain-name	The domain name in a string form. A domain name is an identification string that defines a realm of administrative autonomy, authority, or control in the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS).
Default	No static domain name	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ip domain-list mydomain.com`
	`switch (config) # show hosts`
	`Hostname: switch`
	`Name server: 10.211.0.121 (dynamic)`
	`Name server: 172.30.0.126 (dynamic)`
	`Name server: 10.4.0.135 (dynamic)`
	`Domain name: mydomain.com (configured)`
	`Domain name: lab.mtl.com (dynamic)`
	`Domain name: vmlab.mtl.com (dynamic)`
	`Domain name: yok.mtl.com (dynamic)`
	`Domain name: mtl.com (dynamic)`
	`IP 1.1.1.1 maps to hostname p`
	`IP 127.0.0.1 maps to hostname localhost`
	`IPv6 ::1 maps to hostname localhost6`
	`Automatically map hostname to loopback address: yes`
	`Automatically map hostname to IPv6 loopback address: no`
	`switch (config) #`	

Related Commands	show hosts	
Note		

ip/ipv6 host

{ip | ipv6} host <hostname> <IP Address>
no {ip | ipv6} host <hostname> <IP Address>

Configures the static hostname IPv4 or IPv6 address mappings.
The no form of the command clears the static mapping.

Syntax Description	hostname	The hostname in a string form.
	IP Address	The IPv4 or IPv6 address.
Default	No static domain name.	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ip host my-host 2.2.2.2`
	`switch (config) # ipv6 host my-ipv6-host  2001::8f9`
	`switch (config) # show hosts`
	`Hostname: switch`
	`Name server: 9.9.9.9 (configured)`
	`Name server: 10.211.0.121 (dynamic)`
	`Name server: 172.30.0.126 (dynamic)`
	`Name server: 10.4.0.135 (dynamic)`
	`Domain name: mydomain.com (configured)`
	`Domain name: lab.mtl.com (dynamic)`
	`Domain name: vmlab.mtl.com (dynamic)`
	`Domain name: yok.mtl.com (dynamic)`
	`Domain name: mtl.com (dynamic)`
	`IP 1.1.1.1 maps to hostname p`
	`IP 127.0.0.1 maps to hostname localhost`
	`IP 2.2.2.2 maps to hostname my-host`
	`IPv6 2001::8f9 maps to hostname my-ipv6-host`
	`IPv6 ::1 maps to hostname localhost6`
	`Automatically map hostname to loopback address: yes`
	`Automatically map hostname to IPv6 loopback address: yes`
	`switch (config) #`	

Related Commands	show hosts	
Note		

ip/ipv6 map-hostname

{ip |ipv6} map-hostname
no {ip | ipv6} map-hostname

Maps between the currently-configured hostname and the loopback address 127.0.0.1.
The no form of the command clears the mapping.

Syntax Description	N/A
Default	IPv4 mapping is enabled by default IPv6 mapping is disabled by default
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # ip map-hostname`
	`switch (config) # # show hosts`
	`Hostname: switch`
	`Name server: 9.9.9.9 (configured)`
	`Name server: 10.211.0.121 (dynamic)`
	`Name server: 172.30.0.126 (dynamic)`
	`Name server: 10.4.0.135 (dynamic)`
	`Domain name: mydomain.com (configured)`
	`Domain name: lab.mtl.com (dynamic)`
	`Domain name: vmlab.mtl.com (dynamic)`
	`Domain name: yok.mtl.com (dynamic)`
	`Domain name: mtl.com (dynamic)`
	`IP 1.1.1.1 maps to hostname p`
	`IP 127.0.0.1 maps to hostname localhost`
	`IP 2.2.2.2 maps to hostname my-host`
	`IPv6 2001::8f9 maps to hostname my-ipv6-host`
	`IPv6 ::1 maps to hostname localhost6`
	`Automatically map hostname to loopback address: yes`
	`Automatically map hostname to IPv6 loopback address: yes`
	`switch (config) #`
	`switch (config) # ping my-host-name`
	`PING localhost (127.0.0.1) 56(84) bytes of data.`
	`64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.078 ms`
	`64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.052 ms`
	`64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.058 ms`

Related Commands	show hosts
Note	• If no mapping is configured, a mapping between the hostname and the IPv4 loopback address 127.0.0.1 will be added • The no form of the command maps the hostname to the IPv6 loopback address if there is no statically configured mapping from the hostname to an IPv6 address (disabled by default) • Static host mappings are preferred over DNS results. As a result, with this option set, you will not be able to look up your hostname on your configured DNS server; but without it set, some problems may arise if your hostname cannot be looked up in DNS.

show hosts

show hosts

Displays hostname, DNS configuration, and static host mappings.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show hosts`
	`Hostname: my-host-name`
	`Name server: 9.9.9.9 (configured)`
	`Name server: 10.211.0.121 (dynamic)`
	`Name server: 172.30.0.126 (dynamic)`
	`Name server: 10.4.0.135 (dynamic)`
	`Domain name: mydomain.com (configured)`
	`Domain name: lab.mtl.com (dynamic)`
	`Domain name: vmlab.mtl.com (dynamic)`
	`Domain name: yok.mtl.com (dynamic)`
	`Domain name: mtl.com (dynamic)`
	`IP 1.1.1.1 maps to hostname p`
	`IP 127.0.0.1 maps to hostname localhost`
	`IP 2.2.2.2 maps to hostname my-host`
	`IPv6 ::1 maps to hostname localhost6`
	`Automatically map hostname to loopback address: yes`
	`Automatically map hostname to IPv6 loopback address: no`
	`switch (config) #`

Related Commands	N/A
Note	

4.1.6.3 Routing

ip/ipv6 route

{ip | ipv6} route <network-prefix> <netmask> {<nexthop-address> | <ifname>}
no ip route <network-prefix> <netmask> {<nexthop-address> | <ifname>}

Sets a static route for a given IP.
The no form of the command deletes the static route.

Syntax Description	network-prefix	IPv4 or IPv6 network prefix.
	netmask	IPv4 netmask formats are: • /24 • 255.255.255.0 IPv6 netmask format is: • /48 (as a part of the network prefix)
	nexthop-address	The IPv4 or IPv6 address of the next hop router for this route.
	ifname	The interface name (e.g., mgmt0, mgmt1).
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ip route 20.20.20.0 255.255.255.0 mgmt0` `switch (config) # show ip route`	

```
Destination       Mask             Gateway          Interface   Source
default           0.0.0.0          172.30.0.1       mgmt0       DHCP
10.10.10.10       255.255.255.255  0.0.0.0          mgmt0       static
20.10.10.10       255.255.255.255  172.30.0.1       mgmt0       static
20.20.20.0        255.255.255.0    0.0.0.0          mgmt0       static
172.30.0.0        255.255.0.0      0.0.0.0          mgmt0       interface
```

Related Commands	show ip route
Note	

ipv6 default-gateway

ipv6 default-gateway {<ip-address> | <ifname>}
no ipv6 default-gateway

Sets a static default gateway.
The no form of the command deletes the default gateway.

Syntax Description	ip address	The default gateway IP address (IPv4 or IPv6).
	ifname	The interface name (e.g., mgmt0, mgmt1).
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	First version
	3.2.0500	removed IPv4 configuration option
Role	admin	

Example	`switch (config) # ip default-gateway ::1`
	`switch (config) # show ip default-gateway static`
	`Configured default gateways:`
	`  ::1`
	`switch (config) #`	

Related Commands	show ip route	
Note	• The configured default gateway will not be used if DHCP is enabled. • In order to configure ipv4 default-gateway use ‘ip route’ command.	

show ip/ipv6 route

show {ip | ipv6} route [static]

Displays the routing table in the system.

Syntax Description	static	Filters the table with the static route entries.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show ip route`
	`Destination Mask Gateway Interface Source`
	`default 0.0.0.0 172.30.0.1 mgmt0 DHCP`
	`10.10.10.10 255.255.255.255 0.0.0.0 mgmt0 static`
	`20.10.10.10 255.255.255.255 172.30.0.1 mgmt0 static`
	`20.20.20.0 255.255.255.0 0.0.0.0 mgmt0 static`
	`172.30.0.0 255.255.0.0 0.0.0.0 mgmt0 interface`
	`switch (config) # show ipv6 route`
	`Destination prefix`
	`Gateway Interface Source`
	`----------`
	`::/0`
	`:: mgmt0 static`
	`::1/128`
	`:: lo local`
	`2222:2222:2222::/64`
	`:: mgmt1 interface`
	`switch (config) #`	

Related Commands	show ip default-gateway	
Note		

show ip/ipv6 default-gateway

show {ip | ipv6} default-gateway [static]

Displays the default gateway.

Syntax Description	static	Displays the static configuration of the default gateway.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ip default-gateway 10.10.10.10`
	`switch (config) # show ip default-gateway`
	`Active default gateways:`
	`   172.30.0.1 (interface: mgmt0)`
	`switch (config) # show ip default-gateway static`
	`Configured default gateway: 10.10.10.10`	

Related Commands	show ip default-gateway	
Note	The configured IPv4 default gateway will not be used if DHCP is enabled.	

4.1.6.4 Network to Media Resolution (ARP & NDP)

IPv4 network use Address Resolution Protocol (ARP) to resolve IP address to MAC address, while IPv6 network uses Network Discovery Protocol (NDP) that performs basically the same as ARP.

ip arp

ip arp <IP address> <MAC address>
no ip arp <IP address> <MAC address>

Sets a static ARP entry.
The no form of the command deletes the static ARP.

Syntax Description	IP address	IPv4 address.
	MAC address	MAC address.
Default	N/A	
Configuration Mode	Config Interface Management	
History	3.2.0500	
Role	admin	

Example	`switch (config interface mgmt0) #ip arp 20.20.20.20 aa:aa:aa:aa:aa:aa`
	`switch (config interface mgmt0) # show ip arp`
	`ARP Timeout: 1500`
	
	`Total number of entries: 6`
	
	`Address Type MAC Address Interface`
	`10.209.1.103 Dynamic 00:02:C9:11:A1:78 mgmt0`
	`10.209.1.168 Dynamic 00:02:C9:5E:C3:28 mgmt0`
	`10.209.1.104 Dynamic 00:02:C9:11:A1:E6 mgmt0`
	`10.209.1.153 Dynamic 00:02:C9:11:A1:86 mgmt0`
	`10.209.1.105 Dynamic 00:02:C9:5E:0B:56 mgmt0`
	`10.209.0.1 Dynamic 00:00:5E:00:01:01 mgmt0`
	`20.20.20.20 Static AA:AA:AA:AA:AA:AA mgmt0`
	
	`switch (config interface mgmt0) #`	

Related Commands	show ip arp ip route	
Note		

ip arp timeout

ip arp timeout <timeout-value>
no ip arp timeout

Sets the dynamic ARP cache timeout.
The no form of the command sets the timeout to default.

Syntax Description	timeout-value	Time (in seconds) that an entry remains in the ARP cache. Valid values are from 240 to 28800.
Default	1500 seconds	
Configuration Mode	Config	
History	3.2.0230	
Role	admin	

Example	`switch (config) # ip arp timeout 2000`
	`switch (config) # show ip arp`
	
	`ARP Timeout: 2000`
	
	`Total number of entries: 55`
	`IP Address  MAC Address  Interface`
	`1.0.0.2  00:02:c9:5c:30:40  Vlan11`
	`1.0.0.3  00:11:22:33:44:55  Vlan11`
	`2.0.0.2  00:02:c9:5c:30:40  Vlan12`
	`3.0.0.2  00:02:c9:5c:30:40  Vlan13`
	`4.0.0.2  00:02:c9:5c:30:40  Vlan14`
	`switch (config) #`	

Related Commands	ip arp show ip arp	
Note	This value is used as the ARP timeout whenever a new IP interface is created.	

show ip arp

show ip arp [interface <type>| <ip-address> | count]

Displays ARP table.

Syntax Description	interface type	Filters the table according to a specific interface (i.e. mgmt0)
	ip-address	Filters the table to the specific ip-address
	count	Shows ARP statistics
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.3000	
Role	admin	
Example		

```
switch-626a54 [standalone: master] (config) # show ip arp

Total number of entries: 3

  Address             Type           Hardware Address         Interface
  ------------------------------------------------------------------------
---
  10.209.0.1           Dynamic ETH     00:00:5E:00:01:01         mgmt0
  10.209.1.120         Dynamic ETH     00:02:C9:62:E8:C2         mgmt0
  10.209.1.121         Dynamic ETH     00:02:C9:62:E7:42         mgmt0
switch (config) # show ip arp count
ARP Table size: 3 (inband: 0, out of band: 3)
switch (config) #
```

Related Commands	
Note	

ipv6 neighbor

ipv6 neighbor <IPv6 address> <ifname> <MAC address>
no ipv6 neighbor <IPv6 address> <ifname> <MAC address>

Adds a static neighbor entry.
The no form of the command deletes the static entry.

Syntax Description	IPv6 address	The IPv6 address.
	ifname	The management interface (i.e. mgmt0, mgmt1).
	MAC address	The MAC address.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ipv6 neighbor 2001:db8:701f::8f9 mgmt0 00:11:22:33:44:55` `switch (config) #`	
Related Commands	show ipv6 neighbor ipv6 route arp clear ipv6 neighbors	
Note	• ARP is used only with IPv4. In IPv6 networks, Neighbor Discovery Protocol (NDP) is used similarly. • Use The no form of the command to remove static entries. Dynamic entries can be cleared via the “clear ipv6 neighbors” command.	

clear ipv6 neighbors

clear ipv6 neighbors

Clears the dynamic neighbors cache.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	`switch (config) # clear ipv6 neighbors` `switch (config) #`
Related Commands	ipv6 neighbor show ipv6 neighbor arp
Note	• Clearing Neighbor Discovery Protocol (NDP) cache removes only the dynamic entries learned and not the static entries configured • Use the no form of the ipv6 neighbor command to remove static entries

show ipv6 neighbors

show ipv6 neighbors [static]

Displays the Neighbor Discovery Protocol (NDP) table.

Syntax Description	static	Filters only the table of the static entries.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show ipv6 neighbors`
	`IPv6 Address Age MAC Address State Interf`
	`---`
	`2001::2 9428 AA:AA:AA:AA:AA:AA permanent mgmt0`
	`switch (config) #`	

Related Commands	ipv6 neighbor clear ipv6 neighbor show ipv6	
Note		

4.1.6.5 DHCP

ip dhcp

ip dhcp {default-gateway yield-to-static| hostname <hostname>| primary-intf <ifname> | send-hostname }
no ip dhcp {default-gateway yield-to-static| hostname | | primary-intf | send-hostname}

Sets global DHCP configuration.
The no form of the command deletes the DHCP configuration.

Syntax Description	yield-to-static|	Does not allow you to install a default gateway from DHCP if there is already a statically configured one.
	hostname	Specifies the hostname to be sent during DHCP client negotiation if send-hostname is enabled.
	primary-intf <ifname>	Sets the interface from which a non-interface-specific configuration (resolver and routes) will be accepted via DHCP.
	send-hostname	Enables the DHCP client to send a hostname during negotiation.
Default	no ip dhcp yield-to-static no ip dhcp hostname ip ip dhcp primary-intf mgmt0 no ip dhcp send-hostname	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ip dhcp default-gateway yield-to-static`
	`switch (config) # show ip dhcp`
	`DHCP primary interface:`
	`  Configured: mgmt0`
	`  Active:  mgmt0`
	
	`DHCP: yield default gateway to static configuration: yes`
	
	`DHCP Client Options:`
	`  Send Hostname:  no`
	`  Client Hostname:  switch (using system hostname)`
	`switch (config) #`	

Related Commands	show ip dhcp dhcp [renew]	
Note	DHCP is supported for IPv4 networks only.	

show ip dhcp

show ip dhcp

Displays the DHCP configuration and status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show ip dhcp`
	`DHCP primary interface:`
	`  Configured: mgmt0`
	`  Active:  mgmt0`
	
	`DHCP: yield default gateway to static configuration: yes`
	
	`DHCP Client Options:`
	`  Send Hostname:  no`
	`  Client Hostname:  switch (using system hostname)`
	`switch (config) #`

Related Commands	ip dhcp dhcp [renew]
Note	

4.1.6.6 IP Diagnostic Tools

ping

ping [-LRUbdfnqrvVaA] [-c count] [-i interval] [-w deadline] [-p pattern] [-s packetsize] [-t ttl] [-I interface or address] [-M mtu discovery hint] [-S sndbuf] [-T timestamp option] [-Q tos] [hop1 ...] destination

Sends ICMP echo requests to a specified host.

Syntax Description	Linux Ping options	http://linux.about.com/od/commands/l/blcmdl8_ping.htm
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ping 172.30.2.2`
	`PING 172.30.2.2 (172.30.2.2) 56(84) bytes of data.`
	`64 bytes from 172.30.2.2: icmp_seq=1 ttl=64 time=0.703 ms`
	`64 bytes from 172.30.2.2: icmp_seq=2 ttl=64 time=0.187 ms`
	`64 bytes from 172.30.2.2: icmp_seq=3 ttl=64 time=0.166 ms`
	`64 bytes from 172.30.2.2: icmp_seq=4 ttl=64 time=0.161 ms`
	`64 bytes from 172.30.2.2: icmp_seq=5 ttl=64 time=0.153 ms`
	`64 bytes from 172.30.2.2: icmp_seq=6 ttl=64 time=0.144 ms`
	`^C`
	`--- 172.30.2.2 ping statistics ---`
	`6 packets transmitted, 6 received, 0% packet loss, time 5004ms`
	`rtt min/avg/max/mdev = 0.144/0.252/0.703/0.202 ms`
	`switch (config) #`	

Related Commands	traceroutes	
Note		

traceroute

traceroute [-46dFITUnrAV] [-f first_ttl] [-g gate,...] [-i device] [-m max_ttl] [-N squeries] [-p port] [-t tos] [-l flow_label] [-w waittime] [-q nqueries] [-s src_addr] [-z sendwait] host [packetlen]

Traces the route packets take to a destination.

Syntax Description	-4	Uses IPv4.
	-6	Uses IPv6.
	-d	Enables socket level debugging.
	-F	Sets DF (do not fragment bit) on.
	-I	Uses ICMP ECHO for tracerouting.
	-T	Uses TCP SYN for tracerouting.
	-U	Uses UDP datagram (default) for tracerouting.
	-n	Does not resolve IP addresses to their domain names.
	-r	Bypasses the normal routing and send directly to a host on an attached network.
	-A	Performs AS path lookups in routing registries and print results directly after the corresponding addresses.
	-V	Prints version info and exit.
	-f	Starts from the first_ttl hop (instead from 1).
	-g	Routes packets throw the specified gateway (maximum 8 for IPv4 and 127 for IPv6).
	-i	Specifies a network interface to operate with.
	-m	Sets the max number of hops (max TTL to be reached). Default is 30.
	-N	Sets the number of probes to be tried simultaneously (default is 16).
	-p	Uses destination port. It is an initial value for the UDP destination port (incremented by each probe, default is 33434), for the ICMP seq number (incremented as well, default from 1), and the constant destination port for TCP tries (default is 80).
	-t	Sets the TOS (IPv4 type of service) or TC (IPv6 traffic class) value for outgoing packets.
	-l	Uses specified flow_label for IPv6 packets.
	-w	Sets the number of seconds to wait for response to a probe (default is 5.0). Non-integer (float point) values allowed too.
	-q	Sets the number of probes per each hop. Default is 3.
	-s	Uses source src_addr for outgoing packets.
	-z	Sets minimal time interval between probes (default is 0). If the value is more than 10, then it specifies a number in milliseconds, else it is a number of seconds (float point values allowed too).

Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # traceroute 192.168.10.70`
	`traceroute to 192.168.10.70 (192.168.10.70), 30 hops max, 40 byte pack-ets`
	`1 172.30.0.1 (172.30.0.1) 3.632 ms 2.849 ms 3.544 ms`
	`2 10.222.128.46 (10.222.128.46) 3.176 ms 3.289 ms 3.656 ms`
	`3 10.158.128.30 (10.158.128.30) 15.331 ms 15.819 ms 16.388 ms`
	`4 10.158.128.65 (10.158.128.65) 20.468 ms 7.893 ms 12.27 ms`
	`5 10.7.34.115 (10.7.34.115) 16.405 ms 11.985 ms 12.264 ms`
	`6 192.168.10.70 (192.168.10.70) 16.377 ms 16.091 ms 20.475 ms`
	`switch (config) #`

Related Commands	
Note	

tcpdump

tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [-C file_size]
[-E algo:secret] [-F file] [-i interface] [-M secret]
[-r file] [-s snaplen] [-T type] [-w file]
[-W filecount] [-y datalinktype] [-Z user]
[expression]

Invokes standard binary, passing command line parameters straight through. Runs in foreground, printing packets as they arrive, until the user hits Ctrl+C.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # tcpdump`
	`......`
	`09:37:38.678812 IP 192.168.10.7.ssh > 192.168.10.1.54155: P`
	`1494624:1494800(176) ack 625 win 90`
	`<nop,nop,timestamp 5842763 858672398>`
	`09:37:38.678860 IP 192.168.10.7.ssh > 192.168.10.1.54155: P`
	`1494800:1495104(304) ack 625 win 90`
	`<nop,nop,timestamp 5842763 858672398>`
	`...`
	`9141 packets captured`
	`9142 packets received by filter`
	`0 packets dropped by kernel`
	`switch (config) #`

Related Commands	N/A
Note	

4.2 NTP, Clock & Time Zones

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC) and is designed to mitigate the effects of variable network latency. NTP can usually maintain time to within tens of milliseconds over the public Internet, and can achieve better than one millisecond accuracy in local area networks under ideal conditions.

4.2.1 Commands

clock set

clock set <hh:mm:ss> [<yyyy/mm/dd>]

Sets the time and date.

Syntax Description	hh:mm:ss	Time.
	yyyy/mm/dd	Date.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # clock set 23:23:23 2010/08/19`
	`switch (config) # show clock`
	`Time:  23:23:26`
	`Date:  2010/08/19`
	`Time zone:  UTC`
	`(Etc/UTC)`
	`UTC offset: same as UTC`
	`switch (config) #`	

Related Commands	show clock	
Note	If not specified, the date will be left the same.	

clock timezone

clock timezone [<zone word> [<zone word> [<zone word>] [<zone word>]]]

Sets the system time zone. The time zone may be specified in one of three ways:

- A nearby city whose time zone rules to follow. The system has a large list of cities which can be displayed by the help and completion system. They are organized hierarchically because there are too many of them to display in a flat list. A given city may be required to be specified in two, three, or four words, depending on the city.
- An offset from UTC. This will be in the form UTC-offset UTC, UTC-offset UTC+<0-14>, UTC-offset UTC-<1-12>.
- UTC (Universal Time, which is almost identical to GMT), and this is the default time zone

The no form of the command resets time zone to its default (GMT).

Syntax Description	zone word	The possible forms this could take include: continent, city, continent, country, city, continent, region, country, city, ocean, and/or island.
Default	GMT	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # clock timezone America North United_States Other New_York`
	`switch (config) # show clock`
	`Time: 04:21:44`
	`Date: 2012/02/26`
	`Time zone: America North United_States Other New_York`
	`switch (config) #`	

Related Commands	show clock	
Note		

ntp

ntp {disable | enable | {peer | server} <IP address> [version <number> | disable]}
no ntp {disable | enable | {peer | server} <IP address> [disable]}

Configures NTP.
The no form of the command negates NTP options.

Syntax Description	disable	Disables NTP.
	enable	Enables NTP.
	peer or server	Configures an NTP peer or server node.
	IP address	IPv4 or IPv6 address.
	version <number>	Specifies the NTP version number of this peer. Possible values are 3 or 4.
Default	NTP is enabled. NTP version number is 4.	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # no ntp peer 192.168.10.24 disable` `switch (config) #`	
Related Commands	N/A	
Note		

ntpdate

ntpdate <IP address>

Sets the system clock using the specified SNTP server.

Syntax Description	IP address IP.
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # ntpdate 192.168.10.10`
	`26 Feb 17:25:40 ntpdate[15206]: adjust time server 192.168.10.10 offset -0.000092 sec`
	`switch (config) #`

Related Commands	N/A
Note	This is a one-time operation and does not cause the clock to be kept in sync on an ongoing basis. It will generate an error if SNTP is enabled since the socket it requires will already be in use.

show clock

show clock

Displays the current system time, date and time zone.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # show clock`
	`Time: 04:21:44‘`
	`Date: 2012/02/26`
	`Time zone: America North United_States Other New_York`
	`switch (config) #`

Related Commands	N/A
Note	

show ntp

show ntp

Displays the current NTP settings.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # show ntp`
	`NTP is enabled.`
	`Clock is unsynchronized.`
	`No NTP peers or servers configured.`
	`switch (config) #`

Related Commands	N/A
Note	

-

4.3 Software Management

4.3.1 Upgrading MLNX-OS Software – Preconditions

Prior to upgrading MLNX-OS software from version 3.2.0100 and lower, please remove any old configuration from your system.

To remove old configuration:

Step 1. Clear your system of any old configuration. Run from CMM:

```
system:switch[2]> clear -cnfg
OK
system:switch[2]>
```

Step 2. Follow the steps described in Section 4.3.2, “Upgrading MLNX-OS Software,” on page 130.

4.3.2 Upgrading MLNX-OS Software

When upgrading from a software version older than 3.2.0100 to software version 3.3.0000 or higher, the upgrade procedure must be done in two steps. First update the software to 3.2.0300-100 (for InfiniBand platforms) or 3.2.0506 (for Ethernet platforms), then update to the desired software version.

The system being upgraded becomes indisposed throughout the upgrade procedure.

The upgrade procedure burns the software image as well as the firmware should there be a need.

You have to read and accept the End-User License Agreement (EULA) after image upgrade in case the EULA is modified. The EULA link is only available upon first login to CLI.

To upgrade MLNX-OS software on your system, perform the following steps:

Step 1. Change to Config mode.

```
switch > enable
switch # configure terminal
switch (config) #
```

Step 2. Obtain the previously available image (.img file). You *must* delete this image in the next step to make room for fetching the new image.

```
switch (config) # show images
Installed images:

  Partition 1:
  SX_PPC_M460EX SX_3.3.3130 2013-03-20 21:32:25 ppc
```

```
  Partition 2:
  SX_PPC_M460EX SX_3.3.3130 2013-03-20 21:32:25 ppc

Images available to be installed:

  image-PPC_M460EX-SX_3.3.3256.img
  SX_PPC_M460EX SX_3.3.3256 2013-03-20 21:32:25 ppc

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

No image install currently in progress.

Require trusted signature in image being installed: yes (default)
switch (config) #
```

Step 3. Delete the old image (if one exists) that is listed under `Images available to be installed` prior to fetching the new image. Use the command `image delete` for this purpose.

```
switch (config) # image delete image-PPC_M460EX-SX_3.0.1224.img
switch (config) #
```

When deleting an image, you delete the file but not the partition. This is recommended so as to not overload system resources.

Step 4. Fetch the new software image.

```
switch (config) # image fetch scp://username:password@192.168.10.125/var/www/html/
<image_name>
Password (if required): ****** 100.0%[##################################################
###############]
switch (config) #
```

Step 5. Display the available images.

To recover from image corruption (e.g., due to power interruption), there are two installed images on the system. See the commands:

`image boot next`

`image boot location`.

```
switch (config) # show images
Installed images:
  Partition 1:
  SX <old ver> 2013-04-28 16:02:50
```

```
  Partition 2:
  SX <new ver> 2013-04-28 16:52:50

Images available to be installed:
  new_image.img
  SX <new ver> 2013-04-28 16:52:50

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

No image install currently in progress.

Require trusted signature in image being installed: yes (default)
switch (config) #
```

Step 6. Install the new image.

```
switch (config) # image install <image_name>
Step 1 of 4: Verify Image
 100.0%  [##################################################################]
Step 2 of 4: Uncompress Image
 100.0%  [##################################################################]
Step 3 of 4: Create Filesystems
 100.0%  [##################################################################]
Step 4 of 4: Extract Image
 100.0%  [##################################################################]
switch (config) #
```

CPU utilization may go up to 100% during image upgrade.

Step 7. Have the new image activate during the next boot. Run:

```
switch (config) # image boot next
```

Step 8. Run `show images` to review your images. Run:

```
switch (config) # show images
Images available to be installed:
  new_image.img
  SX <new ver> 2011-04-28 16:52:50

Installed images:
  Partition 1:
  SX <old ver> 2011-04-28 16:02:50
```

```
  Partition 2:
  SX <new ver> 2011-04-28 16:52:50

Last boot partition: 1
Next boot partition: 2

No boot manager password is set.
switch (config) #
```

Step 9. Save current configuration. Run:

```
switch (config) # configuration write
switch (config)#
```

Step 10. Reboot the switch to run the new image. Run:

```
switch (config) # reload
Configuration has been modified; save first? [yes] yes
Configuration changes saved.
Rebooting...
switch (config)#
```

After software reboot, the software upgrade will also automatically upgrade the firmware version.

In order to upgrade the system on dual management system refer to Section 4.3.2, “Upgrading MLNX-OS Software,” on page 130.

When performing upgrade from the WebUI, make sure that the image you are trying to upgrade to is not located already in the system (i.e. fetched from the CLI).

4.3.3 Deleting Unused Images

➢ ***To delete unused images:***

Step 1. Enter Config mode. Run:

```
switch >
switch > enable
switch # configure terminal
```

Step 2. Get a list of the unused images. Run

```
switch (config) # show images
Images available to be installed:
  image-PPC_M460EX-SX_3.1.1224.img
  SX-OS_PPC_M460EX SX_3.1.1224 2011-04-28 12:29:48 ppc
Installed images:
```

```
Partition 1:
SX-OS_PPC_M460EX 3.1.0000-dev-HA 2011-04-10 12:02:49 ppc
Partition 2:
SX-OS_PPC_M460EX 3.1.0000-dev-HA 2011-04-10 12:02:49 ppc

Last boot partition: 1
Next boot partition: 1
Boot manager password is set.
No image install currently in progress.
Require trusted signature in image being installed: yes
switch (config) #
```

Step 3. Delete the unused images. Run:

```
switch config) # image delete image-PPC_M460EX-SX_3.0.1224.img
switch (config) #
```

When deleting an image, you delete the file but not the partition. This is recommended so as to not overload system resources.

4.3.4 Downgrading MLNX-OS Software

Prior to downgrading software, please make sure the following prerequisites are met:

Step 1. Log into your switch via the CLI using the console port.

Step 2. Backup your configuration according to the following steps:

1. Change to Config mode. Run:

```
switch-112094 [standalone: master] > enable
switch-112094 [standalone: master] # configure terminal
switch-112094 [standalone: master] (config) #
```

2. Disable paging of CLI output. Run:

```
switch-112094 [standalone: master] (config) # no cli default paging enable
```

3. Display commands to recreate current running configuration. Run:

```
switch-112094 [standalone: master] (config) # show running-config
```

4. Copy the output to a text file.

4.3.4.1 Downloading Image

Step 1. Log into the system to obtain the serial number. Run:

```
switch-112094 [standalone: master] (config) # show inventory
```

Step 2. Download the requested MLNX-OS version from the following link:

http://support.mellanox.com/SupportWeb/

Step 3. Enter your username and password when prompted.

Step 4. Log into the switch via the CLI using the console port.

Step 5. Change to Config mode. Run:

```
switch > enable
switch # configure terminal
switch (config) #
```

Step 6. Delete all previous images from the `Images available to be installed` prior to fetching the new image. Run:

```
switch (config) # image delete image-EFM_PPC_M405EX-ppc-m405ex 20090531-190132.img
```

Step 7. Fetch the requested software image. Run:

```
switch (config) # image fetch scp://username:password@192.168.10.125/var/www/html/
<image_name>
100.0%[################################################## ###############]
```

4.3.4.2 Downgrading Image

The procedure below assumes that booting and running is done from Partition 1 and the downgrade procedure is performed on Partition 2.

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Show all image files on the system. Run:

```
switch (config) # show images
Images available to be installed:
new_image.img
<downgrade version> 2010-09-19 16:52:50
Installed images:
Partition 1:
<current version> 2010-09-19 03:46:25
Partition 2:
<current version> 2010-09-19 03:46:25
Last boot partition: 1
Next boot partition: 1
No boot manager password is set.
switch (config) #
```

Step 4. Install the MLNX-OS image. Run:

```
switch (config) # image install <image_name>
Step 1 of 4: Verify Image
100.0% [####################################################################]
Step 2 of 4: Uncompress Image
100.0% [####################################################################]
Step 3 of 4: Create Filesystems
100.0% [####################################################################]
```

```
Step 4 of 4: Extract Image
100.0% [########################################################################]
switch (config) #
```

Step 5. Show all image files on the system. Run:

```
switch (config) # show images
Images available to be installed:
new_image.img
 <downgrade version> 2010-09-19 16:52:50
Installed images:
Partition 1:
 <current version> 2010-09-19 03:46:25
Partition 2:
 <downgrade version> 2010-09-19 16:52:50
Last boot partition: 1
Next boot partition: 2
No boot manager password is set.
switch (config) #
```

Step 6. Set the boot location to be the other partition (next). Run:

```
switch (config) # image boot next
```

There are two installed images on the system. Therefore, if one of the images gets corrupted (due to power interruption, for example), in the next reboot the image will go up from the second partition.

In case you are downloading to an older software version which has never been run yet on the switch, use the following command sequence as well:

switch (config) # no boot next fallback-reboot enable

switch (config) # configuration write

Step 7. Reload the switch. Run:

```
switch (config) # reload
```

4.3.4.3 Switching to Partition with Older Software Version

The system saves a backup configuration file when upgrading from an older software version to a newer one. If the system returns to the older software partition, it uses this backup configuration file. Note that all configuration changes done with the new software are lost when returning to the older software version.

There are 2 instances where the backup configuration file does not exist:

- The user has run “reset factory” command, which clears all configuration files in the system
- The user has run “configuration switch-to” to a configuration file with different name then the backup file

Also note that the configuration file becomes empty if the switch is downgraded to a software version which has never been installed yet.

To allow switching partition to the older software version, in these cases above, follow the steps below:

Step 1. Run the command:

```
switch (config)# no boot next fallback-reboot enable
```

Step 2. Set the boot partition. Run:

```
switch (config)# image boot next
```

Step 3. Save the configuration. Run:

```
switch (config)# configuration write
```

Step 4. Reload the system. Run:

```
switch (config)# reload
```

4.3.5 Upgrading System Firmware

Each MLNX-OS software package version has a default switch firmware version. When you update the MLNX-OS software to a new version, an automatic firmware update process will be attempted by MLNX-OS. This process is described below.

4.3.5.1 After Updating MLNX-OS Software

Upon rebooting your switch system after updating the MLNX-OS software, MLNX-OS compares its default firmware version with the currently programmed firmware versions on all the switch modules (leafs and spines on director-class switches, or simply the switch card on edge switch systems).

If one or more of the switch modules is programmed with a firmware version other than the default version, then MLNX-OS automatically attempts to burn the default firmware version instead.

If a firmware update takes place, then the login process is delayed a few minutes.

To verify that the firmware update was successful, log into MLNX-OS and run the command “show asic-version” (can be run in any mode). This command lists all of the switch modules along with their firmware versions. Make sure that all the firmware versions are the same and match the default firmware version. If the firmware update failed for one or more modules, then the following warning is displayed.

Some subsystems are not updated with a default firmware.

If you detect a mismatch in firmware version for one or more modules of the switch system, please contact your assigned Mellanox Technologies field application engineer.

4.3.5.2 Importing Firmware and Changing the Default Firmware

To perform an automatic firmware update by MLNX-OS for a different switch firmware version without changing the MLNX-OS version, import the firmware package as described below. MLNX-OS sets it as the new default firmware and performs the firmware update automatically as described in the previous subsections.

Default Firmware Change on Standalone Systems

Step 1. Import the firmware image (.mfa file). Run:

```
switch (config) # image fetch image fetch scp://root@1.1.1.1:/tmp/fw-SX-rel-9_2_6440-
FIT.tgz
Password (if required): *******
100.0% [#################################################################################]
switch (config) # image default-chip-fw fw-SX-rel-9_2_6440-FIT.mfa
Installing default firmware image. Please wait...
Default Firmware 9.2.6440 updated. Please save configuration and reboot for new FW to
take effect.
switch (config) #
```

Step 2. Save the configuration. Run:

```
switch (config) # configuration write
switch (config) #
```

Step 3. Reboot the system to enable auto update.

Step 4.

4.3.6 Commands

This chapter displays all the relevant commands used to manage the system software image.

image boot

image boot {location <location ID> | next}

Specifies the default location where the system should be booted from.

Syntax Description	location ID	Specifies the default destination location. There can be up to 2 images on the system. The possible values are 1 or 2.
	next	Sets the boot location to be the next once after the one currently booted from, thus avoiding a cycle through all the available locations.
Default	N/A	
Configuration Mode	enable/config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # image boot location 2` `switch (config) #`	
Related Commands	show images	
Note		

boot next

boot next fallback-reboot enable
no boot next fallback-reboot enable

Sets the default setting for next boot. Normally, if the system fails to apply the configuration on startup (after attempting upgrades or downgrades, as appropriate), it will reboot to the other partition as a fallback.
The no form of the command tells the system not to do that, only for the next boot.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.2.0506
Role	admin
Example	`switch (config) # boot fallback-reboot enable` `switch (config) #`
Related Commands	show images
Note	• Normally, if the system fails to apply the configuration on startup (after attempting upgrades or downgrades, as appropriate) it reboots to the other partition as a fallback. • The no form of this command tells the system not to do that **only** for the next boot. In other words, this setting is not persistent, and goes back to enabled automatically after each boot. • When downgrading to an older software version which has never been run yet on a system, the “fallback reboot” **always** happens, unless the command “no boot next fallback-reboot enable” is used. However, this also happens when the older software version *has* been run before, but the configuration file has been switched since upgrading. In general, a downgrade only works (without having the fallback reboot forcibly disabled) if the process can find a snapshot of the configuration file (by the same name as the currently active one) which was taken before upgrading from the older software version. If that is not found, a fallback reboot is performed in preference to falling back to the initial database because the latter generally involves a loss of network connectivity, and avoiding that is of paramount importance.

image default-chip-fw

image default-chip-fw <file name>

Sets the default firmware package to be installed.

Syntax Description	filename	Specifies the firmware filename.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # image default-chip-fw image-SX_PPC_M460EX-ppc-m460ex-20120122-084759.img` `switch (config) #`	
Related Commands	image install-chip fw show images	
Note		

image delete

image delete <image name>

Deletes the specified image file.

Syntax Description	image name	Specifies the image name.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # image delete image-MLXNX-OS-201140526-010145.img` `switch (config) #`	
Related Commands	show images	
Note		

image fetch

image fetch <URL> [<filename>]

Downloads an image from the specified URL or via SCP.

Syntax Description	URL	HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username[:password]@hostname/path/filename.
	filename	Specifies a filename for this image to be stored as locally.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # image fetch scp://<username>@192.168.10.125/var/www/html/<image_name>`
	`Password  ******`
	`100.0%[##################################################################]`
	`switch (config) #`	

Related Commands	show images	
Note	• Please delete the previously available image, prior to fetching the new image • See section “Upgrading MLNX-OS SX Software,” in the *Mellanox SwitchX® User Manual* for a full upgrade example	

image install

image install <image filename> [location <location ID>] | [progress <prog-options>] [verify <ver-options>]

Installs the specified image file.

Syntax Description	image filename	Specifies the image name.
	location ID	Specifies the image destination location.
	prog-options	• "no-track" overrides CLI default and does not track the installation progress • "track" overrides CLI default and tracks the installation progress
	ver-options	• "check-sig" requires an image to have either a valid signature or no signature • "ignore-sig" allows unsigned or invalidly signed images to be installed • "require-sig" requires from the installed image to have a valid signature. If a valid signature is not found on the image, the image cannot be installed.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # image install SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-22 08:47:59 ppc`
	`Step 1 of 4: Verify Image`
	`100.0%`
	`[####################################################################]`
	`Step 2 of 4: Uncompress Image`
	`100.0%`
	`[####################################################################]`
	`Step 3 of 4: Create Filesystems`
	`100.0%`
	`[####################################################################]`
	`Step 4 of 4: Extract Image`
	`100.0%`
	`[####################################################################]`
	`switch (config) #`	

Related Commands	show images	
Note	• The image cannot be installed on the "active" location (the one which is currently being booted) • On a two-location system, the location is chosen automatically if no location is specified	

image move

image move <src image name> <dest image name>

Renames the specified image file.

Syntax Description	src image name	Specifies the old image name.
	dest image name	Specifies the new image name.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # image move image1.img image2.img` `switch (config) #`	
Related Commands	show images	
Note		

image options

image options require-sig
no image options require-sig

Requires from all the installed images a valid signature.
The no form of the command does not require a signature. However if one is present, it must be valid.

Syntax Description	require-sig	Requires images to be signed by a trusted signature.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # image options require-sig` `switch (config) #`	
Related Commands	show images	
Note		

show bootvar

show bootvar

Displays the installed system images and the boot parameters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # show bootvar`
	`Installed images:`
	`  Partition 1:`
	`  SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-22 08:47:59 ppc`
	`  Last dobincp: 2012/01/23 14:54:23`
	
	`  Partition 2:`
	`  SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-18 09:52:41 ppc`
	`  Last dobincp: 2012/01/19 16:48:23`
	
	`Last boot partition: 1`
	`Next boot partition: 1`
	
	`Boot manager password is set.`
	
	`No image install currently in progress.`
	
	`Image signing: trusted signature always required`
	`Admin require signed images: yes`
	
	`Settings for next boot only:`
	`   Fallback reboot on configuration failure: yes (default)`
	`switch (config) #`

Related Commands	N/A
Note	

show images

show image

Displays information about the system images and boot parameters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show images`
	`Images available to be installed:`
	`  image-SX_PPC_M460EX-ppc-m460ex-20120122-084759.img`
	`  SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-22 08:47:59 ppc`
	
	`Installed images:`
	`  Partition 1:`
	`  SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-22 08:47:59 ppc`
	`  Last dobincp: 2012/01/23 14:54:23`
	
	`  Partition 2:`
	`  SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-18 09:52:41 ppc`
	`  Last dobincp: 2012/01/19 16:48:23`
	
	`Last boot partition: 1`
	`Next boot partition: 1`
	
	`Boot manager password is set.`
	
	`No image install currently in progress.`
	
	`Image signing: trusted signature always required`
	`Admin require signed images: yes`
	
	`Settings for next boot only:`
	`   Fallback reboot on configuration failure: yes (default)`
	`switch (config) #`

Related Commands	N/A
Note	

4.4 Configuration Management

4.4.1 Saving a Configuration File

To save the current configuration to the active configuration file, you can either use the `configuration write` command (requires running in Config mode) or the `write memory` command (requires running in Enable mode).

- To save the configuration to the active configuration file, run:

```
switch (config) # configuration write
```

- To save the configuration to a user-specified file without making the new file the active configuration file, run:

```
switch (config) # configuration write to myconf no-switch
```

- To save the configuration to a user-specified file and make the new file the active configuration file, run:

```
switch (config) # configuration write to myconf
```

- To display the available configuration files and the active file, run:

```
switch (config) # show configuration files
initial
myconf (active)
switch (config) #
```

4.4.2 Loading a Configuration File

By default, or after a system reset, the system loads the default “initial” configuration file.

➢ ***To load a different configuration file and make it the active configuration:***

```
switch [standalone: master] >
switch [standalone: master] > enable
switch [standalone: master] # configure terminal
switch [standalone: master] (config) # configuration switch-to myconfig
switch [standalone: master] (config) #
```

4.4.3 Managing Configuration Files

There are two types of configuration files that can be applied on the switch, BIN files (binary) and text-based configuration files.

4.4.3.1 BIN Configuration Files

BIN configuration files are not human readable and cannot be edited.

➢ ***To create a new BIN configuration file***

```
switch (config) # configuration new my-filename
```

➢ ***To upload a BIN configuration file from a switch to an external file server***

```
switch (config) # configuration upload my-filename scp://root@my-server/root/tmp/my-filename
```

- ***To fetch a BIN configuration file***

```
switch (config) # configuration fetch scp://root@my-server/root/tmp/my-filename
```

- ***To see the available configuration files***

```
switch (config) # show configuration files
initial (active)
my-filename

Active configuration: initial
Unsaved changes:      no
switch (config) #
```

- ***To load a BIN configuration file:***

```
switch (config) # configuration switch-to my-filename
```

Applying a new BIN configuration file changes the whole switch's configuration and requires system reboot which can be preformed using the command `reload`.

4.4.3.2 Text Configuration Files

Text configuration files are text based and editable.

- ***To create a new text-based configuration file***:

```
switch (config) # configuration text generate active running save my-filename
```

- ***To apply a text-based configuration file:***

```
switch (config) # configuration text file my-filename apply
```

Applying a text-based configuration file to an existing/running data port configuration may result in unpredictable behavior. It is therefore suggested to first clear the switch's configuration by applying a specific configuration file (following the procedure in Section 4.4.3.1) or by resetting the switch back to factory default.

- ***To upload a text-based configuration file from a switch to an external file server***

```
switch (config) # configuration text file my-filename upload scp://root@my-server/root/
tmp/my-filename
```

- ***To fetch a text-based configuration file from an external file server to a switch***

```
switch (config) # configuration text fetch scp://root@my-server/root/tmp/my-filename
```

- ***To apply a text-based configuration file:***

```
switch (config) # configuration text file my-filename apply
```

When applying a text-based configuration file, the configuration is appended to the switch's existing configuration. Reboot is not required.

4.4.4 Commands

4.4.4.1 File System

debug generate dump

debug generate dump

Generates a debug dump.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # debug generate dump`
	`Generated dump sysdump-switch-112104-201140526-091707.tgz`
	`switch (config) #`

Related Commands	file debug-dump
Note	The dump can then be manipulated using the “file debug-dump...” commands.

file debug-dump

file debug-dump {delete {<filename> | latest} | email {<filename> | latest} | upload {{<filename> | latest} <URL>}}

Manipulates debug dump files.

Syntax Description	delete {<filename> | latest}	Deletes a debug dump file.
	email {<filename> | latest}	Emails a debug dump file to pre-configured recipients for “informational events”, regardless of whether they have requested to receive “detailed” notifications or not.
	upload {{<filename> | latest} <URL>}}	Uploads a debug dump file to a remote host. The URL to the remote host: HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username[:password]@hostname/path/filename.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	Initial release
	3.3.4000	Added “latest” parameter
Role	admin	
Example	`switch (config) # file debug-dump email sysdump-switch-112104-20114052-091707.tgz` `switch (config) #`	
Related Commands	show files debug-dump	
Note		

file stats

file stats {delete <filename> | move {<source filename> | <destination filename>} | upload <filename> <URL>}

Manipulates statistics report files.

Syntax Description	delete <filename>	Deletes a stats report file.
	move <source filename> <destination filename>	Renames a stats report file.
	upload <filename> <URL>	Uploads a stats report file. URL - HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username[:password]@host-name/path/filename.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # file stats move memory-1.csv memory-2.csv` `switch (config) #`	
Related Commands	show files stats show files stats <filename>	
Note		

file tcpdump

file tcpdump {delete <filename> | upload <filename> <URL>}

Manipulates tcpdump output files.

Syntax Description	delete <filename>	Deletes the specified tcpdump output file.
	upload <filename> <URL>	Uploads the specified tcpdump output file to the specified URL. URL - HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username[:password]@hostname/path/filename.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # file tcmpdump delete my-tcpdump-file.txt` `switch (config) #`	
Related Commands	show files stats tcpdump	
Note		

reload

reload [force | halt [noconfirm] | noconfirm]

Reboots or shuts down the system.

Syntax Description	force	Forces an immediate reboot of the system even if the system is busy.
	halt	Shuts down the system.
	noconfirm	Reboots the system without asking about unsaved changes.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # reload`
	`Configuration has been modified; save first? [yes] yes`
	`Configuration changes saved.`
	`...`
	`switch (config) #`	

Related Commands	reset factory	
Note		

show files debug-dump

show files debug-dump [<filename>]

Displays a list of debug dump files.

Syntax Description	filename	Displays a summary of the contents of a particular debug dump file.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show files debug-dump sysdump-switch-112104-20114052-091707.tgz`
	`System information:`
	
	`Hostname: switch-112104`
	`Version:  SX_PPC 3.1.0000 2011-05-25 13:59:00 ppc`
	`Date:     2012-01-26 09:17:07`
	`Uptime:   0d 18h 47m 48s`
	
	`================================================`
	`Output of 'uname -a':`
	
	`Linux switch-112104 2.6.27-MELLANOXuni-m405ex SX_PPC 3.1.0000 #1 2012-01-25 13:59:00 ppc ppc`
	`ppc GNU/Linux`
	
	`================================================`
	
	`.....................................................`
	`switch (config) #`	

Related Commands	file debug-dump	
Note		

show files stats

show files stats <filename>

Displays a list of statistics report files.

Syntax Description	filename	Display the contents of a particular statistics report file.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show files stats`
	`memory-201140524-111745.csv`
	`switch (config) #`	

Related Commands	file stats	
Note		

show files system

show files system [detail]

Displays usage information of the file systems on the system.

Syntax Description	detail	Displays more detailed information on file-system.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show files system`
	`Statistics for /config filesystem:`
	`  Bytes Total  100 MB`
	`  Bytes Used  3 MB`
	`  Bytes Free  97 MB`
	`  Bytes Percent Free  97%`
	`  Bytes Available  97 MB`
	`  Inodes Total  0`
	`  Inodes Used  0`
	`  Inodes Free  0`
	`  Inodes Percent Free  0%`
	
	`Statistics for /var filesystem:`
	`  Bytes Total  860 MB`
	`  Bytes Used  209 MB`
	`  Bytes Free  651 MB`
	`  Bytes Percent Free  75%`
	`  Bytes Available  651 MB`
	`  Inodes Total  0`
	`  Inodes Used  0`
	`  Inodes Free  0`
	`  Inodes Percent Free  0%`
	`switch (config) #`	

Related Commands	N/A	
Note		

show files tcpdump

show files tcpdump

Displays a list of statistics report files.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # show files stats`
	`test`
	`dump3`
	`switch (config) #`

Related Commands	file tcpdump tcpdump
Note	

4.4.4.2 Configuration Files

configuration audit

configuration audit max-changes <number>

Chooses settings related to configuration change auditing.

Syntax Description	max-changes	Set maximum number of audit messages to log per change.
Default	1000	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # configuration audit max-changes 100`
	`switch (config) # show configuration audit`
	`Maximum number of changes to log: 100`
	`switch (config) #`	

Related Commands	show configuration	
Note	N/A	

configuration copy

configuration copy <source name> <dest name>

Copies a configuration file.

Syntax Description	source name	Name of source file.
	dest name	Name of destination file. If the file of specified file-name does not exist a new file will be created with said filename.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # configuration copy initial.bak example` `switch (config) #`	
Related Commands		
Note	• This command does not affect the current running configuration • The active configuration file may not be the target of a copy. However, it may be the source of a copy in which case the original remains active.	

configuration delete

configuration delete <filename>

Deletes a configuration file.

Syntax Description	filename	Name of file to delete.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show configuration files`
	`example  initial  initial.bak  initial.prev`
	`switch (config) # configuration delete example`
	`switch (config) # show configuration files`
	`initial  initial.bak  initial.prev`
	`switch (config) #`	

Related Commands	show configuration	
Note	• This command does not affect the current running configuration • The active configuration file may not be deleted	

configuration fetch

configuration fetch <URL> [<name>]

Downloads a configuration file from a remote host.

Syntax Description	URL	HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username[:password]@hostname/path/filename.
	name	The configuration file name.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # configuration fetch scp://root:password@ 192.168.10.125/tmp/conf1` `switch (config) #`	
Related Commands	configuration switch-to	
Note	• The downloaded file should not override the active configuration file, using the <name> parameter • If no name is specified for a configuration fetch, it is given the same name as it had on the server • No configuration file may have the name “active”	

configuration jump-start

configuration jump-start

Runs the initial-configuration wizard.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # configuration jump-start`
	`Mellanox configuration wizard`
	`Step 1: Hostname? [switch-3cc29c]`
	`Step 2: Use DHCP on mgmt0 interface? y`
	`Step 3: Admin password (Enter to leave unchanged)?`
	`You have entered the following information:`
	`1. Hostname: switch-3cc29c`
	`2. Use DHCP on mgmt0 interface: yes`
	`3. Enable IPv6: yes`
	`4. Enable IPv6 autoconfig (SLAAC) on mgmt0 interface: yes`
	`53. Admin password (Enter to leave unchanged): (unchanged)`
	`To change an answer, enter the step number to return to.`
	`Otherwise hit <enter> to save changes and exit.`
	`Choice:`
	`Configuration changes saved.`
	`switch (config) #`

Related Commands	N/A
Note	• The wizard is automatically invoked whenever the CLI is launched when the active configuration file is fresh (i.e. not modified from its initial contents) • This command invokes the wizard on demand – see chapter “Initializing the Switch for the First Time” in the Mellanox *MLNX-OS SwitchX User Manual*

configuration merge

configuration merge <filename>

Merges the “shared configuration” from one configuration file into the running configuration.

Syntax Description	filename	Name of file from which to merge settings.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # configuration merge new-config-file` `switch (config) #`	
Related Commands		
Note	• No configuration files are modified during this process • The configuration name must be a non-active configuration file	

configuration move

configuration move <source name> <dest name>

Moves a configuration file.

Syntax Description	source name	Old name of file to move.
	dest name	New name for moved file.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show configuration files`
	`example1 initial initial.bak initial.prev`
	`switch (config) # configuration move example1 example2`
	`switch (config) # show configuration files`
	`example2 initial initial.bak initial.prev`
	`switch (config) #`	

Related Commands	show configuration	
Note	• This command does not affect the current running configuration • The active configuration file may not be the target of a move	

configuration new

configuration new <filename> [factory [keep-basic] [keep-connect]]

Creates a new configuration file under the specified name. The parameters specify what configuration, if any, to carry forward from the current running configuration.

Syntax Description	filename	Names for new configuration file.
	factory	Creates new file with only factory defaults.
	keep-basic	Keeps licenses and host keys.
	keep-connect	Keeps configuration necessary for connectivity (interfaces, routes, and ARP).
Default	Keeps licenses and host keys	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show configuration files`
	`initial  initial.bak  initial.prev`
	`switch (config) # configuration new example2`
	`switch (config) # show configuration files`
	`example2  initial  initial.bak  initial.prev`
	`switch (config) #`	

Related Commands	show configuration	
Note		

configuration switch-to

configuration switch-to <filename>

Loads the configuration from the specified file and makes it the active configuration file.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # show configuration files`
	`initial (active)`
	`newcon`
	`initial.prev`
	`initial.bak`
	`switch (config) # configuration switch-to newcon`
	`switch (config) # show configuration files`
	`initial`
	`newcon (active)`
	`initial.prev`
	`initial.bak`
	`switch (config) #`

Related Commands	show configuration files
Note	The current running configuration is lost and not automatically saved to the previous active configuration file.

configuration text fetch

configuration text fetch <URL> [apply [discard | fail-continue | filename | overwrite | verbose] | filename <filename> | overwrite [apply | filename <filename>]]

Fetches a text configuration file (list of CLI commands) from a specified URL.

Syntax Description	apply	Applies the file to the running configuration (i.e. executes the commands in it). This option has the following parameters: • discard: Does not keep downloaded configuration text file after applying it to the system • fail-continue: If applying commands, continues execution even if one of them fails • overwrite: If saving the file and the filename already exists, replaces the old file • verbose: Displays all commands being executed and their output instead of just those that get errors
	filename	Specifies filename for saving downloaded text file.
	overwrite	Downloads the file and saves it using the same name it had on the server. This option has the following parameters: • apply: Applies the downloaded configuration to the running system • filename: Specifies filename for saving downloaded text file
Default	N/A	
Configuration Mode	Config	
History	3.2.1000	First version
	3.2.3000	Updated command
Role	admin	
Example	`switch (config) # configuration fetch text scp://username[:password]@hostname/path/filename`	
Related Commands	N/A	
Note		

configuration text file

configuration text file <filename> {apply [fail-continue] [verbose] | delete | rename <filename> | upload < URL>}

Performs operations on text-based configuration files.

Syntax Description	filename <file>	Specifies the filename.
	apply	Applies the configuration on the system.
	fail-continue	Continues execution of the commands even if some commands fail.
	verbose	Displays all commands being executed and their output, instead of just those that get errors.
	delete	Deletes the file.
	rename <filename>	Renames the file.
	upload <URL>	Supported types are HTTP, HTPPS, FTP, TFTP, SCP and SFTP. For example: scp://username[:password]@hostname/path/filename.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # configuration text file my-config-file delete` `switch (config) #`	
Related Commands	show configuration files	
Note		

configuration text generate

configuration text generate {active {running | saved} | file <filename> } {save <filename> | upload <URL>}

Generates a new text-based configuration file from this system's configuration.

Syntax Description	active	Generates from currently active configuration.
	running	Uses running configuration.
	saved	Uses saved configuration.
	file <filename>	Generates from inactive saved configuration.
	save	Saves new file to local persistent storage.
	upload <URL>	Supported types are HTTP, HTPPS, FTP, TFTP, SCP and SFTP. For example: scp://username[:password]@hostname/path/filename.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # configuration text generate file initial.prev save example`
	`switch (config) # show configuration files`
	`initial (active)`
	`initial.prev`
	`initial.bak`
	`Active configuration: initial`
	`Unsaved changes:  yes`
	`switch (config) #`	

Related Commands	show configuration files	
Note		

configuration upload

configuration upload {active | <name>} <URL or scp or sftp://username:password@hostname[:port]/path/filename>

Uploads a configuration file to a remote host.

Syntax Description	active	Upload the active configuration file.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # configuration upload active scp://root:password@192.168.10.125/tmp/conf1` `switch (config) #`	
Related Commands	N/A	
Note	No configuration file may have the name “active”.	

write

write {memory [local] | terminal}

Saves or displays the running configuration.

Syntax Description	memory	Saves running configuration to the active configuration file. It is the same as “configuration write”.
	local	Saves the running configuration only on the local node. It is the same as “configuration write local”.
	terminal	Displays commands to recreate current running configuration. It is the same as “show running-config”.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # write terminal`
	`##`
	`## Running database "initial"`
	`## Generated at 20114/05/27 10:05:16 +0000`
	`## Hostname: switch`
	`##`
	`##`
	`## Network interface configuration`
	`##`
	`interface mgmt0 comment ""`
	`interface mgmt0 create`
	`interface mgmt0 dhcp`
	`interface mgmt0 display`
	`interface mgmt0 duplex auto`
	`interface mgmt0 mtu 1500`
	`no interface mgmt0 shutdown`
	`interface mgmt0 speed auto`
	`no interface mgmt0 zeroconf`
	`##`
	`## Local user account configuration`
	`##`
	`username a** capability admin`
	`no username a** disable`
	`username a** disable password`
	`......`
	`switch (config) #`	

Related Commands	show running-config configuration write	
Note		

show configuration

show configuration [audit | files [<filename>] | running | text files]

Displays a list of CLI commands that will bring the state of a fresh system up to match the current persistent state of this system.

Syntax Description	audit	Displays settings for configuration change auditing.
	files [<filename>]	Displays a list of configuration files in persistent storage if no filename is specified. If a filename is specified, it displays the commands to recreate the configuration in that file. In the latter case, only non-default commands are shown, as for the normal “show configuration” command.
	running	Displays commands to recreate current running configuration. Same as “show configuration” except that it applies to the currently running configuration, rather than the current persisted configuration.
	text files	Displays names of available text-based configuration files.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5006	Removed “running full” and “full” parameters
Role	monitor/admin	
Example		
Related Commands		
Note		

```
switch (config) # show configuration
##
## Active saved database "newcon"
## Generated at 20114/05/25 10:18:52 +0000
## Hostname: switch-3cc29c
##
##
## Network interface configuration
##
interface mgmt0 comment ""
interface mgmt0 create
interface mgmt0 dhcp
interface mgmt0 display
interface mgmt0 duplex auto
interface mgmt0 mtu 1500
no interface mgmt0 shutdown
interface mgmt0 speed auto
no interface mgmt0 zeroconf
switch (config) #
```

show running-config

show running-config

Displays commands to recreate current running configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000 3.3.4402 Removed “full” parameter
Role	monitor/admin

Example	`switch (config) # show running-config`
	`##`
	`## Running database "initial"`
	`## Generated at 2012/02/28 14:59:02 +0000`
	`## Hostname: switch-5ea5d8`
	`##`
	
	`##`
	`## License keys`
	`##`
	`license install LK2-EFM_SX-5M11-5K11-5HGL-0KAL-64QK-8C2Q-60Q3-6C1G`
	
	`##`
	`## Network interface configuration`
	`##`
	`interface mgmt0 create`
	`interface mgmt0 comment ""`
	`interface mgmt0 dhcp`
	`interface mgmt0 display`
	`interface mgmt0 duplex auto`
	`interface mgmt0 mtu 1500`
	`no interface mgmt0 shutdown`
	`...`
	`switch (config) #`

Related Commands	
Note	

4.5 Logging

4.5.1 Monitor

➢ ***To print logging events to the terminal:***

Set the modules or events you wish to print to the terminal. For example, run:

```
switch (config) # logging monitor events notice
switch (config) # logging monitor sx-sdk warning
```

These commands print system events in severity “notice” and sx-sdk module notifications in severity “warning” to the screen. For example, in case of interface-down event, the following gets printed to the screen.

```
switch (config) #
Wed Jul 10 11:30:42 2013: Interface IB1/17 changed state to DOWN
Wed Jul 10 11:30:43 2013: Interface IB1/18 changed state to DOWN
switch (config) #
```

To see a list of the events, refer to Table 18, “Supported Event Notifications and MIB Mapping,” on page 210.

4.5.2 Remote Logging

➢ ***To configure remote syslog to send syslog messages to a remote syslog server:***

Step 1. Enter Config mode. Run:

```
switch >
switch > enable
switch # configure terminal
```

Step 2. Set remote syslog server. Run

```
switch (config) # logging <IP address>
```

Step 3. Set the minimum severity of the log level to `info`. Run:

```
switch (config) # logging <IP address> trap info
```

Step 4. Override the log levels on a per-class basis. Run:

```
switch (config) # logging <IP address> trap override class <class name>
```

4.5.3 Switch Power-On Self-Test

As the switch powers on, it begins the Power On Self-Test (POST), a series of tests as part of its power-up procedure to ensure that the switch functions properly. During the POST, the switch logs any errors encountered. Some POST errors are critical, others are not.

The updated POST diagnostic code gets stored inside the “POST Diagnostic Register”.

Table 17 lists the POST return codes and their meanings.

Table 17 - POST Return Codes

Return Code	Severity	Meaning	POST Section
0x5	Critical	System initialization failure.	Standard POST

Table 17 - POST Return Codes

Return Code	Severity	Meaning	POST Section
0x10	Critical	Failure connecting to the main management process.	Standard POST
0x15	Critical	VPD initialization failure.	Standard POST
0x20	Critical	CPLD initialization failure.	Standard POST
0x25	Critical	Default IP configuration failure.	Standard POST
0x30	Critical	Temperature sensors failure.	Extended POST
0x35	Critical	Voltage sensors failure.	Extended POST
0x40	Critical	RAM memory failure.	Full POST
0x45	Critical	NAND memory failure.	Full POST
0x80	Non-critical	Incorrect firmware version.	Standard POST
0xff	Non-critical	POST ended successfully	Standard POST

4.5.4 Commands

logging local override

logging local override [class <class> priority <log-level>]
no logging local override [class <class> priority <log-level>]

Enables class-specific overrides to the local log level.
The no form of the command disables all class-specific overrides to the local log level without deleting them from the configuration, but disables them so that the logging level for all classes is determined solely by the global setting.

Syntax Description	override	Enables class-specific overrides to the local log level.
	class	Sets or removes a per-class override on the logging level. All classes which do not have an override set will use the global logging level set with "logging local <log level>". Classes that do have an override will do as the override specifies. If "none" is specified for the log level, MLNX-OS will not log anything from this class. Classes available: • debug-module - debug module functionality • protocol-stack - protocol stack modules functionality • mgmt-back - system management back-end components • mgmt-core - system management core • mgmt-front - system management front-end components • mlx-daemons - management daemons • sx-sdk - switch SDK
	log-level	• alert - alert notification, action must be taken immediately • crit - critical condition • debug - debug level messages • emerg - system is unusable (emergency) • err - error condition • info - informational condition • none - disables the logging locally and remotely • notice - normal, but significant condition • warning - warning condition
Default	Override is disabled.	
Configuration Mode	Config	
History	3.1.0000	
	3.3.4150	Added debug-module class Changed iss-modules with protocol-stack
Role	admin	

Example	`switch (config) # logging local override class mgmt-front priority warning`
	`switch (config) # show logging`
	`Local logging level: info`
	`  Override for class mgmt-front: warning`
	`Default remote logging level: notice`
	`No remote syslog servers configured.`
	`Allow receiving of messages from remote hosts: no`
	`Number of archived log files to keep: 10`
	`Log rotation size threshold: 5.000% of partition (43 megabytes)`
	`Log format: standard`
	`Subsecond timestamp field: disabled`
	`Levels at which messages are logged:`
	`  CLI commands: notice`
	`  Audit messages: notice`
	`switch (config) #`

Related Commands	show logging logging local
Note	

logging <syslog IP address>

logging <syslog IP address> [trap {<log-level> | override class <class> priority <log-level>}]
no logging <syslog IP address> [trap {<log-level> | override class <class> priority <log-level>}]

Enables (by setting the IP address) sending logging messages, with ability to filter the logging messages according to their classes.
The no form of the command stops sending messages to the remote syslog server.

Syntax Description	syslog IP address	IPv4 address of the remote syslog server.
	log-level	• alert - alert notification, action must be taken immediately • crit - critical condition • debug - debug level messages • emerg - system is unusable (emergency) • err - error condition • info - informational condition • none - disables the logging locally and remotely • notice - normal, but significant condition • warning - warning condition
	class	Sets or removes a per-class override on the logging level. All classes which do not have an override set will use the global logging level set with “logging local <log level>”. Classes that do have an override will do as the override specifies. If “none” is specified for the log level, MLNX-OS will not log anything from this class. Classes available: • iss-modules - protocol stack • mgmt-back - system management back-end • mgmt-core - system management core • mgmt-front - system management front-end • mlx-daemons - management daemons • sx-sdk - switch SDK
	log-level	• alert - alert notification, action must be taken immediately • crit - critical condition • debug - debug level messages • emerg - system is unusable (emergency) • err - error condition • info - informational condition • none - disables the logging locally and remotely • notice - normal, but significant condition • warning - warning condition
Default	Remote logging is disabled	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # logging local info`
	`switch (config) # show logging`
	`Local logging level: info`
	`Default remote logging level: notice`
	`No remote syslog servers configured.`
	`Allow receiving of messages from remote hosts: no`
	`Number of archived log files to keep: 10`
	`Log rotation size threshold: 5.000% of partition (43 megabytes)`
	`Log format: standard`
	`Subsecond timestamp field: disabled`
	`Levels at which messages are logged:`
	`  CLI commands: notice`
	`  Audit messages: notice`
	`switch (config) #`

Related Commands	show logging logging local override
Note	

logging receive

logging receive
no logging receive

Enables receiving logging messages from a remote host.
The no form of the command disables the option of receiving logging messages from a remote host.

Syntax Description	N/A
Default	Receiving logging is disabled
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # logging receive`
	`switch (config) # show logging`
	`Local logging level: info`
	`Default remote logging level: notice`
	`No remote syslog servers configured.`
	`Allow receiving of messages from remote hosts: yes`
	`Number of archived log files to keep: 10`
	`Log rotation size threshold: 5.000% of partition (43 megabytes)`
	`Log format: standard`
	`Subsecond timestamp field: disabled`
	`Levels at which messages are logged:`
	`  CLI commands: notice`
	`  Audit messages: notice`
	`switch (config) #`

Related Commands	show logging logging local logging local override
Note	• This does not log to the console TTY port • In-band management should be enabled in order to open a channel from the host to the CPU • If enabled, only log messages matching or exceeding the minimum severity specified with the “logging local” command will be logged, regardless of what is sent from the remote host

logging format

logging format {standard | welf [fw-name <hostname>]}
no logging format {standard | welf [fw-name <hostname>]}

Sets the format of the logging messages.
The no form of the command resets the format to its default.

Syntax Description	standard	Standard format.
	welf	WebTrends Enhanced Log file (WELF) format.
	hostname	Specifies the firewall hostname that should be associated with each message logged in WELF format. If no firewall name is set, the hostname is used by default.
Default	standard	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # logging format standard`
	`switch (config) # show logging`
	`Local logging level: info`
	`Default remote logging level: notice`
	`No remote syslog servers configured.`
	`Allow receiving of messages from remote hosts: yes`
	`Number of archived log files to keep: 10`
	`Log rotation size threshold: 5.000% of partition (43 megabytes)`
	`Log format: standard`
	`Subsecond timestamp field: disabled`
	`Levels at which messages are logged:`
	`  CLI commands: notice`
	`  Audit messages: notice`
	`switch (config) #`	

Related Commands	show logging	
Note		

logging fields

logging fields seconds {enable | fractional-digits <f-digit> | whole-digits <w-digit>}
no logging fields seconds {enable | fractional-digits <f-digit> | whole-digits <w-digit>}

Specifies whether to include an additional field in each log message that shows the number of seconds since the Epoch or not.
The no form of the command disallows including an additional field in each log message that shows the number of seconds since the Epoch.

Syntax Description	enable	Specifies whether to include an additional field in each log message that shows the number of seconds since the Epoch or not.
	f-digit	The fractional-digits parameter controls the number of digits to the right of the decimal point. Truncation is done from the right. Possible values are: 1, 2, 3, or 6.
	w-digit	The whole-digits parameter controls the number of digits to the left of the decimal point. Truncation is done from the left. Except for the year, all of these digits are redundant with syslog's own date and time. Possible values: 1, 6, or all.
Default	disabled	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # logging fields seconds enable
switch (config) # logging fields seconds whole-digits 1
switch (config) # show logging
Local logging level: info
  Override for class mgmt-front: warning
Default remote logging level: notice
No remote syslog servers configured.
Allow receiving of messages from remote hosts: no
Number of archived log files to keep: 10
Log rotation size threshold: 5.000% of partition (43 megabytes)
Log format: standard
Subsecond timestamp field: enabled
Subsecond timestamp precision: 1 whole digit; 3 fractional digits
Levels at which messages are logged:
  CLI commands: notice
  Audit messages: notice
switch (config) #
```

Related Commands	show logging
Note	This is independent of the standard syslog date and time at the beginning of each message in the format of “July 15 18:00:00”. Aside from indicating the year at full precision, its main purpose is to provide subsecond precision.

logging level

logging level {cli commands <log-level> | audit mgmt <log-level>}

Sets the severity level at which CLI commands or the management audit message that the user executes are logged. This includes auditing of both configuration changes and actions.

Syntax Description	cli commands	Sets the severity level at which CLI commands which the user executes are logged.
	audit mgmt	Sets the severity level at which all network management audit messages are logged.
	log-level	• alert - alert notification, action must be taken immediately • crit - critical condition • debug - debug level messages • emerg - system is unusable (emergency) • err - error condition • info - informational condition • none - disables the logging locally and remotely • notice - normal, but significant condition • warning - warning condition
Default	CLI commands and audit message are set to notice logging level	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # logging level cli commands info`
	`switch (config) # show logging`
	`Local logging level: info`
	`  Override for class mgmt-front: warning`
	`Default remote logging level: notice`
	`No remote syslog servers configured.`
	`Allow receiving of messages from remote hosts: no`
	`Number of archived log files to keep: 10`
	`Log rotation size threshold: 5.000% of partition (43 megabytes)`
	`Log format: standard`
	`Subsecond timestamp field: enabled`
	`Subsecond timestamp precision: 1 whole digit; 3 fractional digits`
	`Levels at which messages are logged:`
	`  CLI commands: info`
	`  Audit messages: notice`
	`switch (config) #`	

Related Commands	show logging	
Note		

logging files delete

logging files delete {current | oldest [<number of files>]}

Deletes the current or oldest log files.

Syntax Description	current	Deletes current log file.
	oldest	Deletes oldest log file.
	number of files	Sets the number of files to be deleted.
Default	CLI commands and audit message are set to notice logging level	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # logging files delete current` `switch (config) #`	
Related Commands	show logging show log files	
Note		

logging files rotation

logging files rotation {criteria { frequency <freq> | size <size-mb>| size-pct <size-percentage>} | force | max-number <number-of-files>}

Sets the rotation criteria of the logging files.

Syntax Description	freq	Sets rotation criteria according to time. Possible options are: • Daily • Weekly • Monthly
	size-mb	Sets rotation criteria according to size in mega bytes. The range is 1-9999.
	size-percentage	Sets rotation criteria according to size in percentage of the partition where the logging files are kept in. The percentage given is truncated to three decimal points (thousandths of a percent).
	force	Forces an immediate rotation of the log files. This does not affect the schedule of auto-rotation if it was done based on time: the next automatic rotation will still occur at the same time for which it was previously scheduled. Naturally, if the auto-rotation was based on size, this will delay it somewhat as it reduces the size of the active log file to zero.
	number-of-files	The number of log files will be kept. If the number of log files ever exceeds this number (either at rotation time, or when this setting is lowered), the system will delete as many files as necessary to bring it down to this number, starting with the oldest.
Default	10 files are kept by default with rotation criteria of 5% of the log partition size	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # logging files rotation criteria size-pct 6`
	`switch (config) # show logging`
	`Local logging level: info`
	`  Override for class mgmt-front: warning`
	`Default remote logging level: notice`
	`No remote syslog servers configured.`
	`Allow receiving of messages from remote hosts: no`
	`Number of archived log files to keep: 10`
	`Log rotation size threshold: 6.000% of partition (51.60 megabytes)`
	`Log format: standard`
	`Subsecond timestamp field: enabled`
	`Subsecond timestamp precision: 1 whole digit; 3 fractional digits`
	`Levels at which messages are logged:`
	`  CLI commands: info`
	`  Audit messages: notice`
	`switch (config)`

Related Commands	show logging show log files
Note	

logging files upload

logging files upload {current | <file-number>} <url>

Uploads a log file to a remote host.

Syntax Description	current	The current log file. The current log file will have the name “messages” if you do not specify a new name for it in the upload URL.
	file-number	An archived log file. The archived log file will have the name “messages<n>.gz” (while “n” is the file number) if you do not specify a new name for it in the upload URL. The file will be compressed with gzip.
	url	Uplaods URL path. FTP, TFTP, SCP, and SFTP are supported. For example: scp://username[:password]@hostname/path/filename.
Default	10 files are kept by default with rotation criteria of 5% of the log partition size	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # logging files uplaod 1 scp://admin@scpserver`	
Related Commands	show logging show log files	
Note		

logging monitor

logging monitor <facility> <priority-level>
no logging monitor <facility> <priority-level>

Sets monitor log facility and level to print to the terminal.
The no form of the command disables printing logs of facilities to the terminal.

Syntax Description	facility	• mgmt-front • mgmt-back • mgmt-core • events • sx-sdk • mlnx-daemons • iss-modules
	priority-level	• none • emerg • alert • crit • err • warming • notice • info • debug
Default	no logging monitor	
Configuration Mode	Config	
History	3.3.4000	
Role	admin	
Example	`switch (config) # logging monitor events notice` `switch (config) #`	
Related Commands		
Note		

logging debug-files

logging debug-files {delete {current | oldest} | rotation {criteria | force | max-num} | update {<number> | current}}

Configures settings for debug log files.

Syntax Description	delete {current | oldest}	Deletes certain debug-log files. • current: Deletes the current active debug-log file • oldest: Deletes some of the oldest debug-log files

	rotation {criteria {frequency {daily | weekly | monthly} | size <size> | size-pct <percentage>} | force | max-num}	Configures automatic rotation of debug-logging files.
		• criteria: Sets how the system decides when to rotate debug files.
		  • frequency: Rotate log files on a fixed time-based schedule
		  • size: Rotate log files when they pass a size threshold in megabytes
		  • size-pct: Rotate logs when they surpass a specified percentage of disk
		• forces: Forces an immediate rotation of the log files
		• max-num: Specifies the maximum number of old log files to keep

	update {<number> | current}	Uploads a local debug-log file to a remote host. • current: Uploads log file “messages” to a remote host • number: Uploads compressed log file “debug.<number>.gz” to a remote host. Range is 1-10.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config) # logging debug-files delete current` `switch (config) #`	
Related Commands		
Note		

show logging

show logging

Displays the logging configurations.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show logging`
	`Local logging level: info`
	`  Override for class mgmt-front: warning`
	`Default remote logging level: notice`
	`No remote syslog servers configured.`
	`Allow receiving of messages from remote hosts: no`
	`Number of archived log files to keep: 10`
	`Log rotation size threshold: 5.000% of partition (43 megabytes)`
	`Log format: standard`
	`Subsecond timestamp field: enabled`
	`Subsecond timestamp precision: 1 whole digit; 3 fractional digits`
	`Levels at which messages are logged:`
	`  CLI commands: info`
	`  Audit messages: notice`
	`switch (config) #`

Related Commands	logging fields logging files rotation logging level logging local logging receive logging <syslog IP address>
Note	

show log

show log [continues | files [<file-number>]] [[not] matching <reg-exp>]

Displays the log file with optional filter criteria.

Syntax Description	continues	Displays the last few lines of the current log file and then continues to display new lines as they come in until the user hits Ctrl+C, similar to LINUX “tail” utility.
	files	Displays the list of log files.
	<file-number>	Displays an archived log file, where the number may range from 1 up to the number of archived log files available.
	[not] matching <reg-exp>	The file is piped through a LINUX “grep” utility to only include lines either matching, or not matching, the provided regular expression.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
	3.3.4402	Updated example and added note
Role	admin	

Example

```
switch (config) # show log matching "Executing|Action"
Jan 19 10:55:38 arc-switch14 cli28202: [cli.NOTICE]: user admin: Executing command: en
Jan 19 11:19:32 arc-switch14 cli28202: [cli.NOTICE]: user admin: Executing command: image
install image-SX_PPC_M460EX-ppc-m460ex-20140119-115026.img
Jan 19 11:19:32 arc-switch14 mgmtd4064: [mgmtd.NOTICE]: Action ID 326: requested by: user
admin (System Administrator) via CLI
Jan 19 11:19:32 arc-switch14 mgmtd4064: [mgmtd.NOTICE]: Action ID 326: descr: install
system software image
Jan 19 11:19:32 arc-switch14 mgmtd4064: [mgmtd.NOTICE]: Action ID 326: param: image file-
name: image-SX_PPC_M460EX-ppc-m460ex-20140119-115026.img, version: SX_PPC_M460EX
3.0.0000-dev-master-HA 2014-01-19 11:50:26 ppc
Jan 19 11:19:32 arc-switch14 mgmtd4064: [mgmtd.NOTICE]: Action ID 326: param: switch next
boot location after install: no
switch (config) #
```

Related Commands	logging fields logging files rotation logging level logging local logging receive logging <syslog IP address> show logging
Note	When using a regular expression containing | (OR), the expression should be surrounded by quotes (“<expression>”), otherwise it is parsed as filter (PIPE) command.

4.6 Debugging

- ***To use the debugging logs feature:***

Step 1. Enable debugging. Run:

Step 2. Display the debug level set. Run:

Step 3. Display the logs. Run:

4.6.1 Commands

debug ethernet all

debug ethernet all
no debug ethernet all

Enables debug traces for Ethernet modules.
The no form of the command disables the debug traces for all Ethernet modules.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.3.4150
Role	admin
Example	`switch (config) # debug ethernet all` `switch (config) #`
Related Commands	
Note	

debug ethernet dcbx

debug ethernet dcbx {all | management | fail-all | control-panel | tlv}

Configures the trace level for DCBX.
The no form of the command disables the configured DCBX debug traces.

Syntax Description	all	Enables all traces.
	management	Management messages.
	fail-all	All failure traces.
	control-panel	Control plane traces.
	tlv	TLV related trace configuration.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config) # debug ethernet dcbx all` `switch (config) #`	
Related Commands		
Note		

debug ethernet ip

debug ethernet ip {all | arp all | dhcp-relay {all | error} | igmp-snooping {all | forward-db-messages | group-info | Init-shut | packet-dump | query | system-resources-management | source-info | timer | vlan-info} | interface {all | arp-packet-dump | buffer | enet-packet-dump | error | fail-all | filter | trace-error | trace-event} | ospf {adjacency | all | configuration | ddp-packet | helper | Interface | ism | lrq-packet | lsa_packet | lsu-packet}}

Enables debug traces for Ethernet routing specific modules.
The no form of the command disables the debug traces for ethernet routing protocols.

Syntax Description	all	Enables debug traces for all routing modules.
	arp all	Enables the trace level for ARP.
	dhcp-relay {all | error}	Configures the trace level for DHCP. • all: Enables track traces • error: Error code debug messages
	igmp-snooping {all | forward-db-messages | group-info | Init-shut | packet-dump | query | system-resources-management | source-info | timer | vlan-info}	Configures the trace level for IGMP snooping. • all: Enables track traces • forward-db-messages: Forwarding database messages • group-info: Group information messages • Init-shut: Init and shutdown messages • packet-dump: Packet dump messages • query: Query related messages • system-resources-management: System resources management messages • source-info: Source information messages • timer: Timer messages • vlan-info: VLAN information messages
	interface {all | arp-packet-dump | buffer | enet-packet-dump | error | fail-all | filter | trace-error | trace-event}	Configures the trace level for interface. • all: Enable track traces • arp-packet-dump: ARP packet dump trace • buffer: Buffer trace • enet-packet-dump: ENET packet dump trace • error: Trace error messages • fail-all: All failures including Packet Validation Trace • filter: Lower layer traces • trace-error: Trace error messages • trace-event:
	ospf {adjacency | all | configuration | ddp-packet | helper | Interface | ism | lrq-packet | lsa_packet | lsu-packet}	Configures the trace level for OSPF. • adjacency: Adjacency formation debug messages • all: Enable track traces • configuration: Configuration debug messages • ddp-packet: DDP packet debug messages • helper: Helper debug messages • Interface: Interface debug messages • ism: Interface State Machine debug messages • lrq-packet: Link State Request Packet debug messages • lsa_packet: Link State Acknowledge Packet debug messages • lsu-packet: Link State Update Packet debug messages • nsm: Neighbor State Machine debug messages
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config) # debug ethernet ip arp all` `switch (config) #`	

Related Commands
Note

debug ethernet lacp

debug ethernet lacp {all | all-resource | data-path | fail-all | init-shut | management | memory | packet}
no debug ethernet lacp {all | all-resources | data-path | fail-all | init-shut | management | memory | packet}

Configures the trace level for LACP.
The no form of the command disables the configured LACP debug traces.

Syntax Description	all	Enables all traces.
	all-resource	BPDU related messages.
	data-path	Init and shutdown traces.
	fail-all	Management messages.
	init-shut	Memory related messages.
	management memory	IP packet dump trace.
	memory	All failure traces.
	packet	OS resource trace.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config) # debug ethernet lacp all` `switch (config) #`	
Related Commands		
Note		

debug ethernet lldp

debug ethernet lldp {all | control-panel | critical-event | data-path | fail-all | init-shut | management | memory | neigh-add | neigh-age-out | neigh-del | neigh-drop | neigh-updt | tlv}
no debug ethernet lldp {all | control-panel | critical-event | data-path | fail-all | init-shut | management | memory | neigh-add | neigh-age-out | neigh-del | neigh-drop | neigh-updt | tlv}

Configures the trace level for LLDP.
The no form of the command disables the configured LLDP debug traces.

Syntax Description	all	Enables all traces.
	control-panel	Control plane traces.
	critical-event	Critical traces.
	data-path	IP packet dump trace.
	fail-all	All failure traces.
	init-shut	Init and shutdown traces.
	management	Management messages.
	memory	Memory related messages.
	neigh-add	Neighbor add traces.
	neigh-age-out	Neighbor ageout traces.
	neigh-del	Neighbor delete traces.
	neigh-drop	Neighbor drop traces.
	neigh-updt	Neighbor update traces.
	tlv	TLV related trace configuration
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config) # debug ethernet lldp all` `switch (config) #`	
Related Commands		
Note		

debug ethernet port

debug ethernet port all

Configures the trace level for port.
The no form of the command disables the configured port debug traces.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.3.4150
Role	admin
Example	`switch (config) # debug ethernet port all` `switch (config) #`
Related Commands	
Note	

debug ethernet qos

debug ethernet qos {all | all-resource | control-panel | fail-all | filters | init-shut | management | memory | packet}
no debug ethernet qos {all | all-resource | control-panel | fail-all | filters | init-shut | management | memory | packet}

Configures the trace level for QoS.
The no form of the command disables the configured QoS debug traces.

Syntax Description	all	Enables all traces.
	all-resource	OS resource traces.
	control-panel	Control plane traces.
	fail-all	All failure traces.
	filters	Lower layer traces.
	init-shut	Init and shutdown traces.
	management	Management messages.
	memory	Memory related messages.
	packet	BPDU related messages.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config) # debug ethernet port all` `switch (config) #`	
Related Commands		
Note		

debug ethernet spanning-tree

debug ethernet spanning-tree {all | error | event | filters | init-shut | management | memory | packet | port-info-state-machine | port-receive-state-machine | port-role-selection-state-machine | port-transit-state-machine | port-transmit-state-machine | protocol-migration-state-machine | timers}
no debug ethernet spanning-tree {all | error | event | filters | init-shut | management | memory | packet | port-info-state-machine | port-receive-state-machine | port-role-selection-state-machine | port-transit-state-machine | port-transmit-state-machine | protocol-migration-state-machine | timers}

Configures the trace level for spanning-tree.
The no form of the command disables the configured spanning-tree debug traces.

Syntax Description	all	Enables all traces.
	error	Error messages trace.
	event	Events related messages.
	filters	Lower later traces.
	init-shut	Init and shutdown traces.
	management	Management messages.
	memory	Memory related messages.
	packet	BPDU related messages.
	port-info-state-machine	Port information messages.
	port-receive-state-machine	Port received messages.
	port-role-selection-state-machine	Port role selection messages.
	port-transit-state-machine	Port transition messages.
	port-transmit-state-machine	Port transmission messages.
	protocol-migration-state-machine	Protocol migration messages.
	timers	Timer modules message.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config) # debug ethernet spanning-tree all` `switch (config) #`	

Related Commands
Note

debug ethernet vlan

debug ethernet vlan {all | fwd | priority | filters}
no debug ethernet vlan {all | fwd | priority | filters}

Configures the trace level for VLAN.
The no form of the command disables the configured VLAN debug traces.

Syntax Description	all	Enables all traces
	fwd	Forward.
	priority	Priority.
	filters	Lower layer traces.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config) # debug ethernet vlan all` `switch (config) #`	
Related Commands		
Note		

show debug ethernet

show debug ethernet {dcbx | ip {arp | dhcp-relay | igmp-snooping | interface | ospf} | lacp | lldp | port | qos | spanning-tree | vlan}

Displays debug level configuration on a specific switch.

Syntax Description	dcbx	Displays the trace level for spanning tree.
	ip	Displays debug trace level for ethernet routing module. • arp • dhcp-relay • igmp-snooping • interface • ospf
	lacp	Displays the trace level for LACP.
	lldp	Displays the trace level for LLDP.
	port	Displays the trace level for port.
	qos	Displays the trace level for QoS.
	spanning-tree	Displays the trace level for spanning tree.
	vlan	Displays the trace level for VLAN.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4150	
Role	admin	

Example	`switch (config) # show debug ethernet dcbx`
	`dcbx protocol :`
	`management is ON`
	`fail-all is ON`
	`control-panel is ON`
	`tlv is ON`
	`switch (config) #`	

Related Commands		
Note		

show log debug

show log debug [continuous | files | matching | not]

Displays current event debug-log file in a scrollable pager.

Syntax Description	continuous	Displays new event log messages as they arrive.
	files	Displays archived debug log files.
	matching	Displays event debug logs that match a given regular expression.
	not	Displays event debug logs that do not meet certain criteria.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4150	
Role	admin	

Example	`switch (config) # show log debug`
	Jun 15 16:20:47 switch-627e4c last message repeated 7 times
	Jun 15 16:20:47 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>QoSHwQueueDelete i4IfIndex[137]
	Jun 15 16:20:47 switch-627e4c last message repeated 7 times
	Jun 15 16:20:47 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>QoSHwQueueDelete i4IfIndex[141]
	Jun 15 16:20:47 switch-627e4c last message repeated 7 times
	Jun 15 16:20:48 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: ==FsHwSetSpeed sx_api_port_speed_admin_set = 0
	Jun 15 16:20:48 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: ==FsHwGetSpeed sx_api_port_speed_oper_get = 0
	Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[89], u1ConfigOption[6]
	Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[33], u1ConfigOption[6]
	Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[73], u1ConfigOption[6]
	Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[121], u1ConfigOption[6]
	Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[133], u1ConfigOption[6]
	Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[13], u1ConfigOption[6]
	Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[81], u1ConfigOption[6]
	Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[117], u1ConfigOption[6]
	Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[65], u1ConfigOption[6]
	.
	.
	.
	`switch (config) #`	

Related Commands		
Note		

4.7 Event Notifications

MLNX-OS features a variety of supported events. Events are printed in the system log file, and, optionally, can be sent to the system administrator via email, SNMP trap or directly prompted to the terminal.

4.7.1 Supported Events

The following table presents the supported events and maps them to their relevant MIB OID.

Table 18 - Supported Event Notifications and MIB Mapping

Event Name	Event Description	MIB OID	Comments
asic-chip-down	ASIC (chip) down	Mellanox-EFM-MIB: asicChipDown	Not supported
cpu-util-high	CPU utilization has risen too high	Mellanox-EFM-MIB: cpuUtilHigh	
disk-space-low	File system free space has fallen too low	Mellanox-EFM-MIB: diskSpaceLow	
health-module-status	Health module status changed	Mellanox-EFM-MIB: systemHealthStatus	
insufficient-fans	Insufficient amount of fans in system	Mellanox-EFM-MIB: insufficientFans	
insufficient-fans-recover	Insufficient amount of fans in system recovered	Mellanox-EFM-MIB: insufficientFansRecover	
insufficient-power	Insufficient power supply	Mellanox-EFM-MIB: insufficientPower	
interface-down	An interface's link state has changed to DOWN	RFC1213: linkdown (SNMPv1)	Supported for Ethernet, InfiniBand and management interfaces for 1U and blade systems
interface-up	An interface's link state has changed to UP	RFC1213: linkup (SNMPv1)	Supported for Ethernet, InfiniBand and management interfaces for 1U and blade systems.
internal-bus-error	Internal bus (I^2C) error	Mellanox-EFM-MIB: internalBusError	
liveness-failure	A process in the system is detected as hung	Not implemented	
low-power	Low power supply	Mellanox-EFM-MIB: lowPower	
low-power-recover	Low power supply recover	Mellanox-EFM-MIB: lowPowerRecover	

Table 18 - Supported Event Notifications and MIB Mapping

Event Name	Event Description	MIB OID	Comments
new_root	Local bridge became a root bridge	Bridge-MIB: newRoot	Supported for Ethernet
paging-high	Paging activity has risen too high	N/A	Not supported
power-redundancy-mismatch	Power redundancy mis-match	Mellanox-EFM-MIB: powerRedundancyMis-match	Supported for SX65xx only systems
process-crash	A process in the system has crashed	Mellanox-EFM-MIB: procCrash	
process-exit	A process in the system unexpectedly exited	Mellanox-EFM-MIB: procUnexpectedExit	
snmp-authtrap	An SNMPv3 request has failed authentication	Not implemented	
topology_change	Topology change trig-gered by a local bridge	Bridge-MIB: topolo-gyChange	Supported for Ethernet
unexpected-shutdown	Unexpected system shut-down	Mellanox-EFM-MIB: unexpectedShutdown	
To send, use the CLI com-mand: `snmp-server notify send-test`	Send a testing event	testTrap	
N/A	Reset occurred due to over-heating of ASIC	Mellanox-EFM-MIB: asicOverTempReset	Not supported
temperature-too-high	Temperature is too high	Mellanox-EFM-MIB: asicOverTemp	

4.7.2 Terminal Notifications

- ***To print events to the terminal:***

  Set the events you wish to print to the terminal. Run:

```
switch (config) # logging monitor events notice
```

  This command prints system events in the severity “notice” to the screen. For example, in case of interface-down event, the following gets printed to the screen.

```
switch (config) #
Wed Jul 10 11:30:42 2013: Interface IB1/17 changed state to DOWN
Wed Jul 10 11:30:43 2013: Interface IB1/18 changed state to DOWN
switch (config) #
```

4.7.3 Email Notifications

- ***To configure MLNX-OS to send you emails for all configured events and failures:***

Step 1. Enter to Config mode. Run:

```
switch >
switch > enable
switch # configure terminal
```

Step 2. Set your mailhub to the IP address to be your mail client's server – for example, Microsoft Outlook exchange server.

```
switch (config) # email mailhub <IP address>
```

Step 3. Add your email address for notifications. Run:

```
switch (config) # email notify recipient <email address>
```

Step 4. Configure the system to send notifications for a specific event. Run:

```
switch (config) # email notify event <event name>
```

Step 5. Show the list of events for which an email is sent. Run:

```
switch (config) # show email events
Failure events for which emails will be sent:
  process-crash: A process in the system has crashed
  unexpected-shutdown: Unexpected system shutdown

Informational events for which emails will be sent:
  asic-chip-down: ASIC (Chip) Down
  cpu-util-high: CPU utilization has risen too high
  cpu-util-ok: CPU utilization has fallen back to normal levels
  disk-io-high: Disk I/O per second has risen too high
  disk-io-ok: Disk I/O per second has fallen back to acceptable levels
  disk-space-low: Filesystem free space has fallen too low
.
.
.
switch (config) #
```

Step 6. Have the system send you a test email. Run:

```
switch # email send-test

The last command should generate the following email:
-----Original Message-----
From: Admin User [mailto:do-not-reply@switch.]
Sent: Sunday, May 01, 2011 11:17 AM
To: <name>
Subject: System event on switch: Test email for event notification

==== System information:
Hostname: switch
Version:  <version> 2011-05-01 14:56:31
          ...
Date:     2011/05/01 08:17:29
Uptime:   17h 8m 28.060s
```

```
This is a test email.
==== Done.
```

4.7.4 Commands

4.7.4.1 Email Notification

email autosupport ssl mode

email autosupport ssl mode {none | tls | tls-none}
no email autosupport ssl mode

Configures type of security to use for auto-support email.
The no form of the command resets auto-support email security mode to its default.

Syntax Description	none	Does not use TLS to secure auto-support email.
	tls	Uses TLS over the default server port to secure auto-support email and does not send an email if TLS fails.
	tls-none	Attempts TLS over the default server port to secure auto-support email, and falls back on plaintext if this fails.
Default	tls-none	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # email autosupport ssl mode tls`	
Related Commands	N/A	
Note		

email autosupport ssl cert-verify

email autosupport ssl cert-verify
no email autosupport ssl cert-verify

Verifies server certificates.
The no form of the command does not verify server certificates.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.2.3000
Role	admin
Example	`switch (config) # email autosupport ssl cert-verify`
Related Commands	N/A
Note	

email autosupport ssl ca-list

email autosupport ssl ca-list {<ca-list-name> | default_ca_list | none}
no email autosupport ssl ca-list

Configures supplemental CA certificates for verification of server certificates. The no form of the command removes supplemental CA certificate list.

Syntax Description	default_ca_list	Default supplemental CA certificate list.
	none	No supplemental list; uses built-in list only.
Default	default_ca_list	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # email autosupport ssl ca-list default_ca_list`	
Related Commands	N/A	
Note		

email dead-letter

email dead-letter {cleanup max-age <duration> | enable}
no email dead-letter

Configures settings for saving undeliverable emails.
The no form of the command disables sending of emails to vendor auto-support upon certain failures.

Syntax Description	duration	Example: “5d4h3m2s” for 5 days, 4 hours, 3 minutes, 2 seconds.
	enable	Saves dead-letter files for undeliverable emails.
Default	Save dead letter is enabled The default duration is 14 days	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # email dead-letter enable` `switch (config) #`	
Related Commands	show email	
Note		

email domain

email domain <hostname or IP address>
no email domain

Sets the domain name from which the emails will appear to come from (provided that the return address is not already fully-qualified). This is used in conjunction with the system hostname to form the full name of the host from which the email appears to come.
The no form of the command clears email domain override.

Syntax Description	hostname or IP address IP address.
Default	No email domain
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # email domain mellanox`
	`switch (config) # show email`
	`Mail hub: 10.0.8.11`
	`Mail hub port: 125`
	`Domain: mellanox`
	`Return address: do-not-reply`
	`Include hostname in return address: yes`
	`...`
	`switch (config) #`

Related Commands	show emails
Note	

email mailhub

email mailhub <hostname or IP address>
no email mailhub

Sets the mail relay to be used to send notification emails.
The no form of the command clears the mail relay to be used to send notification emails.

Syntax Description	hostname or IP address Hostname or IP address.
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # email mailhub 10.0.8.11`
	`switch (config) # show email`
	`Mail hub: 10.0.8.11`
	`Mail hub port: 25`
	`Domain: (not specified)`
	`Return address: do-not-reply`
	`Include hostname in return address: yes`
	`...`
	`switch (config) #`

Related Commands	show email [events]
Note	

email mailhub-port

email mailhub-port <hostname or IP address>
no email mailhub-port

Sets the mail relay port to be used to send notification emails.
The no form of the command resets the port to its default.

Syntax Description	hostname or IP address hostname or IP address.
Default	25
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # email mailhub-port 125`
	`switch (config) # show email`
	`Mail hub: 10.0.8.11`
	`Mail hub port: 125`
	`Domain: (system domain name)`
	`Return address: do-not-reply`
	`Include hostname in return address: yes`
	`...`
	`switch (config) #`

Related Commands	show email
Note	

email notify event

email notify event <event name>
no email notify event <event name>

Enables sending email notifications for the specified event type.
The no form of the command disables sending email notifications for the specified event type.

Syntax Description	event name	Example event names would include “process-crash” and “cpu-util-high”.

Default

No events are enabled

Configuration Mode

Config

History

3.1.0000

Role

admin

Example

```
switch (config) # email notify event process-crash
switch (config) # show email events
Failure events for which emails will be sent:
process-crash: A process in the system has crashed
unexpected-shutdown: Unexpected system shutdown

Informational events for which emails will be sent:
liveness-failure: A process in the system was detected as hung
process-exit: A process in the system unexpectedly exited
cpu-util-ok: CPU utilization has fallen back to normal levels
cpu-util-high: CPU utilization has risen too high
disk-io-ok: Disk I/O per second has fallen back to acceptable levels
...
temperature-too-high: Temperature has risen too high

All events for which autosupport emails will be sent:
process-crash: A process in the system has crashed
liveness-failure: A process in the system was detected as hungswitch
(config) #
switch (config) #
```

Related Commands

show email

Note

This does not affect auto-support emails. Auto-support can be disabled overall, but if it is enabled, all auto-support events are sent as emails.

email notify recipient

email notify recipient <email addr> [class {info | failure} | detail]
no email notify recipient <email addr> [class {info | failure} | detail]

Adds an email address from the list of addresses to which to send email notifications of events.
The no form of the command removes an email address from the list of addresses to which to send email notifications of events.

Syntax Description	email addr	Email address of intended recipient.
	class	Specifies which types of events are sent to this recipient.
	info	Sends informational events to this recipient.
	failure	Sends failure events to this recipient.
	detail	Sends detailed event emails to this recipient.
Default	No recipients are added	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # email notify recipient user2@autosupport.mellanox.com`
	`switch (config) # show email`
	`Mail hub:`
	`Mail hub port: 25`
	`Domain: (not specified)`
	`Return address: user1`
	`Include hostname in return address: no`
	`Dead letter settings:`
	`Save dead.letter files: yes`
	`Dead letter max age: (none)`
	`Email notification recipients:`
	`user2@autosupport.mellanox.com (all events, in detail)`
	`Autosupport emails`
	`Enabled: no`
	`Recipient: autosupport@autosupport.mellanox.com`
	`Mail hub: autosupport.mellanox.com`
	`switch (config) #`	

Related Commands	show email	
Note		

email return-addr

email return-addr <username>
no email domain

Sets the username or fully-qualified return address from which email notifications are sent.

- If the string provided contains an "@" character, it is considered to be fully-qualified and used as-is.
- Otherwise, it is considered to be just the username, and we append "@<host-name>.<domain>". The default is "do-not-reply", but this can be changed to "admin" or whatnot in case something along the line does not like fictitious addresses.

The no form of the command resets this attribute to its default.

Syntax Description	username	Username.
Default	do-not-reply	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # email return-addr user1`
	`switch (config) # show email`
	`Mail hub:`
	`Mail hub port: 25`
	`Domain: (not specified)`
	`Return address: user1`
	`Include hostname in return address: yes`
	`...`
	`switch (config) #`	

Related Commands	show email	
Note		

email return-host

email return-host
no email return-host

Includes the hostname in the return address for emails.
The no form of the command does not include the hostname in the return address for emails.

Syntax Description	N/A
Default	No return host
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # no email return-host`
	`switch (config) # show email`
	`Mail hub:`
	`Mail hub port:    25`
	`Domain:           (system domain name)`
	`Return address:   my-address`
	`Include hostname in return address: no`
	
	`Current reply address: host@localdomain`
	
	`Dead letter settings:`
	`  Save dead.letter files: yes`
	`  Dead letter max age:    5 days`
	
	`No recipients configured.`
	
	`Autosupport emails`
	`  Enabled:      no`
	`  Recipient:    autosupport@autosupport.mellanox.com`
	`  Mail hub:     autosupport.mellanox.com`
	`switch (config) #`

Related Commands	show email
Note	This only takes effect if the return address does not contain an “@” character.

email send-test

email send-test

Sends test-email to all configured event and failure recipients.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	`switch (config) # email autosupport enable` `switch (config) #`
Related Commands	show email [events]
Note	

email ssl mode

email ssl mode {none | tls | tls-none}
no email ssl mode

Sets the security mode(s) to try for sending email.
The no form of the command resets the email SSL mode to its default.

Syntax Description	none	No security mode, operates in plaintext.
	tls	Attempts to use TLS on the regular mailhub port, with STARTTLS. If this fails, it gives up.
	tls-none	Attempts to use TLS on the regular mailhub port, with STARTTLS. If this fails, it falls back on plaintext.
Default	default-cert	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # email ssl mode tls-none`	
Related Commands	N/A	
Note		

email ssl cert-verify

email ssl cert-verify
no email ssl cert-verify

Enables verification of SSL/TLS server certificates for email.
The no form of the command disables verification of SSL/TLS server certificates for email.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.2.3000
Role	admin
Example	`switch (config) # email ssl cert-verify`
Related Commands	N/A
Note	This command has no impact unless TLS is used.

email ssl ca-list

email ssl ca-list {<ca-list-name> | default-ca-list | none}
no email ssl ca-list

Specifies the list of supplemental certificates of authority (CA) from the certificate configuration database that is to be used for verification of server certificates when sending email using TLS, if any.
The no form of the command uses no list of supplemental certificates.

Syntax Description	ca-list-name	Specifies CA list name.
	default-ca-list	Uses default supplemental CA certificate list.
	none	Uses no list of supplemental certificates.
Default	default-ca-list	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # email ssl ca-list none`	
Related Commands	N/A	
Note	This command has no impact unless TLS is used, and certificate verification is enabled.	

show email

show email [events]

Shows email configuration or events for which email should be sent upon.

Syntax Description	events show event list
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show email`
	`Mail hub:`
	`Mail hub port:  25`
	`Domain:  (system domain name)`
	`Return address:  my-address`
	`Include hostname in return address: no`
	
	`Current reply address: host@localdomain`
	
	`Dead letter settings:`
	`  Save dead.letter files: yes`
	`  Dead letter max age:  5 days`
	
	`No recipients configured.`
	
	`Autosupport emails`
	`  Enabled:  no`
	`  Recipient:  autosupport@autosupport.mellanox.com`
	`  Mail hub:  autosupport.mellanox.com`
	`switch (config) #`

Related Commands	show email
Note	

4.8 mDNS

Multicast DNS (mDNS) protocol is used by the SM HA to deliver control information between the InfiniBand nodes via the management interface. To block sending mDNS traffic from the management interface run the command `no ha dns enable`.

4.8.1 Commands

ha dns enable

ha dns enable
no ha dns enable

Allows mDNS traffic.
The no form of the command blocks mDNS traffic from being sent from mgmt0.

Syntax Description	N/A
Default	Enabled.
Configuration Mode	Config
History	3.3.4000
Role	admin
Example	`switch (config) # no ha dns enable` `switch (config) #`
Related Commands	
Note	

4.9 User Management and Security

4.9.1 Authentication, Authorization and Accounting (AAA)

AAA is a term describing a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing the MLNX-OS switch. The MLNX-OS switch supports Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control device Plus (TACACS+) protocols.

- **Authentication** - authentication provides the initial method of identifying each individual user, typically by entering a valid username and password before access is granted. The AAA server compares a user's authentication credentials with the user credentials stored in a database. If the credentials match, the user is granted access to the network or devices. If the credentials do not match, authentication fails and network access is denied.
- **Authorization** - following the authentication, a user must gain authorization for performing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.
- **Accounting** - the last level is accounting, which measures the resources a user consumes during access. This includes the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information, and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

Authentication, authorization, and accounting services are often provided by a dedicated AAA server, a program that performs these functions. Network access servers interface with AAA servers using the Remote Authentication Dial-In User Service (RADIUS) protocol.

4.9.1.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service), widely used in network environments, is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for embedded network devices such as routers, modem servers, switches and so on. RADIUS is currently the de-facto standard for remote authentication. It is prevalent in both new and legacy systems.

It is used for several reasons:

- RADIUS facilitates centralized user administration
- RADIUS consistently provides some level of protection against an active attacker

4.9.1.2 TACACS+

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for providing NAS (Network Access Security). NAS ensures secure access from remotely connected users. TACACS implements the TACACS Client and provides the AAA (Authentication, Authorization and Accounting) functionalities.

TACACS is used for several reasons:

- Facilitates centralized user administration
- Uses TCP for transport to ensure reliable delivery
- Supports inbound authentication, outbound authentication and change password request for the authentication service
- Provides some level of protection against an active attacker

4.9.1.3 LDAP

LDAP (Lightweight Directory Access Protocol) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. LDAP is based on a client/server model. The switch acts as a client to the LDAP server. A remote user (the remote administrator) interacts only with the switch, not the back-end server and database.

LDAP authentication consists of the following components:

- A protocol with a frame format that utilizes TCP over IP
- A centralized server that stores all the user authorization information
- A client: in this case, the switch

Each entry in the LDAP server is referenced by its Distinguished Name (DN). The DN consists of the user-account name concatenated with the LDAP domain name. If the user-account name is John, the following is an example DN:

```
uid=John,ou=people,dc=domain,dc=com
```

4.9.2 User Accounts

There are two user account types: *admin* and *monitor*. As *admin*, the user is privileged to execute all the available operations. As *monitor*, the user can execute operations that display system configuration and status, or set terminal settings.

Table 19 - User Roles (Accounts) and Default Passwords

User Role	Default Password
admin	admin
monitor	monitor

4.9.3 Commands

4.9.3.1 User Accounts

username

username <username> [capability <cap> | disable [login | password] | full-name <name> | nopassword | password [0 | 7] <password>]
no username <username> [capability | disable [login | password] | full-name]

Creates a user and sets its capabilities, password and name.
The no form of the command deletes the user configuration.

Syntax Description	username	Specifies a username and creates a user account. New users are created initially with admin privileges but is disabled.
	cap	User capabilities: • admin - full administrative capabilities • monitor - read only capabilities and actions, can not change the running configuration
	disable [login | password]	• Disable - disable this account • Disable login - disable all logins to this account • Disable password - disable login to this account using a local password
	name	Full name of the user.
	nopassword	The next login of the user will not require password.
	0 | 7	• 0: specifies a login password in cleartext • 7: specifies a login password in encrypted text
	password	Specifies a password for the user in string form. If [0 | 7] was not specified then the password is in cleartext.
Default	The following usernames are available by default: • admin • monitor • xmladmin • xmluser	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # username monitor full-name smith
switch (config) # show usernames
USERNAME    FULL NAME               CAPABILITY  ACCOUNT STATUS
USERID      System Administrator    admin       Password set
admin       System Administrator    admin       Password set
monitor     smith                   monitor     Password set (SHA512)
xmladmin    XML Admin User          admin       No password required
xmluser     XML Monitor User        monitor     No password required
switch (config) #
```

Related Commands

show usernames
show users

Note

- To enable a user account, just set a password on it (or use the "... nopassword" command to enable it with no password required for login)
- Removing a user account does not terminate any current sessions that user has open; it just prevents new sessions from being established
- Encrypted password is useful for the "show configuration" command, since the cleartext password cannot be recovered after it is set

show usernames

show usernames

Displays list of users and their capabilities.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show usernames`
	`USERNAME  FULL NAME  CAPABILITY  ACCOUNT STATUS`
	`USERID  System Administrator  admin  Password set`
	`admin  System Administrator  admin  Password set`
	`monitor  smith  monitor  Password set (SHA512)`
	`xmladmin  XML Admin User  admin  No password required`
	`xmluser  XML Monitor User  monitor  No password required`
	`switch (config) #`

Related Commands	username show users
Note	

show users

show users [history]

Displays logged in users and related information such as idle time and what host they have connected from.

Syntax Description	history	Displays current and historical sessions.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show users`
	`USERNAME  FULL NAME  LINE  HOST  IDLE`
	`admin  System Administrator  pts/0  172.22.237.174  0d0h34m4s`
	`admin  System Administrator  pts/1  172.30.0.127  1d3h30m49s`
	`admin  System Administrator  pts/3  172.22.237.34  0d0h0m0s`
	`switch (config) #show users history`
	`admin  pts/3 172.22.237.34  Wed Feb  1 11:56  still logged in`
	`admin  pts/3 172.22.237.34  Wed Feb  1 11:42 - 11:46  (00:04)`
	
	`wtmp begins Wed Feb  1 11:38:10 2012`
	`switch (config) #`	

Related Commands	username show usernames	
Note		

show whoami

show whoami

Displays username and capabilities of user currently logged in.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show whoami`
	`Current user: admin`
	`Capabilities: admin`
	`switch (config) #`

Related Commands	username show usernames show users
Note	

4.9.3.2 AAA Methods

aaa accounting

aaa accounting changes default stop-only tacacs+
no aaa accounting changes default stop-only tacacs+

Enables logging of system changes to an AAA accounting server.
The no form of the command disables the accounting.

Syntax Description	N/A	
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	First version
	3.2.3000	Removed ‘time’ parameter from the command.
Role	admin	

Example	`switch (config) # aaa accounting changes default stop-only tacacs+`
	`switch (config) # show aaa`
	`AAA authorization:`
	`  Default User: admin`
	`  Map Order: local-only`
	`Authentication method(s):`
	`  local`
	`  radius`
	`  tacacs+`
	`  ldap`
	`Accounting method(s):`
	`  tacacs+`
	`switch (config) #`	

Related Commands	show aaa	
Note	• TACACS+ is presently the only accounting service method supported • Change accounting covers both configuration changes and system actions that are visible under audit logging, however this feature operates independently of audit logging, so it is unaffected by the “logging level audit mgmt” or “configuration audit” commands • Configured TACACS+ servers are contacted in the order in which they appear in the configuration until one accepts the accounting data, or the server list is exhausted • Despite the name of the “stop-only” keyword, which indicates that this feature logs a TACACS+ accounting “stop” message, and in contrast to configuration change accounting, which happens after configuration database changes, system actions are logged when the action is started, not when the action has completed	

aaa authentication login

aaa authentication login default <auth method> [<auth method> [<auth method> [<auth method> [<auth method>]]]]
no aaa authentication login

Sets a sequence of authentication methods. Up to four methods can be configured. The no form of the command resets the configuration to its default.

Syntax Description	auth-method	• local • radius • tacacs+ • ldap
Default	local	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # aaa authentication login default local radius tacacs+ ldap`
	`switch (config) # show aaa`
	`AAA authorization:`
	`  Default User: admin`
	`  Map Order: local-only`
	`Authentication method(s):`
	`  local`
	`  radius`
	`  tacacs+`
	`  ldap`
	`Accounting method(s):`
	`  tacacs+`
	`switch (config) #`	

Related Commands	show aaa	
Note	The order in which the methods are specified is the order in which the authentication is attempted. It is required that “local” is one of the methods selected. It is recommended that “local” be listed first to avoid potential problems logging in to local accounts in the face of network or remote server issues.	

aaa authentication attempts track enable

aaa authentication attempts track enable
no aaa authentication attempts track enable

Enables tracking of authentication failures.
The no form of the command disables tracking of authentication failures.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.2.3000
Role	admin
Example	`switch (config) # aaa authentication attempts track enable`
Related Commands	N/A
Note	• This is required for the lockout functionality described below, but can also be used on its own for informational purposes. • Disabling tracking does not clear any records of past authentication failures, or the locks in the database. However, it does prevent any updates to this database from being made: no new failures are recorded. It also disables lockout, preventing new lockouts from being recorded and existing lockouts from being enforced.

aaa authentication attempts lockout

aaa authentication attempts lockout {enable | lock-time | max-fail | unlock-time}
no aaa authentication attempts lockout {enable | lock-time | max-fail | unlock-time}

Configures lockout of accounts based on failed authentication attempts.
The no form of the command clears configuration for lockout of accounts based on failed authentication attempts.

Syntax Description	enable	Enables locking out of user accounts based on authentication failures. This both suspends enforcement of any existing lockouts, and prevents any new lockouts from being recorded. If lockouts are later re-enabled, any lockouts that had been recorded previously resume being enforced; but accounts which have passed the max-fail limit in the meantime are NOT automatically locked at this time. They would be permitted one more attempt, and then locked, because of how the locking is done: lockouts are applied after an authentication failure, if the user has surpassed the threshold at that time. Lockouts only work if tracking is enabled. Enabling lockouts automatically enables tracking. Disabling tracking automatically disables lockouts.
	lock-time	Sets maximum permitted consecutive authentication failures before locking out users. Unlike the “max-fail” setting, this does take effect immediately for all accounts If both unlock-time and lock-time are set, the unlock-time must be greater than the lock-time This is not based on the number of consecutive failures, and is therefore divorced from most of the rest of the tally feature, except for the tracking of the last login failure
	max-fail	Sets maximum permitted consecutive authentication failures before locking out users. This setting only impacts what lockouts are imposed while the setting is active; it is not retroactive to previous logins. So if max-fail is disabled or changed, this does not immediately cause any users to be changed from locked to unlocked or vice-versa.
	unlock-time	Enables the auto-unlock of an account after a specified number of seconds if a user account is locked due to authentication failures, counting from the last valid login attempt. Unlike the “max-fail” setting, this does take effect immediately for all accounts. If both unlock-time and lock-time are set, the unlock-time must be greater than the lock-time. Careful with disabling the unlock-time, particularly if you have max-fail set to something, and have not overridden the behavior for the admin (i.e. they are subject to lockouts also). If the admin account gets locked out, and there are no other administrators who can aid, the user may be forced to boot single-user and use the pam_tallybyname command-line utility to unlock your account manually. Even if one is careful not to incur this many authentication failures, it makes the system more subject to DOS attacks.

Default	N/A
Configuration Mode	Config
History	3.2.3000
Role	admin
Example	`switch (config) # aaa authentication attempts lockout enable`
Related Commands	N/A
Note	

aaa authentication attempts class-override

aaa authentication attempts class-override {admin [no-lockout] | unknown {no-track | hash-username}}
no aaa authentication attempts class-override {admin | unknown {no-track | hash-username}}

Overrides the global settings for tracking and lockouts for a type of account.
The no form of the command removes this override and lets the admin be handled according to the global settings.

Syntax Description	admin	Overrides the global settings for tracking and lockouts for the admin account. This applies only to the single account with the username “admin”. It does not apply to any other users with administrative privileges.
	no-lockout	Prevents the admin user from being locked out, though the authentication failure history is still tracked (if tracking is enabled overall).
	unknown	Overrides the global settings for tracking and lockouts for unknown accounts. The “unknown” class here contains the following categories: • Real remote usernames which simply failed authentication • Mis-typed remote usernames • Passwords accidentally entered as usernames • Bogus usernames made up as part of an attack on the system
	hash-username	Applies a hash function to the username, and stores the hashed result in lieu of the original.
	no-track	Does not track authentication for such users (which of course also implies no-lockout).
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # aaa authentication attempts class-override admin no-lockout`	
Related Commands	N/A	
Note		

aaa authentication attempts reset

aaa authentication attempts reset {all | user <username>} [{no-clear-history | no-unlock}]

Clears the authentication history for and/or unlocks specified users.

Syntax Description	all	Applies function to all users.
	user	Applies function to specified user.
	no-clear-history	Leaves the history of login failures but unlocks the account.
	no-unlock	Leaves the account locked but clears the history of login failures.
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # aaa authentication attempts reset user admin all`	
Related Commands	N/A	
Note		

clear aaa authentication attempts

clear aaa authentication attempts {all | user <username>} [no-clear-history | no-unlock]

Clears the authentication history for and/or unlocks specified users

Syntax Description	all	Applies function to all users.
	user	Applies function to specified user.
	no-clear-history	Clears the history of login failures.
	no-unlock	Unlocks the account.
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # aaa authentication attempts reset user admin no-clear-history`	
Related Commands	N/A	
Note		

aaa authorization

aaa authorization map [default-user <username> | order <policy>]
no aaa authorization map [default-user | order]

Sets the mapping permissions of a user in case a remote authentication is done. The no form of the command resets the attributes to default.

Syntax Description	username	Specifies what local account the authenticated user will be logged on as when a user is authenticated (via RADIUS or TACACS+) and does not have a local account. If the username is local, this mapping is ignored.
	policy	Sets the user mapping behavior when authenticating users via RADIUS or TACACS+ to one of three choices. The order determines how the remote user mapping behaves. If the authenticated username is valid locally, no mapping is performed. The setting has the following three possible behaviors: • remote-first - If a local-user mapping attribute is returned and it is a valid local username, it maps the authenticated user to the local user specified in the attribute. Otherwise, it uses the user specified by the default-user command. • remote-only - Maps a remote authenticated user if the authentication server sends a local-user mapping attribute. If the attribute does not specify a valid local user, no further mapping is tried. • local-only - Maps all remote users to the user specified by the “aaa authorization map default-user <user name>” command. Any vendor attributes received by an authentication server are ignored.
Default	Default user - admin. Map order - remote-first.	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # aaa authorization map default-user admin
switch (config) # show aaa
AAA authorization:
   Default User: admin
   Map Order: remote-first
Authentication method(s):
   local
Accounting method(s):
   tacacs+
switch (config) #
```

Related Commands	show aaa username
Note	If, for example, the user is locally defined to have admin permission, but in a remote server such as RADIUS the user is authenticated as monitor and the order is remote-first, then the user will be given monitor permissions.

show aaa

show aaa

Displays the AAA configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show aaa`
	`AAA authorization:`
	`  Default User: admin`
	`  Map Order: remote-first`
	`Authentication method(s):`
	`  local`
	`Accounting method(s):`
	`  tacacs+`
	`switch (config) #`

Related Commands	aaa accounting aaa authentication aaa authorization show aaa show usernames username
Note	

show aaa authentication attempts

show aaa authentication attempts [configured | status user <username>]]

Shows the current authentication, authorization and accounting settings.

Syntax Description	authentication attempts	Displays configuration and history of authentication failures.
	configured	Displays configuration of authentication failure tracking.
	status user	Displays status of authentication failure tracking and lockouts for specific user.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.2.1000	
Role	admin	

Example

```
switch (config) # show aaa authentication attempts
Configuration for authentication failure tracking and locking:
   Track authentication failures:                   yes
   Lock accounts based on authentication failures:  yes
   Override treatment of 'admin' user:              (none)
   Override treatment of unknown usernames:         hash-usernames

Configuration for lockouts based on authentication failures:
   Lock account after consecutive auth failures:    5
   Allow retry on locked accounts (unlock time):    after 15 second(s)
   Temp lock after each auth failure (lock time):   none

Username         Known  Locked  Failures  Last fail time      Last fail
from
--------          -----  ------  --------  --------------       -------
-------
0Q72B43EHBKT8CB5AF5PGRX3U3B3TUL4CYJP93N(*) no     no         1     2012/
08/20 14:29:19  ttyS0

(*) Hashed for security reasons
switch-627d3c [standalone: master] (config) #
switch (config) #
```

Related Commands	N/A
Note	

4.9.3.3 RADIUS

radius-server

radius-server {key <secret>| retransmit <retries> | timeout <seconds>}
no radius-server {key | retransmit | timeout}

Sets global RADIUS server attributes.
The no form of the command resets the attributes to their default values.

Syntax Description	secret	Sets a secret key (shared hidden text string), known to the system and to the RADIUS server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry (1-60).
Default	3 seconds, 1 retry	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) #radius-server retransmit 3`
	`switch (config) # show radius`
	`RADIUS defaults:`
	`  Key:  3333`
	`  Timeout:  3`
	`  Retransmit:  1`
	`No RADIUS servers configured.`
	`switch (config) #`	

Related Commands	aaa authorization radius-server host show radius	
Note	Each RADIUS server can override those global parameters using the command “radius-server host”.	

radius-server host

radius-server host <IP address> {enable | auth-port <port> | key <secret>| retransmit <retries> | timeout <seconds>}
no radius-server host <IP address> {enable | auth-port }

Configures RADIUS server attributes.
The no form of the command resets the attributes to their default values and deletes the RADIUS server.

Syntax Description	IP address	RADIUS server IP address.
	enable	Administrative enable of the RADIUS server.
	port	RADIUS server UDP port number.
	secret	Sets a secret key (shared hidden text string), known to the system and to the RADIUS server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry (1-60).
Default	3 seconds, 1 retry Default UDP port is 1812	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # radius-server host 40.40.40.40
switch (config) # show radius
RADIUS defaults:
    Key:             3333
    Timeout:         3
    Retransmit:      1
RADIUS servers:
   40.40.40.40:1812
      Enabled:         yes
      Key:             3333 (default)
      Timeout:         3 (default)
      Retransmit:      1 (default)
switch (config) #
```

Related Commands

aaa authorization
radius-server
show radius

Note

- RADIUS servers are tried in the order they are configured
- If you do not specify a parameter for this configured RADIUS server, the configuration will be taken from the global RADIUS server configuration. Refer to “radius-server” command.

show radius

show radius

Displays RADIUS configurations.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show radius`
	`RADIUS defaults:`
	`  Key:  3333`
	`  Timeout:  3`
	`  Retransmit:  1`
	`RADIUS servers:`
	`  40.40.40.40:1812`
	`  Enabled:  yes`
	`  Key:  3333 (default)`
	`  Timeout:  3 (default)`
	`  Retransmit:  1 (default)`
	`switch (config) #`

Related Commands	aaa authorization radius-server radius-server host
Note	

4.9.3.4 TACACS+

tacacs-server

tacacs-server {key <secret>| retransmit <retries> | timeout <seconds>}
no tacacs-server {key | retransmit | timeout}

Sets global TACACS+ server attributes.
The no form of the command resets the attributes to default values.

Syntax Description	secret	Set a secret key (shared hidden text string), known to the system and to the TACACS+ server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry (1-60).
Default	3 seconds, 1 retry	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) #tacacs-server retransmit 3`
	`switch (config) # show tacacs`
	`TACACS+ defaults:`
	`  Key:  3333`
	`  Timeout:  3`
	`  Retransmit:  1`
	`No TACACS+ servers configured.`
	`switch (config) #`	

Related Commands	aaa authorization show radius show tacacs tacacs-server host	
Note	Each TACACS+ server can override those global parameters using the command “tacacs-server host”.	

tacacs-server host

tacacs-server host <IP address> {enable | auth-port <port> | auth-type <type> | key <secret> | retransmit <retries> | timeout <seconds>}
no tacacs-server host <IP address> {enable | auth-port}

Configures TACACS+ server attributes.
The no form of the command resets the attributes to their default values and deletes the TACACS+ server.

Syntax Description	IP address	TACACS+ server IP address.
	enable	Administrative enable for the TACACS+ server.
	port	TACACS+ server UDP port number.
	type	Authentication type. Possible values are: • ASCII • PAP (Password Authentication Protocol)
	secret	Sets a secret key (shared hidden text string), known to the system and to the TACACS+ server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry (1-60).
Default	3 seconds, 1 retry Default TCP port is 49 Default auth-type is PAP	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # tacacs-server host 40.40.40.40
switch (config) # show tacacs
TACACS+ defaults:
    Key:             3333
    Timeout:         3
    Retransmit:      1
TACACS+ servers:
   40.40.40.40:49
      Enabled:         yes
      Auth-type         PAP
      Key:             3333 (default)
      Timeout:         3 (default)
      Retransmit:      1 (default)
switch (config) #
```

Related Commands	aaa authorization show tacacs tacacs-server
Note	• TACACS+ servers are tried in the order they are configured • A PAP auth-type similar to an ASCII login, except that the username and password arrive at the network access server in a PAP protocol packet instead of being typed in by the user, so the user is not prompted • If the user does not specify a parameter for this configured TACACS+ server, the configuration will be taken from the global TACACS+ server configuration. Refer to “tacacs-server” command.

show tacacs

show tacacs

Displays TACACS+ configurations.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show tacacs`
	`TACACS+ defaults:`
	`  Key:  3333`
	`  Timeout:  3`
	`  Retransmit:  1`
	`TACACS+ servers:`
	`  40.40.40.40:49`
	`  Enabled:  yes`
	`  Auth-type  PAP`
	`  Key:  3333 (default)`
	`  Timeout:  3 (default)`
	`  Retransmit:  1 (default)`
	`switch (config) #`

Related Commands	aaa authorization tacacs-server tacacs-server host
Note	

4.9.3.5 LDAP

ldap base-dn

ldap base-dn <string>
no ldap base-dn

Sets the base distinguished name (location) of the user information in the schema of the LDAP server.
The no form of the command resets the attribute to its default values.

Syntax Description	string	A case-sensitive string that specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request. For example: “ou=users,dc=example,dc=com”, with no spaces. when: ou - Organizational unit dc - Domain component cn - Common name sn - Surname
Default	ou=users,dc=example,dc=com	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # ldap base-dn ou=department,dc=example,dc=com
switch (config) # show ldap
User base DN      : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute   : sAMAccountName
Bind DN           :
Bind password     :
Group base DN     :
Group attribute   : member
LDAP version      : 3
Referrals         : yes
Server port       : 389
Search Timeout    : 5
Bind Timeout      : 5
SSL mode          : none
Server SSL port   : 636 (not active)
SSL ciphers       : TLS1.2 (not active)
SSL cert verify   : yes
SSL ca-list       : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

Related Commands	show ldap
Note	

ldap bind-dn/bind-password

ldap {bind-dn | bind-password} <string>
no ldap {bind-dn | bind-password}

Gives the distinguished name or password to bind to on the LDAP server. This can be left empty for anonymous login (the default).
The no form of the command resets the attribute to its default values.

Syntax Description	string	A case-sensitive string that specifies distinguished name or password to bind to on the LDAP server.
Default	“”	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # ldap bind-dn my-dn
switch (config) # ldap bind-password my-password
switch (config) # show ldap
User base DN      : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute   : sAMAccountName
Bind DN           : my-dn
Bind password     : my-password
Group base DN     :
Group attribute   : member
LDAP version      : 3
Referrals         : yes
Server port       : 389
Search Timeout    : 5
Bind Timeout      : 5
SSL mode          : none
Server SSL port   : 636 (not active)
SSL ciphers       : TLS1.2 (not active)
SSL cert verify   : yes
SSL ca-list       : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

Related Commands	show ldap
Note	For anonymous login, bind-dn and bind-password should be empty strings “”.

ldap group-attribute/group-dn

ldap {group-attribute {<group-att> |member | uniqueMember} | group-dn <group-dn>}
no ldap {group-attribute | group-dn}

Sets the distinguished name or attribute name of a group on the LDAP server. The no form of the command resets the attribute to its default values.

Syntax Description	group-att	Specifies a custom attribute name.
	member	groupOfNames or group membership attribute.
	uniqueMember	groupOfUniqueNames membership attribute.
	group-dn	DN of group required for authorization.
Default	group-att: member group-dn: “”	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # ldap group-attribute member
switch (config) # ldap group-dn my-group-dn
switch (config) # show ldap
User base DN      : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute   : sAMAccountName
Bind DN           : my-dn
Bind password     : my-password
Group base DN     : my-group-dn
Group attribute   : member
LDAP version      : 3
Referrals         : yes
Server port       : 389
Search Timeout    : 5
Bind Timeout      : 5
SSL mode          : none
Server SSL port   : 636 (not active)
SSL ciphers       : TLS1.2 (not active)
SSL cert verify   : yes
SSL ca-list       : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

Related Commands	show ldap
Note	• The user's distinguished name must be listed as one of the values of this attribute, or the user will not be authorized to log in • After login authentication, if the group-dn is set, a user must be a member of this group or the user will not be authorized to log in. If the group is not set ("" - the default) no authorization checks are done.

ldap host

ldap host <IP Address> [order <number> last]
no ldap host <IP Address>

Adds an LDAP server to the set of servers used for authentication.
The no form of the command deletes the LDAP host.

Syntax Description	IP Address	IPv4 or IPv6 address.
	number	The order of the LDAP server.
	last	The LDAP server will be added in the last location.
Default	No hosts configured	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # ldap host 10.10.10.10
switch (config) # show ldap
User base DN      : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute   : sAMAccountName
Bind DN           : my-dn
Bind password     : my-password
Group base DN     : my-group-dn
Group attribute   : member
LDAP version      : 3
Referrals         : yes
Server port       : 389
Search Timeout    : 5
Bind Timeout      : 5
SSL mode          : none
Server SSL port   : 636 (not active)
SSL ciphers       : TLS1.2 (not active)
SSL cert verify   : yes
SSL ca-list       : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

Related Commands	show aaa show ldap
Note	• The system will select the LDAP host to try according to its order • New servers are by default added at the end of the list of servers

ldap login-attribute

ldap login-attribute {<string> | uid | sAMAccountName}
no ldap login-attribute

Sets the attribute name which contains the login name of the user.
The no form of the command resets this attribute to its default.

Syntax Description	string	Custom attribute name.
	uid	LDAP login name is taken from the user login user-name.
	sAMAccountName	SAM Account name, active directory login name.
Default	sAMAccountName	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	
Example		

```
switch (config) # ldap login-attribute uid
switch (config) # show ldap
User base DN      : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute   : uid
Bind DN           : my-dn
Bind password     : my-password
Group base DN     : my-group-dn
Group attribute   : member
LDAP version      : 3
Referrals         : yes
Server port       : 389
Search Timeout    : 5
Bind Timeout      : 5
SSL mode          : none
Server SSL port   : 636 (not active)
SSL ciphers       : TLS1.2 (not active)
SSL cert verify   : yes
SSL ca-list       : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

Related Commands	show aaa show ldap
Note	

ldap port

ldap port <port>
no ldap port

Sets the TCP port on the LDAP server to connect to for authentication.
The no form of the command resets this attribute to its default value.

Syntax Description	port	TCP port number.
Default	389	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # ldap port 1111
switch (config) # show ldap
User base DN      : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute   : uid
Bind DN           : my-dn
Bind password     : my-password
Group base DN     : my-group-dn
Group attribute   : member
LDAP version      : 3
Referrals         : yes
Server port       : 1111
Search Timeout    : 5
Bind Timeout      : 5
SSL mode          : none
Server SSL port   : 636 (not active)
SSL ciphers       : TLS1.2 (not active)
SSL cert verify   : yes
SSL ca-list       : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

Related Commands

show aaa
show ldap

Note

ldap referrals

ldap referrals
no ldap referrals

Enables LDAP referrals.
The no form of the command disables LDAP referrals.

Syntax Description	N/A
Default	LDAP referrals are enabled
Configuration Mode	Config
History	3.1.0000 3.3.5050 Updated Example
Role	admin

Example	`switch (config) # no ldap referrals`
	`switch (config) # show ldap`
	`User base DN : ou=department,dc=example,dc=com`
	`User search scope : subtree`
	`Login attribute : uid`
	`Bind DN : my-dn`
	`Bind password : my-password`
	`Group base DN : my-group-dn`
	`Group attribute : member`
	`LDAP version : 3`
	`Referrals : no`
	`Server port : 1111`
	`Search Timeout : 5`
	`Bind Timeout : 5`
	`SSL mode : none`
	`Server SSL port : 636 (not active)`
	`SSL ciphers : TLS1.2 (not active)`
	`SSL cert verify : yes`
	`SSL ca-list : default-ca-list`
	
	`LDAP servers:`
	`1: 10.10.10.10`
	`2: 10.10.10.12`
	`switch (config) #`

Related Commands	show aaa show ldap
Note	Referral is the process by which an LDAP server, instead of returning a result, will return a referral (a reference) to another LDAP server which may contain further information.

ldap scope

ldap scope <scope>
no ldap scope

Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.
The no form of the command resets the attribute to its default value.

Syntax Description	scope	• one-level - searches the immediate children of the base dn • subtree - searches at the base DN and all its children
Default	subtree	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # ldap scope subtree
switch (config) # show ldap
User base DN      : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute   : uid
Bind DN           : my-dn
Bind password     : my-password
Group base DN     : my-group-dn
Group attribute   : member
LDAP version      : 3
Referrals         : no
Server port       : 1111
Search Timeout    : 5
Bind Timeout      : 5
SSL mode          : none
Server SSL port   : 636 (not active)
SSL ciphers       : TLS1.2 (not active)
SSL cert verify   : yes
SSL ca-list       : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

Related Commands	show aaa show ldap
Note	

ldap ssl

ldap ssl {ca-list <options> | cert-verify | ciphers {all | TLS1.2} | mode <mode> | port <port-number>}
no ldap ssl {cert-verify | ciphers | mode | port}

Sets SSL parameter for LDAP.
The no form of the command resets the attribute to its default value.

Syntax Description	options	This command specifies the list of supplemental certificates of authority (CAs) from the certificate configuration database that is to be used by LDAP for authentication of servers when in TLS or SSL mode. The options are: • default-ca-list - uses default supplemental CA certificate list • none - no supplemental list, uses the built-in one only CA certificates are ignored if “ldap ssl mode” is not configured as either “tls” or “ssl”, or if “no ldap ssl cert-verify” is configured. The default-ca-list is empty in the factory default configuration. Use the command: “crypto certificate ca-list default-ca-list name” to add trusted certificates to that list. The “default-ca-list” option requires LDAP to consult the system’s configured global default CA-list for supplemental certificates.
	cert-verify	Enables verification of SSL/TLS server certificates. This may be required if the server's certificate is self-signed, or does not match the name of the server.
	ciphers {all | TLS1.2}	Sets SSL mode to be used.
	mode	Sets the security mode for connections to the LDAP server. • none – requests no encryption for the LDAP connection • ssl – the SSL-port configuration is used, an SSL connection is made before LDAP requests are sent (LDAP over SSL) • start-tls – the normal LDAP port is used, an LDAP connection is initiated, and then TLS is started on this existing connection
	port-number	Sets the port on the LDAP server to connect to for authentication when the SSL security mode is enabled (LDAP over SSL).
Default	cert-verify: enabled mode: none (LDAP SSL is not activated) port-number: 636 ciphers: all	

Configuration Mode	Config	
History	3.1.0000	First version
	3.2.3000	Added ca-list argument.
	3.3.5050	Added “ssl ciphers” parameter Updated Example
Role	admin	

Example

```
switch (config) # ldap ssl mode ssl
switch (config) # show ldap
User base DN      : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute   : uid
Bind DN           : my-dn
Bind password     : my-password
Group base DN     : my-group-dn
Group attribute   : member
LDAP version      : 3
Referrals         : no
Server port       : 1111
Search Timeout    : 5
Bind Timeout      : 5
SSL mode          : ssl
Server SSL port   : 636 (not active)
SSL ciphers       : TLS1.2 (not active)
SSL cert verify   : yes
SSL ca-list       : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

Related Commands

show aaa
show ldap

Note

- If available, the TLS mode is recommended, as it is standardized, and may also be of higher security
- The port number is used only for SSL mode. In case the mode is TLS, the LDAP port number will be used.

ldap timeout

ldap {timeout-bind | timeout-search} <seconds>
no ldap {timeout-bind | timeout-search}

Sets a global communication timeout in seconds for all LDAP servers to specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.
The no form of the command resets the attribute to its default value.

Syntax Description	timeout-bind	Sets the global LDAP bind timeout for all LDAP servers.
	timeout-search	Sets the global LDAP search timeout for all LDAP servers.
	seconds	Range: 1-60 seconds.
Default	5 seconds	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # ldap timeout-bind 10
switch (config) # show ldap
User base DN      : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute   : uid
Bind DN           : my-dn
Bind password     : my-password
Group base DN     : my-group-dn
Group attribute   : member
LDAP version      : 3
Referrals         : no
Server port       : 1111
Search Timeout    : 5
Bind Timeout      : 10
SSL mode          : none
Server SSL port   : 636 (not active)
SSL ciphers       : TLS1.2 (not active)
SSL cert verify   : yes
SSL ca-list       : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

Related Commands	show aaa show ldap
Note	

ldap version

ldap version <version>
no ldap version

Sets the LDAP version.
The no form of the command resets the attribute to its default value.

Syntax Description	version	Sets the LDAP version. Values: 2 and 3.
Default	3	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```
switch (config) # ldap version 3
switch (config) # show ldap
User base DN      : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute   : uid
Bind DN           : my-dn
Bind password     : my-password
Group base DN     : my-group-dn
Group attribute   : member
LDAP version      : 3
Referrals         : no
Server port       : 1111
Search Timeout    : 5
Bind Timeout      : 10
SSL mode          : none
Server SSL port   : 636 (not active)
SSL ciphers       : TLS1.2 (not active)
SSL cert verify   : yes
SSL ca-list       : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

Related Commands

show aaa
show ldap

Note

show ldap

show ldap

Displays LDAP configurations.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000 3.3.5050 Updated Example
Role	admin

Example	`switch (config) # show ldap`
	`User base DN : ou=department,dc=example,dc=com`
	`User search scope : subtree`
	`Login attribute : uid`
	`Bind DN : my-dn`
	`Bind password : my-password`
	`Group base DN : my-group-dn`
	`Group attribute : member`
	`LDAP version : 3`
	`Referrals : no`
	`Server port : 1111`
	`Search Timeout : 5`
	`Bind Timeout : 10`
	`SSL mode : none`
	`Server SSL port : 636 (not active)`
	`SSL ciphers : TLS1.2 (not active)`
	`SSL cert verify : yes`
	`SSL ca-list : default-ca-list`
	
	`LDAP servers:`
	`1: 10.10.10.10`
	`2: 10.10.10.12`
	`switch (config) #`

Related Commands	show aaa show ldap
Note	

4.10 Cryptographic (X.509, IPSec)

This chapter contains commands for configuring, generating and modifying x.509 certificates used in the system. Certificates are used for creating a trusted SSL connection to the system.

Crypto commands also cover IPSec configuration commands used for establishing a secure connection between hosts over IP layer which is useful for transferring sensitive information.

4.10.1 Commands

crypto ipsec peer local

crypto ipsec peer <IPv4 or IPv6 address> local <IPv4 or IPv6 address> {enable | keying {ike [auth {hmac-md5 | hmac-sha1 | hmac-sha256 | null} | dh-group | disable | encrypt | exchange-mode | lifetime | local | mode | peer-identity | pfs-group | preshared-key | prompt-preshared-key | transform-set] | manual [auth | disable | encrypt | local-spi | mode | remote-spi]}}

Configures ipsec in the system.

Syntax Description	enable	Enables IPSec peering.
	ike	Configures IPSec peering using IKE ISAKMP to manage SA keys. It has the following optional parameters: • auth: Configures the authentication algorithm for IPSec peering • dh-group: Configures the phase1 Diffie-Hellman group proposed for secure IKE key exchange • disable: Configures this IPSec peering administratively disabled • encrypt: Configures the encryption algorithm for IPSec peering • exchange-mode: Configures the IKE key exchange mode to propose for peering • lifetime: Configures the SA lifetime to propose for this IPSec peering • local-identity: Configures the ISAKMP payload identification value to send as local endpoint's identity • mode: Configures the peering mode for this IPSec peering • peer-identity: Configures the identification value to match against the peer's ISAKMP payload identification • pfs-group: Configures the phase2 PFS (Perfect Forwarding Secrecy) group to propose for Diffie-Hellman exchange for this IPSec peering • preshared-key: Configures the IKE pre-shared key for the IPSec peering • prompt-preshared-key: Prompts for the pre-shared key, rather than entering it on the command line • transform-set: Configures transform proposal parameters
	keying	Configures key management for this IPSec peering: • auth: Configures the authentication algorithm for this IPSec peering • disable: Configures this IPSec peering administratively disabled • encrypt: Configures the encryption algorithm for this IPSec peering • local-spi: Configures the local SPI for this manual IPSec peering • mode: Configures the peering mode for this IPSec peering • remote-spi: Configures the remote SPI for this manual IPSec peering
	manual	Configures IPSec peering using manual keys.
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config)# crypto ipsec peer 10.10.10.10 local 10.7.34.139 enable` `switch (config)#`	

Related Commands	N/A
Note	

crypto certificate ca-list

crypto certificate ca-list [default-ca-list name {<cert-name> | system-self-signed}]
no crypto certificate ca-list [default-ca-list name {<cert-name> | system-self-signed}]

Adds the specified CA certificate to the default CA certificate list.
The no form of the command removes the certificate from the default CA certificate list.

Syntax Description	cert-name	The name of the certificate.
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # crypto certificate default-cert name test`	
Related Commands	N/A	
Note	• Two certificates with the same subject and issuer fields cannot both be placed onto the CA list • The no form of the command does not delete the certificate from the certificate database • Unless specified otherwise, applications that use CA certificates will still consult the well-known certificate bundle before looking at the default-ca-list	

crypto certificate default-cert

crypto certificate default-cert name {<cert-name> | system-self-signed}
no crypto certificate default-cert name {<cert-name> | system-self-signed}

Designates the named certificate as the global default certificate role for authentication of this system to clients.
The no form of the command reverts the default-cert name to “system-self-signed” (the “cert-name” value is optional and ignored).

Syntax Description	cert-name	The name of the certificate.
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # crypto certificate default-cert name test`	
Related Commands	N/A	
Note	• A certificate must already be defined before it can be configured in the default-cert role • If the named default-cert is deleted from the database, the default-cert automatically becomes reconfigured to the factory default, the “system-self-signed” certificate	

crypto certificate generation

crypto certificate generation default {country-code | days-valid | email-addr | hash-algorithm {sha1 | sha256} | key-size-bits | locality | org-unit | organization | state-or-prov}

Configures default values for certificate generation.

Syntax Description	country-code	Configures the default certificate value for country code with a two-alphanumeric-character code or -- for none.
	days-valid	Configures the default certificate value for days valid.
	email-addr	Configures the default certificate value for email address.
	hash-algorithm {sha1 | sha256}	Configures the default certificate hashing algorithm.
	key-size-bits	Configures the default certificate value for private key size. (Private key length in bits – at least 1024, but 2048 is strongly recommended.)
	locality	Configures the default certificate value for locality.
	org-unit	Configures the default certificate value for organizational unit.
	organization	Configures the default certificate value for the organization name.
	state-or-prov	Configures the default certificate value for state or province.
Default	N/A	
Configuration Mode	Config	
History	3.2.1000	First version
	3.3.4350	Added “hash-algorithm” parameter
Role	admin	
Example	`switch (config) # crypto certificate generation default hash-algorithm sha256`	
Related Commands	N/A	
Note	The default hashing algorithm used is sha1.	

crypto certificate name

crypto certificate name {<cert-name> | system-self-signed} {comment <new comment> | generate self-signed [comment <cert-comment> | common-name <domain> | country-code <code> | days-valid <days> | email-addr <address> | hash-algorithm {sha1 | sha256} | key-size-bits <bits> | locality <name> | org-unit <name> | organization <name> | serial-num <number> | state-or-prov <name>]} | private-key pem <PEM string> | prompt-private-key | public-cert [comment <comment string> | pem <PEM string>] | regenerate days-valid <days> | rename <new name>}
no crypto certificate name <cert-name>

Configures default values for certificate generation.
The no form of the command clears/deletes certain certificate settings.

Syntax Description	cert-name	Unique name by which the certificate is identified.
	comment	Specifies a certificate comment.
	generate self-signed	Generates certificates. This option has the following parameters which may be entered sequentially in any order: • comment: Specifies a certificate comment (free string) • common-name: Specifies the common name of the issuer and subject (e.g. a domain name) • country-code: Specifies the country codwo-alphanu-meric-character country code, or “--” for none) • days-valid: Specifies the number of days the certificate is valid • email-addr: Specifies the email address • hash-algorithm: Specifies the hashing function used for signature algorithm • key-size-bits: Specifies the size of the private key in bits (private key length in bits - at least 1024 but 2048 is strongly recommended) • locality: Specifies the locality name • org-unit: Specifies the organizational unit name • organization: Specifies the organization name • serial-num: Specifies the serial number for the certificate (a lower-case hexadecimal serial number prefixed with “0x”) • state-or-prov: Specifies the state or province name
	private-key pem	Specifies certificate contents in PEM format.
	prompt-private-key	Prompts for certificate private key with secure echo.
	public-cert	Installs a certificate.
	regenerate	Regenerates the named certificate using configured certificate generation default values for the specified validity period
	rename	Renames the certificate.
Default	N/A	

Configuration Mode	Config	
History	3.2.3000	First version
	3.3.4402	Added “hash-algorithm” parameter
Role	admin	
Example	`switch (config) # crypto certificate name system-self-signed generate self-signed hash-algorithm sha256`	
Related Commands	N/A	
Note		

crypto certificate system-self-signed

crypto certificate system-self-signed regenerate [days-valid <days>]

Configures default values for certificate generation.

Syntax Description	days-valid	Specifies the number of days the certificate is valid
Default	N/A	
Configuration Mode	Config	
History	3.2.1000	
Role	admin	
Example	`switch (config) # crypto certificate system-self-signed regenerate days-valid 3`	
Related Commands	N/A	
Note		

show crypto certificate

show crypto certificate [detail | public-pem | default-cert [detail | public-pem] | [name <cert-name> [detail | public-pem] | ca-list [default-ca-list]]

Displays information about all certificates in the certificate database.

Syntax Description	ca-list	Displays the list of supplemental certificates configured for the global default system CA certificate role.
	default-ca-list	Displays information about the currently configured default certificates of the CA list.
	default-cert	Displays information about the currently configured default certificate.
	detail	Displays all attributes related to the certificate.
	name	Displays information about the certificate specified.
	public-pem	Displays the uninterpreted public certificate as a PEM formatted data string
Default	N/A	
Configuration Mode	Config	
History	3.2.1000	
Role	admin	

Example

```
switch (config)# show crypto certificate
Certificate with name 'system-self-signed' (default-cert)
    Comment:                        system-generated self-signed certif-
icate
    Private Key:                    present
    Serial Number:                  0x546c935511bcafc21ac0e8249fbe0844
    SHA-1 Fingerprint:
fe6df38dd26801971cb2d44f62dbe492b6063c5f

    Validity:
        Starts:                     2012/12/02 13:45:05
        Expires:                    2013/12/02 13:45:05

    Subject:
        Common Name:                IBM-DEV-Bay4
        Country:                    IS
        State or Province:
        Locality:
        Organization:
        Organizational Unit:
        E-mail Address:

    Issuer:
        Common Name:                IBM-DEV-Bay4
        Country:                    IS
        State or Province:
        Locality:
        Organization:
        Organizational Unit:
        E-mail Address:
switch (config)#
```

Related Commands N/A

Note

show crypto ipsec

show crypto ipsec [brief | configured | ike | policy | sa]

Displays information ipsec configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.2.1000
Role	admin

Example	`switch (config)# show crypto ipsec`
	`IPSec Summary`
	`-------------`
	`Crypto IKE is using pluto (Openswan) daemon.`
	`Daemon process state is stopped.`
	
	`No IPSec peers configured.`
	
	`IPSec IKE Peering State`
	`----------------------`
	`Crypto IKE is using pluto (Openswan) daemon.`
	`Daemon process state is stopped.`
	
	`No active IPSec IKE peers.`
	
	`IPSec Policy State`
	`------------------`
	`No active IPSec policies.`
	
	`IPSec Security Association State`
	`------------------------------`
	`No active IPSec security associations.`
	`switch (config)#`

Related Commands	N/A
Note	

4.11 Scheduled Jobs

Use the commands in this section to manage and schedule the execution of jobs

4.11.1 Commands

job

job <job ID>
no job <job ID>

Creates a job.
The no form of the command deletes the job.

Syntax Description	job ID	An integer.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # job 100` `switch (config job 100) #`	
Related Commands	show jobs	
Note	Job state is lost on reboot.	

command

command <sequence #> | <command>
no command <sequence #>

Adds a CLI command to the job.
The no form of the command deletes the command from the job.

Syntax Description	sequence #	An integer that controls the order the command is executed relative to other commands in this job. The commands are executed in an ascending order.
	command	A CLI command.
Default	N/A	
Configuration Mode	Config job	
History	3.1.0000	
Role	admin	

Example	`switch (config)# job 100`
	`switch (config job 100) # command 10 “show power”`
	`switch (config job 100) #`	

Related Commands	show jobs	
Note	• The command must be defined with inverted commas (“”) • The command must be added as it was executed from the “config” mode. For example, in order to change the interface description you need to add the command: “interface <type> <number> description my-description”.	

comment

comment <comment>
no comment

Adds a comment to the job.
The no form of the command deletes the comment.

Syntax Description	comment	The comment to be added (string).
Default	“”	
Configuration Mode	Config job	
History	3.1.0000	
Role	admin	

Example	`switch (config)# job 100`
	`switch (config job 100) # comment Job_for_example`
	`switch (config job 100) #`	

Related Commands	show jobs	
Note		

enable

enable
no enable

Enables the specified job.
The no form of the command disables the specified job.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config job
History	3.1.0000
Role	admin

Example	`switch (config)# job 100`
	`switch (config job 100) # enable`
	`switch (config job 100) #`

Related Commands	show jobs
Note	If a job is disabled, it will not be executed automatically according to its schedule; nor can it be executed manually.

execute

execute

Forces an immediate execution of the job.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config job
History	3.1.0000
Role	admin

Example	`switch (config)# job 100`
	`switch (config job 100) # execute`
	`switch (config job 100) #`

Related Commands	show jobs
Note	• The job timer (if set) is not canceled and the job state is not changed: i.e. the time of the next automatic execution is not affected • The job will not be run if not currently enabled

fail-continue

fail-continue
no fail-continue

Continues the job execution regardless of any job failures.
The no form of the command returns fail-continue to its default.

Syntax Description	N/A
Default	A job will halt execution as soon as any of its commands fails
Configuration Mode	Config job
History	3.1.0000
Role	admin

Example	`switch (config)# job 100`
	`switch (config job 100) # fail-continue`
	`switch (config job 100) #`

Related Commands	show jobs
Note	

name

name <job name>
no name

Configures a name for this job.
The no form of the command resets the name to its default.

Syntax Description	name	Specifies a name for the job (string).
Default	“”.	
Configuration Mode	Config job	
History	3.1.0000	
Role	admin	

Example	`switch (config)# job 100`
	`switch (config job 100) # name my-job`
	`switch (config job 100) #`	

Related Commands	show jobs	
Note		

schedule type

schedule type <recurrence type>
no schedule type

Sets the type of schedule the job will automatically execute on.
The no form of the command resets the schedule type to its default.

Syntax Description	recurrence type	The available schedule types are: • daily - the job is executed every day at a specified time • weekly - the job is executed on a weekly basis • monthly - the job is executed every month on a specified day of the month • once - the job is executed once at a single specified date and time • periodic - the job is executed on a specified fixed time interval, starting from a fixed point in time.
Default	once	
Configuration Mode	Config job	
History	3.1.0000	
Role	admin	

Example	`switch (config)# job 100`
	`switch (config job 100) # schedule type once`
	`switch (config job 100) #`	

Related Commands	show jobs	
Note	A schedule type is essentially a structure for specifying one or more future dates and times for a job to execute.	

schedule <recurrence type>

schedule <recurrence type> <interval and date>
no schedule

Sets the type of schedule the job will automatically execute on.
The no form of the command resets the schedule type to its default.

Syntax Description	recurrence type	The available schedule types are: • daily - the job is executed every day at a specified time • weekly - the job is executed on a weekly basis • monthly - the job is executed every month on a specified day of the month • once - the job is executed once at a single specified date and time • periodic - the job is executed on a specified fixed time interval, starting from a fixed point in time.
	interval and date	Interval and date, per recurrence type.
Default	once	
Configuration Mode	Config job	
History	3.1.0000	
Role	admin	

Example	`switch (config)# job 100`
	`switch (config job 100) # schedule monthly interval 10`
	`switch (config job 100) #`	

Related Commands	show jobs	
Note	A schedule type is essentially a structure for specifying one or more future dates and times for a job to execute.	

show jobs

show jobs [<job-id>]

Displays configuration and state (including results of last execution, if any exist) of all jobs, or of one job if a job ID is specified.

Syntax Description	job-id Job ID.
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # show jobs 10`
	`Job 10:`
	`  Status: inactive`
	`  Enabled: yes`
	`  Continue on failure: no`
	`  Schedule Type: once`
	`  Time and date: 1970/01/01 00:00:00 +0000`
	`  Last Exec Time: Thu 2012/04/05 13:11:42 +0000`
	`  Next Exec Time: N/A`
	`  Commands:`
	`  Command 10: show power`
	`  Last Output:`
	`====================`
	`Module Status`
	`====================`
	`PS1 OK`
	`PS2 NOT PRESENT`
	
	`switch (config) #`

Related Commands	show jobs
Note	

4.12 Statistics and Alarms

4.12.1 Commands

stats alarm <alarm-id> clear

stats alarm <alarm ID> clear

Clears alarm state.

Syntax Description	alarm ID	Alarms supported by the system, for example: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # stats alarm cpu_util_indiv clear` `switch (config) #`	
Related Commands	show stats alarm	
Note		

stats alarm <alarm-id> enable

stats alarm <alarm-id> enable
no stats alarm <alarm-id> enable

Enables the alarm.
The no form of the command disables the alarm, notifications will not be received.

Syntax Description	alarm ID	Alarms supported by the system, for example: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
Default	The default is different per alarm-id	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # stats alarm cpu_util_indiv enable` `switch (config) #`	
Related Commands	show stats alarm	
Note		

stats alarm <alarm-id> event-repeat

stats alarm <alarm ID> event-repeat {single | while-not-cleared}
no stats alarm <alarm ID> event-repeat

Configures repetition of events from this alarm.

Syntax Description	alarm ID	Alarms supported by the system, for example: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
	single	Does not repeat events: only sends one event whenever the alarm changes state.
	while-not-cleared	Repeats error events until the alarm clears.
Default	single	
Configuration Mode	Config	
History	3.1.0000	
Role	monitor/admin	
Example	`switch (config) # stats alarm cpu_util_indiv event-repeat single` `switch (config) #`	
Related Commands	show stats alarm	
Note		

stats alarm <alarm-id> {rising | falling}

stats alarm <alarm ID> {rising | falling} {clear-threshold | error-threshold} <threshold-value>

Configure alarms thresholds.

Syntax Description	alarm ID	Alarms supported by the system, for example: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
	falling	Configures alarm for when the statistic falls too low.
	rising	Configures alarm for when the statistic rises too high.
	error-threshold	Sets threshold to trigger falling or rising alarm.
	clear-threshold	Sets threshold to clear falling or rising alarm.
	threshold-value	The desired threshold value, different per alarm.
Default	Default is different per alarm-id	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # stats alarm cpu_util_indiv falling clear-threshold 10` `switch (config) #`	
Related Commands	show stats alarm	
Note	Not all alarms support all four thresholds.	

stats alarm <alarm-id> rate-limit

stats alarm <alarm ID> rate-limit {count <count-type> <count> | reset | window <window-type> <duration>}

Configures alarms rate limit.

Syntax Description	alarm ID	Alarms supported by the system, for example: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
	count-type	Long medium, or short count (number of alarms).
	reset	Set the count and window durations to default values for this alarm.
	window-type	Long medium, or short count, in seconds.
Default	Short window: 5 alarms in 1 hour Medium window: 20 alarms in 1 day Long window: 50 alarms in 7 days	
Configuration Mode	Config	
History	3.1.0000	
Role	monitor/admin	
Example	`switch (config) # stats alarm paging rate-limit window long 2000` `switch (config) #`	
Related Commands	show stats alarm	
Note		

stats chd <chd-id> clear

stats chd <CHD ID> clear

Clears CHD counters.

Syntax Description	CHD ID	CHD supported by the system, for example: • cpu_util - CPU utilization: percentage of time spent • cpu_util_ave - CPU utilization average: percentage of time spent • cpu_util_day - CPU utilization average: percentage of time spent • disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes • disk_io - Operating system aggregate disk I/O average: KB/sec • eth_day • eth_hour • fs_mnt_day - Filesystem system usage average: bytes • fs_mnt_month - Filesystem system usage average: bytes • fs_mnt_week - Filesystem system usage average: bytes • ib_day • ib_hour • intf_day - Network interface statistics aggregation: bytes • intf_hour - Network interface statistics (same as “interface” sample) • intf_util - Aggregate network utilization across all interfaces • memory_day - Average physical memory usage: bytes • memory_pct - Average physical memory usage • paging - Paging activity: page faults • paging_day - Paging activity: page faults
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # stats chd memory_day clear` `switch (config) #`	
Related Commands	show stats chd	
Note		

stats chd <chd-id> enable

stats chd <chd-id> enable
no stats chd <chd-id> enable

Enables the CHD.
The no form of the command disables the CHD.

Syntax Description	chd-id	CHD supported by the system, for example: • cpu_util - CPU utilization: percentage of time spent • cpu_util_ave - CPU utilization average: percentage of time spent • cpu_util_day - CPU utilization average: percentage of time spent • disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes • disk_io - Operating system aggregate disk I/O average: KB/sec • eth_day • eth_hour • fs_mnt_day - Filesystem system usage average: bytes • fs_mnt_month - Filesystem system usage average: bytes • fs_mnt_week - Filesystem system usage average: bytes • ib_day • ib_hour • intf_day - Network interface statistics aggregation: bytes • intf_hour - Network interface statistics (same as “interface” sample) • intf_util - Aggregate network utilization across all interfaces • memory_day - Average physical memory usage: bytes • memory_pct - Average physical memory usage • paging - Paging activity: page faults • paging_day - Paging activity: page faults
Default	Enabled	
Configuration Mode	Config	
History	3.1.0000	
Role	monitor/admin	
Example	`switch (config) # stats chd memory_day enable` `switch (config) #`	
Related Commands	show stats chd	
Note		

stats chd <chd-id> compute time

stats chd <CHD ID> compute time {interval | range} <number of seconds>

Sets parameters for when this CHD is computed.

Syntax Description	CHD ID	Possible IDs: • cpu_util - CPU utilization: percentage of time spent • cpu_util_ave - CPU utilization average: percentage of time spent • cpu_util_day - CPU utilization average: percentage of time spent • disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes • disk_io - Operating system aggregate disk I/O average: KB/sec • eth_day • eth_hour • fs_mnt_day - Filesystem system usage average: bytes • fs_mnt_month - Filesystem system usage average: bytes • fs_mnt_week - Filesystem system usage average: bytes • ib_day • ib_hour • intf_day - Network interface statistics aggregation: bytes • intf_hour - Network interface statistics (same as “interface” sample) • intf_util - Aggregate network utilization across all interfaces • memory_day - Average physical memory usage: bytes • memory_pct - Average physical memory usage • paging - Paging activity: page faults • paging_day - Paging activity: page faults
	interval	Specifies calculation interval (how often to do a new calculation) in number of seconds.
	range	Specifies calculation range, in number of seconds.
	number of seconds	Number of seconds.
Default	Different per CHD	
Configuration Mode	Config	
History	3.1.0000	
Role	monitor/admin	

Example	`switch (config) # stats chd memory_day compute time interval 120`
	`switch (config) # show stats chd memory_day`
	`CHD "memory_day" (Average physical memory usage: bytes):`
	`Source dataset: sample "memory"`
	`Computation basis: time`
	`Interval: 120 second(s)`
	`Range: 1800 second(s)`
	`switch (config) #`	

Related Commands	show stats chd
Note	

stats sample <sample-id> clear

stats sample <sample ID> clear

Clears sample history.

Syntax Description	sample ID	Possible sample IDs are: • congested • cpu_util - CPU utilization: milliseconds of time spent • disk_device_io - Storage device I/O statistics • disk_io - Operating system aggregate disk I/O: KB/sec • eth • fan - Fan speed • fs_mnt_bytes - Filesystem usage: bytes • fs_mnt_inodes - Filesystem usage: inodes • ib • interface - Network interface statistics • intf_util - Network interface utilization: bytes • memory - System memory utilization: bytes • paging - Paging activity: page faults • power - Power supply usage • power-consumption • temperature - Modules temperature
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # stats sample temperature clear` `switch (config) #`	
Related Commands	show stats sample	
Note		

stats sample <sample-id> enable

stats sample <sample-id> enable
no states sample <sample-id> enable

Enables the sample.
The no form of the command disables the sample.

Syntax Description	sample-id	Possible sample IDs are: • congested • cpu_util - CPU utilization: milliseconds of time spent • disk_device_io - Storage device I/O statistics • disk_io - Operating system aggregate disk I/O: KB/sec • eth • fan - Fan speed • fs_mnt_bytes - Filesystem usage: bytes • fs_mnt_inodes - Filesystem usage: inodes • ib • interface - Network interface statistics • intf_util - Network interface utilization: bytes • memory - System memory utilization: bytes • paging - Paging activity: page faults • power - Power supply usage • power-consumption • temperature - Modules temperature
Default	Enabled	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # stats sample temperature enable` `switch (config) #`	
Related Commands	show stats sample	
Note		

stats sample <sample-id> interval

stats sample <sample ID> interval <number of seconds>

Sets the amount of time between samples for the specified group of sample data.

Syntax Description	sample ID	Possible sample IDs are: • congested • cpu_util - CPU utilization: milliseconds of time spent • disk_device_io - Storage device I/O statistics • disk_io - Operating system aggregate disk I/O: KB/sec • eth • fan - Fan speed • fs_mnt_bytes - Filesystem usage: bytes • fs_mnt_inodes - Filesystem usage: inodes • ib • interface - Network interface statistics • intf_util - Network interface utilization: bytes • memory - System memory utilization: bytes • paging - Paging activity: page faults • power - Power supply usage • power-consumption • temperature - Modules temperature
	number of seconds	Interval in seconds.
Default	Different per sample	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # stats sample temperature interval 1`
	`switch (config) # show stats sample temperature`
	`Sample "temperature" (Modules temperature):`
	`  Enabled:  yes`
	`  Sampling interval: 1 second`
	`switch (config) #`	

Related Commands	show stats sample	
Note		

stats clear-all

stats clear all

Clears data for all samples, CHDs, and status for all alarms.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	`switch (config) # stats clear-all` `switch (config) #`
Related Commands	N/A
Note	

stats export

stats export <format> <report name> [{after | before} <yyyy/mm/dd> <hh:mm:ss>] [filename <filename>]

Exports statistics to a file.

Syntax Description	format	Currently the only supported value for <format> is “csv” (comma-separated value).
	report name	Determines dataset to be exported. Possible report names are: • memory - Memory utilization • paging - Paging I/O • cpu_util - CPU utilization
	after | before	Only includes stats collected after or before a specific time.
	yyyy/mm/dd	Date: It must be between 1970/01/01 and 2038/01/19.
	hh:mm:ss	Time: It must be between 00:00:00 and 03:14:07 UTC and is treated as local time.
	filename	Specifies filename to give new report. If a filename is specified, the stats will be exported to a file of that name; otherwise a name will be chosen automatically and will contain the name of the report and the time and date of the export. Any automatically-chosen name will be given a .csv extension.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # stats export csv memory filename mellanoxexample before 2000/08/14 15:59:50 after 2000/08/14 15:01:50`
	`Generated report file: mellanoxexample.csv`
	`switch (config) # show files stats`
	`mellanoxexample.csv`
	`switch (config) #`	

Related Commands	show files stats	
Note		

show stats alarm

show stats alarm [<Alarm ID> [rate-limit]]

Displays status of all alarms or the specified alarm.

Syntax Description	Alarm ID	May be: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
	rate-limit	Displays rate limit parameters.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show stats alarm`
	`Alarm cpu_util_indiv (Average CPU utilization too high):  ok`
	`Alarm disk_io (Operating System Disk I/O per second too high): (disabled)`
	`Alarm fs_mnt (Free filesystem space too low):  ok`
	`Alarm intf_util (Network utilization too high):  (disabled)`
	`Alarm memory_pct_used (Too much memory in use):  (disabled)`
	`Alarm paging (Paging activity too high):  ok`
	`Alarm temperature (Temperature is too high):  ok`
	`switch (config) #`	

Related Commands	stats alarm	
Note		

show stats chd

show stats chd [<CHD ID>]

Displays configuration of all statistics CHDs.

Syntax Description	CHD ID	May be: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show stats chd disk_device_io_hour`
	
	`CHD "disk_device_io_hour" (Storage device I/O read/write statistics for the last`
	` hour: bytes):`
	`  Enabled:  yes`
	`  Source dataset:  sample "disk_device_io"`
	`  Computation basis: data points`
	`  Interval:  1 data point(s)`
	`  Range:  1 data point(s)`
	`switch (config) #`	

Related Commands	stats chd	
Note		

show stats cpu

show stats cpu

Displays some basic stats about CPU utilization:
- the current level
- the peak over the past hour
- the average over the past hour

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # show stats cpu`
	
	`CPU 0`
	`  Utilization:  6%`
	`  Peak Utilization Last Hour: 16% at 2012/02/28 08:47:32`
	`  Avg. Utilization Last Hour: 8%`
	`switch (config) #`

Related Commands	N/A
Note	

show stats sample

show stats sample [<sample ID>]

Displays sampling interval for all samples, or the specified one.

Syntax Description	sample ID	Possible sample IDs are: • congested • cpu_util - CPU utilization: milliseconds of time spent • disk_device_io - Storage device I/O statistics • disk_io - Operating system aggregate disk I/O: KB/sec • eth • fan - Fan speed • fs_mnt_bytes - Filesystem usage: bytes • fs_mnt_inodes - Filesystem usage: inodes • ib • interface - Network interface statistics • intf_util - Network interface utilization: bytes • memory - System memory utilization: bytes • paging - Paging activity: page faults • power - Power supply usage • power-consumption • temperature - Modules temperature
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show stats sample fan`
	`Sample "fan" (Fan speed):`
	`  Enabled:  yes`
	`  Sampling interval: 1 minute 11 seconds`
	`switch (config) #`	

Related Commands	N/A	
Note		

4.12.2 Power Management

4.12.2.1 Width Reduction Power Saving

Link width reduction (LWR) is a Mellanox proprietary power saving feature to be utilized to economize the power usage of the fabric. LWR may be used to manually or automatically configure a certain connection between Mellanox switch systems to lower the width of a link from 4X operation to 1X based on the traffic flow.

LWR is relevant only for 40GbE and InfiniBand FDR speeds in which the links are operational at a 4X width.

When “show interfaces” is used, a port’s speed appears unchanged even when only one lane is active.

LWR has three operating modes per interface:

- Disabled – LWR does not operate and the link remains in 4X under all circumstances.
- Automatic – the link automatically alternates between 4X and 1X based on traffic flow.
- Force – a port is forced to operate in 1X mode lowering the throughput capability of the port. This mode should be chosen in cases where constant low throughput is expected on the port for a certain time period – after which the port should be configured to one of the other two modes, to allow higher throughput to pass through the port.

See command “power-management width” on page 319.

Table 20 - LWR Configuration Behavior

Switch-A Configuration	Switch-B Configuration	Behavior
Disable	Disable	LWR is disabled.
Disable	Force	Transmission from Switch-B to Switch-A operates at 1X. On the opposite direction, LWR is disabled.
Disable	Auto	Depending on traffic flow, transmission from Switch-B to Switch-A may operate at 1X. On the opposite direction, LWR is disabled.
Auto	Force	Transmission from Switch-B to Switch-A operates at 1 lane. Transmission from Switch-A to Switch-B may operate at 1X depending on the traffic.
Auto	Auto	Width of the connection depends on the traffic flow
Force	Force	Connection between the switches operates at 1X

4.12.3 System Reboot

4.12.3.1 Rebooting 1U Switches

➢ ***To reboot a 1U switch system:***

Step 1. Enter Config mode. Run:

```
switch >
switch > enable
switch # configure terminal
```

Step 2. Reboot the system. Run:

```
switch (config) # reload
```

4.12.4 Commands

4.12.4.1 Chassis Management

clear counters

clear counters [all | interface <type> <number>]

Clears switch counters.

Syntax Description	all	Clears all switch counters.
	type	A specific interface type
	number	The interface number.
Default	N/A	
Configuration Mode	Config Interface Port Channel	
History	3.2.3000	
Role	admin	
Example	`switch (config) # clear counters` `switch (config) #`	
Related Commands		
Note		

health

health {max-report-len <length> | re-notif-cntr <counter> | report-clear}

Configures health daemon settings.

Syntax Description	max-report-len <length>	Sets the length of the health report - number of line entries. Possible values: 10-2048.
	re-notif-cntr <counter>	Health control changes notification counter, in seconds. Possible values: 120-7200 seconds.
	report-clear	Clears the health report.
Default	max-report-len: 50 re-notif-cntr:	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # health re-notif-cntr 125` `switch (config) #`	
Related Commands	show health-report	
Note		

power enable

power enable <module name>
no power enable <module name>

Powers on the module.
The no form of the command shuts down the module.

Syntax Description	module name	Enables power for selected module.
Default	Power is enabled on all modules.	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # power enable L01` `switch (config) #`	
Related Commands	show power show power consumers	
Note	This command is not applicable for 1U systems.	

power-management width

power-management width {auto | force}
no power-management width

Sets the width of the interface to be automatically adjusted.
The no form of the command disables power-saving.

Syntax Description	auto	Allows the system to automatically decide whether to work in power-saving mode or not.
	force	Forces power-saving mode on the port.
Default	Disabled	
Configuration Mode	Config Interface Ethernet	
History	3.3.4000	
Role	admin	
Example	`switch (config interface ib 1/1) # power-management width auto` `switch (config) #`	
Related Commands	show interface	
Note		

usb eject

usb eject

Gracefully turns off the USB interface.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	`switch (config) # usb eject` `switch (config) #`
Related Commands	N/A
Note	Applicable only for systems with USB interface.

show fan

show fan

Displays fans status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show fan`
	`switch (config) # show fan`
	`==========`
	`Module Device Fan Speed Status`
	`(RPM)`
	`==========`
	`FAN FAN F1 5340.00 OK`
	`FAN FAN F2 5340.00 OK`
	`FAN FAN F3 5640.00 OK`
	`FAN FAN F4 5640.00 OK`
	`PS1 FAN F1 5730.00 OK`
	`PS2 FAN - - NOT PRESENT`
	`switch (config) #`

Related Commands	N/A
Note	

show version

show version [concise]

Displays version information for the currently running system image.

Syntax Description	concise	The concise variant fits the description onto one line.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show version`
	`Product name:  SX_PPC_M460EX`
	`Product release:  3.0.0000-dev-HA`
	`Build ID:  #1-dev`
	`Build date:  2012-02-26 08:47:51`
	`Target arch:  ppc`
	`Target hw:  m460ex`
	`Built by:  root@r-fit16`
	
	`Uptime:  1d 3h 32m 24.656s`
	
	`Product model:  ppc`
	`Host ID:  0002c911a15e`
	`System memory:  110 MB used / 1917 MB free / 2027 MB total`
	`Swap:  0 MB used / 0 MB free / 0 MB total`
	`Number of CPUs:  1`
	`CPU load averages: 0.18 / 0.19 / 0.16`
	`switch (config) #`	

Related Commands	N/A	
Note		

show uboot

show uboot

Displays u-boot version.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.5006
Role	admin

Example	`switch (config) # show uboot`
	`UBOOT version : U-Boot 2009.01 SX_PPC_M460EX SX_3.2.0330-82 ppc (Dec 20 2012)`
	`switch (config) #`

Related Commands	N/A
Note	

show cpld

show cpld

Displays status of all CPLDs in the system.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000 3.3.4302 Updated example
Role	admin

Example	`switch (config) # show cpld`
	`==================================`
	`Name Type Version`
	`==================================`
	`Cpld1 CPLD_TOR 4`
	`Cpld2 CPLD_PORT1 2`
	`Cpld3 CPLD_PORT2 2`
	`Cpld4 CPLD_MEZZ 3`
	`switch (config) #`

Related Commands	N/A
Note	

show inventory

show inventory

Displays system inventory.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show inventory`
	`==========================================================================`
	`Module Type Part number Serial Number Asic revision`
	`==========================================================================`
	`CHASSIS SX1036 MSX1036B-1SFR MT1205X01549 N/A`
	`MGMT SX1036 MSX1036B-1SFR MT1205X01549 0`
	`FAN SXX0XX_FAN MSX60-FF MT1206X07209 N/A`
	`PS1 SXX0XX_PS MSX60-PF MT1206X06697 N/A`
	`CPU CPU SA000203-B MT1220X01231 N/A`
	`switch (config) #`

Related Commands	N/A
Note	

show module

show module

Displays modules status.

Syntax Description	N/A	
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	First version
	3.3.0000	Added “Is Fatal” column
Role	admin	

Example	`switch (config) # show module`
	`==================================================`
	` Module   Type               Present Power Is Fatal`
	`==================================================`
	` MGMT     SX1036             1       N/A   Not Fatal`
	` FAN      SXX0XX_FAN         1       N/A   Not Fatal`
	` PS1      SXX0XX_PS          1       N/A   Not Fatal`
	` PS2      SXX0XX_PS          0       N/A   Not Fatal`
	` CPU      CPU                1       N/A   Not Fatal`
	`switch (config) #`	

Related Commands	N/A	
Note		

show memory

show memory

Displays memory status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show memory`
	`Total Used Free Used+B/C Free-B/C`
	`Physical 2027 MB 761 MB 1266 MB 1214 MB 813 MB`
	`Swap 0 MB 0 MB 0 MB`
	
	`Physical Memory Borrowed for System Buffers and Cache:`
	`Buffers: 0 MB`
	`Cache: 452 MB`
	`Total Buffers/Cache: 452 MB`
	`switch (config) #`

Related Commands	N/A
Note	

show asic-version

show asic-version

Displays firmware ASIC version.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show asic-version`
	`==========================`
	`SX module Version`
	`==========================`
	`SX 9.1.1260`
	`switch (config) #`

Related Commands	N/A
Note	

show power

show power

Displays power supplies and power usage.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	

```
switch (config) # show power
================================================================
Module         Power    Voltage  Current  Capacity  Grid   Status
               (Watts)           (Amp)    (Watts)   Group
================================================================
PS1            0.00     47.11    0.00     1008      A      OK
PS2            248.82   48.05    5.18     1008      A      OK
PS3            0.00     46.88    0.00     1008      A      OK
PS4            -        -        -        NOT PRESENT
PS5            46.72    47.82    0.98     1008      A      OK
PS6            -        -        -        NOT PRESENT
PS7            -        -        -        NOT PRESENT
PS8            -        -        -        NOT PRESENT
PS9            -        -        -        NOT PRESENT
PS10           -        -        -        NOT PRESENT

Total power used : 295.54 W
Total power capacity : 4032.00 W
Total power budget : 4032.00 W
Total power available : 3736.46 W
Redundancy mode: combined
Redundancy status: OK
switch (config) #
```

Related Commands	N/A
Note	

show power consumers

show power consumers

Displays power consumers.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	

```
switch (config) # show power consumers
================================================
Module         Power    Voltage  Current  Status
               (Watts)           (Amp)
================================================
MGMT           17.47    48.00    0.36     OK
S01            33.26    48.00    0.69     OK
S02            33.50    48.00    0.70     OK
L01            31.73    48.00    0.66     OK
L02            29.76    48.00    0.62     OK
L30            28.61    48.00    0.60     OK
FAN5           14.91    48.00    0.31     OK
FAN2           13.70    48.00    0.29     OK
FAN1           14.21    48.00    0.30     OK
FAN6           15.10    48.00    0.31     OK
FAN4           14.53    48.00    0.30     OK
FAN7           15.04    48.00    0.31     OK
FAN3           15.17    48.00    0.32     OK
FAN8           14.98    48.00    0.31     OK

Total power used : 291.97 W
Max power : 1636.00 W
switch (config) #
```

Related Commands	N/A
Note	

show temperature

show temperature

Displays the system's temperature sensors status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show temperature`
	`==================================================`
	`Module  Component             Reg  CurTemp   Status`
	`                                    (Celsius)`
	`==================================================`
	`MGMT    BOARD_MONITOR         T1   25.00     OK`
	`MGMT    CPU_BOARD_MONITOR     T1   26.00     OK`
	`MGMT    CPU_BOARD_MONITOR     T2   41.00     OK`
	`MGMT    QSFP_TEMP1            T1   23.00     OK`
	`MGMT    QSFP_TEMP2            T1   22.50     OK`
	`MGMT    QSFP_TEMP3            T1   23.00     OK`
	`MGMT    SX                    T1   37.00     OK`
	`switch (config) #`

Related Commands	N/A
Note	

show voltage

show voltage

Displays power supplies voltage level.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000 3.3.5006 Updated Example
Role	admin
Example	switch (config) # show voltage ========== Module Power Meter Reg Expected Voltage Actual Voltage Status High Range Low Range ========== MGMT BOARD_MONITOR USB 5V sensor 5.00 5.15 OK 5.55 4.45 MGMT BOARD_MONITOR Asic I/O sensor 2.27 2.11 OK 2.55 1.99 MGMT BOARD_MONITOR 1.8V sensor 1.80 1.79 OK 2.03 1.57 MGMT BOARD_MONITOR SYS 3.3V sensor 3.30 3.28 OK 3.68 2.92 MGMT BOARD_MONITOR CPU 0.9V sensor 0.90 0.93 OK 1.04 0.76 MGMT BOARD_MONITOR 1.2V sensor 1.20 1.19 OK 1.37 1.03 MGMT CPU_BOARD_MONITOR 12V sensor 12.00 11.67 OK 13.25 10.75 MGMT CPU_BOARD_MONITOR 12V sensor 2.50 2.46 OK 2.80 2.20 MGMT CPU_BOARD_MONITOR 2.5V sensor 3.30 3.26 OK 3.68 2.92 MGMT CPU_BOARD_MONITOR SYS 3.3V sensor 3.30 3.24 OK 3.68 2.92 MGMT CPU_BOARD_MONITOR SYS 3.3V sensor 1.80 1.79 OK 2.03 1.57 MGMT CPU_BOARD_MONITOR 1.8V sensor 1.20 1.24 OK 1.37 1.03 switch (config) #
Related Commands	N/A
Note	

show health-report

	show health-report Displays health report.	
Syntax Description	N/A	
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	First version
	3.3.0000	Output update
Role	admin	

Example	`switch (config) # show health-report`
	`=======================`
	`| ALERTS CONFIGURATION |`
	`=======================`
	`Re-notification counter (sec):[3600]`
	`Report max counter:           [50]`
	`=======================`
	`|    HEALTH REPORT     |`
	`=======================`
	`No Health issues file`
	`switch (config) #`	

Related Commands	N/A	
Note		

show resources

show resources

Displays system resources.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show resources`
	`Total  Used  Free`
	`Physical  2027 MB  761 MB  1266 MB`
	`Swap  0 MB  0 MB  0 MB`
	
	`Number of CPUs:  1`
	`CPU load averages: 0.11 / 0.23 / 0.23`
	
	`CPU 1`
	`  Utilization:  5%`
	`  Peak Utilization Last Hour: 19% at 2012/02/15 13:26:19`
	`  Avg. Utilization Last Hour: 7%`
	`switch (config) #`

Related Commands	N/A
Note	

show system profile

show system profile

Displays system profile.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0000
Role	admin

Example	`switch (config) # show system profile`
	`eth-single-switch`
	`switch (config) #`

Related Commands	system profile
Note	

show system capabilities

show system capabilities

Displays system capabilities.

Syntax Description	N/A	
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	First version
	3.3.0000	Added gateway support
Role	admin	

Example	`switch (config) # show system capabilities`
	`IB: Supported`
	`Ethernet: Supported, Full L2`
	`GW: Supported`
	`Max number of GW ports: 0`
	`Max SM nodes: 648`
	`IB Max licensed speed: FDR`
	`Ethernet Max licensed speed: 56Gb`
	
	`switch (config) #`	

Related Commands	show system profile	
Note		

show system mac

show system mac

Displays system MAC address.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config) # show system mac`
	`00:02:C9:5E:AF:18`
	`switch (config) #`

Related Commands	N/A
Note	

show protocols

show protocols

Displays all protocols enabled in the system.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.3000 3.3.4550 Updated output
Role	admin

Example	`switch (config) # show protocols`
	
	`Ethernet enabled`
	`spanning-tree rstp`
	`lacp disabled`
	`lldp enabled`
	`igmp-snooping disabled`
	`ets enabled`
	`priority-flow-control disabled`
	`sflow disabled`
	`openflow enabled`
	
	`IP routing disabled`
	`ospf disabled`
	`dhcp-relay disabled`
	
	`Infiniband enabled`
	`sm enabled`
	`switch (config) #`

Related Commands	N/A
Note	

4.13 Network Management Interfaces

4.13.1 XML API

MLNX-OS XML API is currently under development. For further information please contact Mellanox support.

4.13.2 Commands

4.13.2.1 SNMP

The commands in this section are used to manage the SNMP server.

snmp-server auto-refresh

snmp-server auto-refresh {enable | interval}
no snmp-server auto-refresh enable

Configures SNMPD refresh settings.
The no form of the command disables SNMPD refresh mechanism.

Syntax Description	enable	Enables SNMPD refresh mechanism.
	interval	Sets SNMPD refresh interval.
Default	Enabled. Interval: 60 secs	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch(config) # snmp-server community private rw`
	`switch (config) # show snmp`
	`SNMP enabled:  yes`
	`SNMP port:  161`
	`System contact:`
	`System location:`
	`Read-only community:  public`
	`Read-write community: private`
	
	`Interface listen enabled: yes`
	`No Listen Interfaces.`
	
	`Traps enabled:  yes`
	`Default trap community:  public`
	`Default trap port:  162`
	
	`No trap sinks configured.`
	`switch(config) #`	

Related Commands	show snmp	
Note	•	

snmp-server community

snmp-server community <community> [ro | rw]
no snmp-server community <community>

Sets a community name for either read-only or read-write SNMP requests.
The no form of the command sets the community string to default.

Syntax Description	community	Community name.
	ro	Sets the read-only community string.
	rw	Sets the read-write community string.
Default	Read-only community: “public” Read-write community: “”	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch(config) # snmp-server community private rw`
	`switch (config) # show snmp`
	`SNMP enabled: yes`
	`SNMP port: 161`
	`System contact:`
	`System location:`
	`Read-only community: public`
	`Read-write community: private`
	
	`Interface listen enabled: yes`
	`No Listen Interfaces.`
	
	`Traps enabled: yes`
	`Default trap community: public`
	`Default trap port: 162`
	
	`No trap sinks configured.`
	`switch(config) #`	

Related Commands	show snmp	
Note	• If neither the “ro” or the “rw” parameters are specified, the read-only community is set as the default community • If the read-only community is specified, only queries can be performed • If the read-write community is specified, both queries and sets can be performed	

snmp-server contact

snmp-server contact <contact name>
no snmp-server contact

Sets a value for the sysContact variable in MIB-II.
The no form of the command resets the parameter to its default value.

Syntax Description	contact name	Contact name.
Default	“”	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # snmp-server contact my-name`
	`switch (config) # show snmp`
	`SNMP enabled:  yes`
	`SNMP port:  161`
	`System contact:  my-name`
	`System location:`
	`Read-only community:  public`
	`Read-write community: private`
	
	`Interface listen enabled: yes`
	`No Listen Interfaces.`
	
	`Traps enabled:  yes`
	`Default trap community:  public`
	`Default trap port:  162`
	
	`No trap sinks configured.`
	`switch (config) #`	

Related Commands	show snmp	
Note		

snmp-server enable

snmp-server enable [communities | mult-communities | notify]
no snmp-server enable [communities | mult-communities | notify]

Enables SNMP-related functionality.
The no form of the command disables the SNMP server.

Syntax Description	enable	Enables SNMP-related functionality: • SNMP engine • SNMP traps
	communities	Enables community-based authentication on this system.
	mult-communities	Enables multiple communities to be configured.
	notify	Enables sending of SNMP traps and informs from this system.
Default	SNMP is enabled by default SNMP server communities are enabled by default SNMP notifies are enabled by default SNMP server multi-communities are disabled by default	
Configuration Mode	Config	
History	3.1.0000	First version
	3.2.1050	Change traps to notify
Role	admin	

Example

```
switch (config) # snmp-server enable
switch (config) # show snmp
SNMP enabled:         yes
SNMP port:            161
System contact:       my-name
System location:
Read-only community:  public
Read-write community: private

Interface listen enabled: yes
No Listen Interfaces.

Traps enabled:            yes
Default trap community:   public
Default trap port:        162

No trap sinks configured.
switch (config) #
```

Related Commands	show snmp
Note	SNMP traps are only sent if there are trap sinks configured with the “snmp-server host...” command, and if these trap sinks are themselves enabled.

snmp-server host

snmp-server host <IP address> {disable | {traps | informs} [<community> | <port> | version <snmp version>]}
no snmp-server host <IPv4 or IPv6 address> {disable | {traps| informs} [<community> | <port>]}

Configures hosts to which to send SNMP traps.
The no form of the commands removes a host from which SNMP traps should be sent.

Syntax Description	IP address	IPv4 or IPv6 address.
	disable	Temporarily disables sending of traps to this host.
	community	Specifies trap community string.
	port	Overrides default UDP port for this trap sink.
	snmp version	Specifies the SNMP version of traps to send to this host.
Default	No hosts are configured Default community is “public” Default UDP port is 162 Default SNMP version is 2c	
Configuration Mode	Config	
History	3.1.0000	First version
	3.2.1050	Add inform option
Role	admin	

Example

```
switch (config) # snmp-server host 10.10.10.10 traps version 1
switch (config) # show snmp
SNMP enabled:         yes
SNMP port:            161
System contact:
System location:

Read-only communities:
   public

Read-write communities:
   (none)

Interface listen enabled: yes
No Listen Interfaces.

Traps enabled:            yes
Default trap community:   public
Default trap port:        162

Trap sinks:
   10.10.10.10
      Enabled: yes
      Type: traps version 1
      Port: 162 (default)
      Community: public (default)
switch (config) #
```

Related Commands

show snmp
snmp-server enable

Note

This setting is only meaningful if traps are enabled, though the list of hosts may still be edited if traps are disabled. Refer to “snmp-server enable” command.

snmp-server listen

snmp-server listen {enable | interface <ifName>}
no snmp-server listen {enable | interface <ifName> }

Configures SNMP server interface access restrictions.
The no form of the command disables the listen interface restricted list for SNMP server.

Syntax Description	enable	Enables SNMP interface restrictions on access to this system.
	ifName	Adds an interface to the “listen” list for SNMP server. For example: “mgmt0”, “mgmt1”.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # snmp listen enable
switch (config) # show snmp
SNMP enabled:         yes
SNMP port:            161
System contact:
System location:
Read-only community:  public
Read-write community: private

Interface listen enabled: yes
No Listen Interfaces.

Traps enabled:            yes
Default trap community:   public
Default trap port:        162

Trap sinks:
   10.10.10.10
      Enabled: yes
      Type: traps version 1
      Port: 3
      Community: public (default)
switch (config) #
```

Related Commands	show snmp
Note	If enabled, and if at least one of the interfaces listed is eligible to be a listen interface, then SNMP requests will only be accepted on those interfaces. Otherwise, SNMP requests are accepted on any interface.

snmp-server location

snmp-server location <system location>
no snmp-server location

Sets a value for the sysLocation variable in MIB-II.
The no form of the command clears the contents of the sysLocation variable.

Syntax Description	system location String.
Default	“”
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # snmp-server location lab`
	`switch (config) # show snmp`
	`SNMP enabled: yes`
	`SNMP port: 161`
	`System contact: my-name`
	`System location: lab`
	`Read-only community: public`
	`Read-write community: private`
	
	`Interface listen enabled: yes`
	`No Listen Interfaces.`
	
	`Traps enabled: yes`
	`Default trap community: public`
	`Default trap port: 162`
	
	`No trap sinks configured.`
	`switch (config) #`

Related Commands	show snmp
Note	

snmp-server notify

snmp-server notify {community <community> | event <event name> | port <port> | send-test}
no snmp-server notify {community | event <event name> | port}

Configures SNMP notifications (traps and informs).
The no form of the commands negate the SNMP notifications.

Syntax Description	community	Sets the default community for traps sent to hosts which do not have a custom community string set.
	event	Specifies which events will be sent as traps.
	port	Sets the default port to which traps are sent.
	send-test	Sends a test trap.
Default	Community: public All informs and traps are enabled Port: 162	
Configuration Mode	Config	
History	3.1.0000	First version
	3.2.1050	Changed traps to notify
Role	admin	

Example

```
switch (config) # snmp-server community public
switch (config) # show snmp
SNMP enabled:         yes
SNMP port:            1000
System contact:       my-name
System location:      lab
Read-only community:  public
Read-write community: private

Interface listen enabled: yes
No Listen Interfaces.

Traps enabled:            yes
Default trap community:   public
Default trap port:        162

No trap sinks configured.
switch (config) #
```

Related Commands

show snmp
show snmp events

Note

- This setting is only meaningful if traps are enabled, though the list of hosts may still be edited if traps are disabled
- Refer to Mellanox MIB file for the list of supported traps

snmp-server port

snmp-server port <port>
no snmp-server port

Sets the UDP listening port for the SNMP agent.
The no form of the command resets the parameter to its default value.

Syntax Description	port	UDP port.
Default	161	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # snmp-server port 1000`
	`switch (config) # show snmp`
	`SNMP enabled:  yes`
	`SNMP port:  1000`
	`System contact:  my-name`
	`System location:  lab`
	`Read-only community:  public`
	`Read-write community: private`
	
	`Interface listen enabled: yes`
	`No Listen Interfaces.`
	
	`Traps enabled:  yes`
	`Default trap community:  public`
	`Default trap port:  162`
	
	`No trap sinks configured.`
	`switch (config) #`	

Related Commands	show snmp	
Note		

snmp-server user

snmp-server user {admin | <username>} v3 {[encrypted] auth <hash-type> <password> [priv <privacy-type> [<password>]] | capability <cap> | enable <sets> | prompt auth <hash-type> [priv <privacy-type>]}
no snmp-server user {admin | <username> } v3 {[encrypted] auth <hash-type> <password> [priv <privacy-type> [<password>]] | capability <cap> | enable <sets> | prompt auth <hash-type> [priv <privacy-type>]}

Specifies an existing username, or a new one to be added.
The no form of the command disables access via SNMP v3 for the specified user.

Syntax Description	v3	Configures SNMP v3 users.
	auth	Configures SNMP v3 security parameters, specifying passwords in plaintext on the command line (note: passwords are always stored encrypted).
	capability	Sets capability level for SET requests.
	enable	Enables SNMP v3 access for this user.
	encrypted	Configures SNMP v3 security parameters, specifying passwords in encrypted form.
	prompt	Configures SNMP v3 security parameters, specifying passwords securely in follow-up prompts, rather than on the command line.
Default	No SNMP v3 users defined	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # snmp-server user admin v3 enable`
	`switch (config) # show snmp user`
	`User name: admin`
	`   Enabled overall:         yes`
	`   Authentication type:     sha`
	`   Privacy type:            aes-128`
	`   Authentication password: (NOT SET; user disabled)`
	`   Privacy password:        (NOT SET; user disabled)`
	`   SET access:`
	`      Enabled:              yes`
	`      Capability level:     admin`
	`switch (config) #`	

Related Commands	show snmp user	
Note		

show snmp

show snmp [auto-refresh | engineID | events | host | user]

Displays SNMP-server configuration and status.

Syntax Description	auto-refresh	SNMP refreshed mechanism status.
	engineID	SNMP Engine ID.
	events	SNMP events.
	host	List of notification sinks.
	user	SNMP users.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show snmp user`
	`User name: Hendrix`
	`  Enabled overall:  yes`
	`  Authentication type:  sha`
	`  Privacy type:  des`
	`  Authentication password: (set)`
	`  Privacy password:  (set)`
	`  Require privacy: yes`
	`  SET access:`
	`  Enabled:  yes`
	`  Capability level:  admin`
	`switch (config) #`	

Related Commands	show snmp	
Note		

show snmp auto-refresh

show snmp auto-refresh

Displays SNMPD refresh mechanism status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch(config) # show snmp auto-refresh`
	`=================`
	`SNMP auto refresh`
	`=================`
	`Auto-refresh enabled:  yes`
	`Refresh interval (sec):  60`
	
	`=====================`
	`Auto-Refreshed tables`
	`=====================`
	`entPhysicalTable`
	`ifTable`
	`ifXTable`
	
	`switch(config) #`

Related Commands	snmp-server auto-refresh
Note	

4.13.2.2 XML API

xml-gw enable

xml-gw enable
no xml-gw enable

Enables the XML gateway.
The no form of the command disables the XML gateway.

Syntax Description	N/A
Default	XML Gateway is enabled
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # xml-gw enable`
	`switch (config) # show xml-gw`
	`XML Gateway enabled:  yes`
	`switch (config) #`

Related Commands	show xml-gw
Note	

show xml-gw

show xml-gw

Displays the XML gateway setting.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # show xml-gw`
	`XML Gateway enabled:  yes`
	`switch (config) #`

Related Commands	xml-gw enable
Note	

5 Ethernet Switching

5.1 Interface

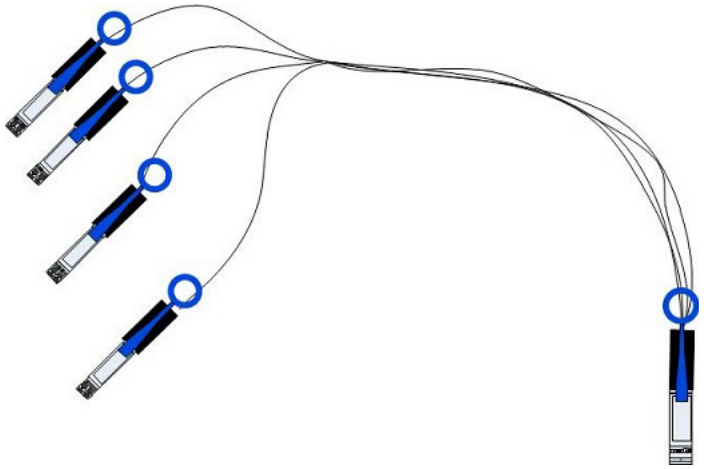
Interface Ethernet have the following physical set of configurable parameters

- Admin state – enabling or disabling the interface.
- Flow control – admin state per direction (send or receive)
- MTU (Maximum Transmission Unit) – 1518-9216 bytes
- Speed – 1/10/40/56GbE (depends on the interface type and system)
- Description – user defined string
- Module-type – the type of the module plugged in the interface

5.1.1 Break-Out Cables

The break-out cable is a unique Mellanox capability, where a single physical 40Gbps port is divided into 2x10Gbps or 4x10Gbps ports. It maximizes the flexibility of the end user to use the Mellanox switch with a combination of 10Gbps and 40Gbps interfaces according to the specific requirements of its network. Certain ports cannot be split at all and there are ports which can be split into 2 ports only. Splitting a port changes the notation of that port from x/y to x/y/z with “x/y” indicating the previous notation of the port prior to the split and “z” indicating the number of the resulting 10G port (1,2 or 1,2,3,4). Each sub-physical port is then handled as an individual port. For example: splitting port 20 into 4 will give the following new ports: 1/20/1, 1/20/2, 1/20/3, 1/20/4.

Figure 10: Break-Out Cable



A split-4 operation results in blocking a 40G port in addition to the one being split. A set of hardware restrictions determine which of the ports can be split.

Specific ports can be split by using a QSFP 1X4 breakout cable to split one 40 Gb/s port into 4 lanes (4 SFP+ connectors). These 4 lanes then go, one lane to each of the 4 SFP+ connectors. Some ports can be split into 2 10 Gb/s ports, using lanes 1 and 2 only. When a QSFP port is split

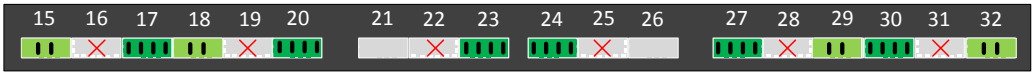
into 2 10Gb/s ports then only SFP+ connectors #1 and #2 are used. Connectors #3 and #4 are left unconnected.

Splitting the interface deletes all configuration on that interface.

When splitting an interface's traffic into 4-10Gb/s data streams (four lanes) one of the other ports on the switch must be disabled (unmapped).

- some ports can be split into 4
- some ports can be split into 2
- some ports become unmapped due to a 1X4 split

Figure 11: Port Splitting Options



This port can be split into 4 10Gb/s SFP+

This port can be split into 2 10Gb/s SFP+

This port is unmapped by the neighboring split 4 port

The maximum number of 10 Gb/s Ethernet ports configurable with this switch is 34.

Table 21 - Port Splitting Options

Port #	Can be split to 4	Turns off port #	Can be split to 2	Port #	Can be split to 4	Turns off port #	Can be split to 2
15	—		YES	24	YES	25	—
16	—		—	25	—		—
17	YES	16	—	26	—		—
18	—		YES	27	YES	28	—
19	—		—	28			—
20	YES	19	—	29			YES
21	—		—	30	YES	31	—
22	—		—	31	—		—
23	YES	22	—	32	—		YES

To see the exact splitting options available per system, refer to each specific system's hardware user manual (Cabling chapter) located on the Mellanox website.

5.1.1.1 Changing the Module Type to a Split Mode

➢ ***To split an interface:***

Step 1. Shut down all the ports related to the interface. Run:

- in case of split-2, shut down the current interface only
- in case of split-4, shut down the current interface and the other interface according to the table above

```
switch (config) # interface ethernet 1/19
switch (config interface ethernet 1/19) # shutdown
switch (config interface ethernet 1/19) # exit
switch (config) # interface ethernet 1/20
switch (config interface ethernet 1/20) # shutdown
```

Step 2. Split the ports as desired. Run:

```
switch (config interface ethernet 1/20) # module-type qsfp-split-4
switch (config interface ethernet 1/20) #
```

Step 3. The following warning will be displayed:
`the following interfaces will be unmapped: 1/20 1/19.`
Choose `Yes` when prompted `Type 'yes' to confirm split`

The `<ports>` field in the warning refers to the affected ports from splitting port `<inf>` in the applied command.

Please beware that splitting a port into 4 prevents you from accessing the splittable port, and an additional one. For example, in the procedure above, ports 19 and 20 become unaccessible.

5.1.1.2 Unsplitting a Split Port

➢ ***To unsplit a split port:***

Step 1. Shut down all of the split ports. Run:

```
switch (config interface ethernet 1/20/4) # shutdown
switch (config interface ethernet 1/20/4) # exit
switch (config) # interface ethernet 1/20/3
switch (config interface ethernet 1/20/3) # shutdown
switch (config interface ethernet 1/20/3) # exit
switch (config) # interface ethernet 1/20/2
switch (config interface ethernet 1/20/2) # shutdown
switch (config interface ethernet 1/20/2) # exit
switch (config) # interface ethernet 1/20/1
switch (config interface ethernet 1/20/1) # shutdown
```

Step 2. From the first member of the split (1/20/1), change the module-type back to QSFP. Run:

```
switch (config interface ethernet 1/20/1) # module-type qsfp
```

The module-type can be changed **only** from the first member of the split and **not** from the interface that was split.

The following warning will be displayed:
`The following interfaces will be unmapped: 1/20/1 1/20/2 1/20/3 1/20/4.`

Step 3. Type “`yes`” when prompted “`Type 'yes' to confirm unsplit`.”

5.1.2 Transceiver Information

MLNX-OS offers the option of viewing the transceiver information of a module or cable connected to a specific interface. The information is a set of read-only parameters burned onto the EEPROM of the transceiver by the manufacture. The parameters include identifier (connector type), cable type, speed and additional inventory attributes.

➢ ***To display transceiver information of a specific interface, run:***

```
switch (config) # show interfaces ethernet 1/20 transceiver
Port 1/60 state
        identifier             : QSFP+
        cable/ module type     : Passive copper, unequalized
        ethernet speed and type: 56GigE
        vendor                 : Mellanox
        cable length           : 1m
        part number            : MC2207130-001
        revision               : A3
        serial number          : MT1238VS04936
switch (config) #
```

The indicated cable length is rounded up to the nearest natural number.

5.1.3 Commands

interface ethernet

interface ethernet <slot>/<port>[/<subport>]-[<slot>/<port>[/<subport>]]

Enters the Ethernet interface or Ethernet interface range configuration mode.

Syntax Description	<slot>/<port>	Ethernet port number.
	subport	Ethernet subport number. to be used in case of split port.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	First version
	3.2.1100	Added range support
Role	admin	

Example	`switch (config) # interface ethernet 1/1`
	`switch (config interface ethernet 1/1) # exit`
	`switch (config) # interface ethernet 1/1-1/10`
	`switch (config interface ethernet 1/1-1/10) #`	

Related Commands	show interfaces ethernet	
Note		

flowcontrol

flowcontrol {receive | send} {off | on} [force]

Enables or disables IEEE 802.3x link-level flow control per direction for the specified interface.

Syntax Description	receive | send	receive - ingresses direction send - egresses direction
	off | on	on - enables IEEE 802.3x link-level flow control for the specified interface on receive or send. off - disables IEEE 802.3x link-level flow control for the specified interface on receive or send
	force	Forces command implementation.
Default	receive off, send off	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.0000	
Role	admin	
Example	`switch (config interface ethernet 1/1) # flowcontrol receive off` `switch (config interface ethernet 1/1) #`	
Related Commands	show interfaces ethernet	
Note	N/A	

mtu

mtu <frame-size>

Configures the Maximum Transmission Unit (MTU) frame size for the interface.

Syntax Description	frame-size	This value may be 1518-9216 bytes.
Default	1522 bytes	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.0000	
Role	admin	
Example	`switch (config interface ethernet 1/1) # mtu 9216` `switch (config interface ethernet 1/1) #`	
Related Commands	show interfaces ethernet	
Note		

shutdown

	shutdown **no shutdown** Disables the interface. The no form of the command enables the interface.
Syntax Description	N/A
Default	The interface is enabled.
Configuration Mode	Config Interface Ethernet Config Interface Port Channel
History	3.1.0000
Role	admin
Example	`switch (config interface ethernet 1/1) # shutdown` `switch (config interface ethernet 1/1) #`
Related Commands	show interfaces ethernet
Note	

description

description <string>
no description

Sets an interface description.
The no form of the command returns the interface description to its default value.

Syntax Description	string	40 bytes
Default	“”	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.0000	
Role	admin	
Example	`switch (config interface ethernet 1/1) # description my-interface` `switch (config interface ethernet 1/1) #`	
Related Commands	show interfaces ethernet	
Note		

speed

speed <port speed> [force]
no speed

Sets the speed of the interface.
The no form of the command sets the speed of the interface to its default value.

Syntax Description	port speed	1000 - 1GbE 10000 - 10GbE 40000 - 40GbE auto - auto negotiates link speed
	force	force changing the speed.
Default	Depends on the port module type, see the “Notes” section below.	
Configuration Mode	Config Interface Ethernet	
History	3.1.0000	
	3.3.3500	Added auto negotiation option
Role	admin	
Example	`switch (config interface ethernet 1/1) # speed 40000` `switch (config interface ethernet 1/1) #`	
Related Commands	show interfaces ethernet	
Note	• 56Gbps port speed requires a license (LIC-6036F-56GE) • The default speed depends on the interface capabilities, interface capable with 40Gbps will have 40Gbps speed by default • Not all interfaces support all speed options	

load-interval

load-interval <time>
no load-interval

Sets the interface counter interval.
The no form of the command resets the interval to its default value.

Syntax Description	time	In seconds.
Default	300 seconds.	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.3.0000	
Role	admin	
Example	`switch (config interface ethernet 1/1) # load-interval 30` `switch (config interface ethernet 1/1) #`	
Related Commands	show interfaces ethernet	
Note	This interval is used for the ingress rate and egress rate counters.	

clear counters

clear counters

Clears the interface counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config Interface Ethernet Config Interface Port Channel
History	3.1.0000
Role	admin
Example	`switch (config interface ethernet 1/1) # clear counters` `switch (config interface ethernet 1/1) #`
Related Commands	show interfaces ethernet
Note	

show interfaces ethernet

show interfaces ethernet <inf> [counters [priority]]

Displays the configuration and status for the interface.

Syntax Description	inf	Interface number: <slot>/<port>.
	counters	Displays interface extended counters.
	priority	Displays interface extended counters, per priority (0-7).
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	
Example		

```
switch (config) # show interfaces ethernet 1/1

Eth1/1

Admin state: Enabled
  Operational state: Up
  Description: N\A
  Mac address: 00:02:c9:71:ed:2d
  MTU: 1500 bytes(Maximum packet size 1522 bytes)
  Flow-control: receive off send off
  Actual speed: 40 Gbps
  Width reduction mode: Not supported
  Switchport mode: access
  Last clearing of "show interface" counters 00:20:39
  60 seconds Ingress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec
  60 seconds Egress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec

Rx
  0                   packets
  0                   unicast packets
  0                   multicast packets
  0                   broadcast packets
  0                   bytes
  0                   error packets
  0                   discard packets

Tx
  63                  packets
  0                   unicast packets
  63                  multicast packets
  0                   broadcast packets
  4032                bytes
  0                   discard packets

switch (config) #
```

Related Commands	
Note	

show interfaces ethernet [<inf>] capabilities

show interfaces ethernet [<inf>] capabilities

Displays the interface capabilities.

Syntax Description	inf	shows only one interface capabilities. Interface number: <slot>/<port>.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show interfaces ethernet 1/1 capabilities`
	`Eth1/1`
	`Speed       : 10000,40000`
	`FlowControl : Send, Receive`
	`switch (config) #`	

Related Commands		
Note		

show interfaces ethernet [<inf>] description

show interfaces ethernet [<inf>] description

Displays the admin status and protocol status for the specified interface.

Syntax Description	inf	Interface number: <slot>/<port>.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show interfaces ethernet 0/1 description`
	`Interface Status Protocol`
	`--------- ------ --------`
	`Ethernet 1/1 Enables up`
	`switch (config) #`	

Related Commands		
Note		

show interfaces ethernet [<inf>] status

show interfaces ethernet [<inf>] status

Displays the status, speed and negotiation mode of the specified interface.

Syntax Description	inf	Interface number: <slot>/<port>.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show interfaces ethernet status`
	
	`Port Operational state Speed Negotiation`
	
	`Eth1/1 Up 40 Gbps No-Negotiation`
	`Eth1/2 Up 10 Gbps No-Negotiation`
	`Eth1/3 Up 40 Gbps No-Negotiation`
	`...`
	`switch (config) #`	

Related Commands		
Note		

show interfaces ethernet [<inf>] transceiver

show interfaces ethernet [<inf>] transceiver

Displays the transceiver info.

Syntax Description	inf	interface number: <slot>/<port>
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show interfaces ethernet 1/1 transceiver`
	`Port 1/1 state`
	`identifier : QSFP+`
	`cable/ module type : Optical cable/ module`
	`ethernet speed and type: 40GBASE - SR4`
	`vendor : Mellanox`
	`cable_length : 50 m`
	`part number : MC2210411-SR4`
	`revision : A1`
	`serial number : TT1151-00006`
	`switch (config) #`	

Related Commands		
Note		

module-type

module-type <type> [force]

Splits or un-splits the interface, as desired.

Syntax Description	type	qsfp - Port runs at 40000/56000Mbps. qsfp-split-2 - Port is split and runs at 2X10000Mbps. qsfp-split-4 - Port is split and runs at 4X10000Mbps.
	force	force the split operation without asking for user confirmation.
Default	interface module type is qsfp (if the interface supports 40Gbps speed)	
Configuration Mode	Config Interface Ethernet	
History	3.1.1400	
Role	admin	

Example	`switch (config interface ethernet 1/4) # module-type qsfp-split-4`
	`the following interfaces will be unmapped: 1/4 1/1`
	`Type 'yes' to confirm split: yes`
	`switch (config interface ethernet 1/4) #`	

Related Commands	switchport mode switchport [trunk | hybrid] allowed-vlan show vlan	
Note	• The affected interfaces should be disabled prior to the operation • in order to un-split the interface - used the command with “qsfp”, the speed is set to 40Gbps “module-type qsfp”. • This command is applicable only on 40Gbps Ethernet ports	

5.2 Link Aggregation Group (LAG)

Link Aggregation protocol describes a network operation in which several same speed links are combined into a single logical entity with the accumulated bandwidth of the originating ports. LAG groups exchange Lag Aggregation Control Protocol (LACP) packets in order to align the functionality between both endpoints of the LAG. To equally send traffic on all LAG links, the switch uses a hash function which can use a set of attributes as key to the hash function.

As many as 16 physical ports can be aggregated on a single LAG.

5.2.1 Configuring Static Link Aggregation Group (LAG)

➢ ***To configure a static LAG:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Create a port-channel entity. Run:

```
switch (config) # interface port-channel 1
switch (config interface port-channel 1) #
```

Step 4. Change back to config mode.

```
switch (config interface port-channel 1) # exit
switch (config) #
```

Step 5. Add a physical port to the port-channel. Run:

```
switch (config interface ethernet 1/4) # channel-group 1 mode on
switch (config interface ethernet 1/4) #
```

If the physical port is operationally up, this port becomes an active member of the aggregation. Consequently, it becomes able to convey traffic.

5.2.2 Configuring Link Aggregation Control Protocol (LACP)

➢ ***To configure LACP:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Create a port-channel entity. Run:

```
switch (config) # interface port-channel 1
switch (config interface port-channel 1) #
```

Step 4. Change back to config mode. Run:

```
switch (config interface port-channel 1) # exit
switch (config) #
```

Step 5. Enable LACP in the switch. Run:

```
switch (config) # lacp
switch (config) #
```

Step 6. Add a physical port to the port-channel. Run:

```
switch (config interface ethernet 1/4) # channel-group 1 mode active/passive
switch (config interface ethernet 1/4) #
```

5.2.3 Commands

interface port-channel

interface port-channel <1-4096>[-<2-4096>]
no interface port-channel <1-4096>[-<2-4096>]

Creates a LAG and enters the LAG configuration mode. There is an option to create a range of LAG interfaces.
The no form of the command deletes the LAG, or range of LAGs.

Syntax Description	1-4096 / 2-4096	LAG number
Default	N/A	
Configuration Mode	Config	
History	3.1.1400	First version
	3.2.1100	Added range support
	3.4.0000	Added note
Role	admin	

Example	`switch (config)# interface port-channel 1`
	`switch (config interface port-channel 1) # exit`
	`switch (config)# interface port-channel 1-10`
	`switch (config interface port-channel 1-10) #`	

Related Commands		
Note	If a LAG is also an IPL, attempting to delete it without first deleting the IPL is rejected by the management.	

lacp

	lacp **no lacp** Enables LACP in the switch. The no form of the command disables LACP in the switch.
Syntax Description	N/A
Default	LACP is disabled.
Configuration Mode	Config
History	3.1.1400
Role	admin
Example	`switch (config)# lacp` `switch (config)#`
Related Commands	
Note	

lacp system-priority

lacp system-priority <1-65535>
no lacp system-priority

Configures the LACP system priority.
The no form of the command sets the LACP system-priority to default.

Syntax Description	1-65535	LACP system-priority.
Default	32768	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	

Example	`switch (config)# lacp system-priority 1`
	`switch (config)# show lacp interfaces port-channel`
	`Port-channel Module Admin Status is enabled`
	`Port-channel System Identifier is 00:02:c9:5c:61:70`
	`LACP System Priority: 3`
	`switch (config)#`	

Related Commands		
Note		

lacp (interface)

lacp {rate fast | port-priority <1-65535>}
no lacp {rate fast | port-priority}

Configures the LACP interface parameters.
The no form of the command sets the LACP interface configuration to default.

Syntax Description	rate fast	Sets LACP PDUs on the port to be in fast (1 second) or slow rate. (30 seconds).
	1-65535	LACP port-priority.
Default	rate - slow (30 seconds) port-priority 32768	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	

Example	`switch (config)# lacp rate fast`
	`switch (config)# show lacp interfaces ethernet 1/7`
	`Port : 1/7`
	`-------------`
	
	`Port State = Down`
	`Channel Group : 1`
	`Pseudo port-channel = Po1`
	`LACP port-priority = 32768`
	`LACP Rate = Slow`
	`LACP Activity : Passive`
	`LACP Timeout : Short`
	
	`Aggregation State : Aggregation, Defaulted,`
	
	`Port State LACP Port Priority Admin Key Oper Key Port Number Port State`
	`----------`
	`1/7 Down 128 1 1 0x7 0x0`
	`switch (config)#`	

Related Commands		
Note	Configuring LACP rate (fast or slow) will configure the peer port to send (fast or slow), it does not make any affect on the local port LACP rate.	

port-channel load-balance

port-channel load-balance <method>
no port-channel load-balance <method>

Configures the port-channel load balancing distribution function method.
The no form of the command sets the distribution function method to default.

Syntax Description	method	Possible load balance methods: • destination-ip • destination-mac • destination-port • source-destination-ip • source-destination-mac • source-destination-port • source-ip • source-mac • source-port
Default	source-destination-mac	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	

Example	`switch (config)# port-channel load-balance ethernet destination-ip source-port source-mac`
	`switch (config)# show interfaces port-channel load-balance`
	`destination-ip,source-mac,source-port`
	`switch (config)#`	

Related Commands		
Note	Several load balance methods can be configured (refer to the example)	

channel-group

channel-group <1-4096> [mode {on | active | passive}]
no channel-group

Assigns and configures a physical interface to a port channel.
The no form of the command removes a physical interface from the port-channel.

Syntax Description	1-4096	The port channel number.
	mode on	Static assignment the port to LAG. LACP will not be enabled on this port.
	mode active/passive	Dynamic assignment of the port to LAG. LACP will be enabled in either passive or active mode.
Default	N/A	
Configuration Mode	Config Interface Ethernet	
History	3.1.1400	
Role	admin	

Example

```
switch (config interface 1/7)# channel-group 1 mode active
switch (config interface 1/7)# show interfaces port-channel summary
Flags: D- Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
U - Up (port-channel)

--------------------------------------------------------------------------
Group Port-      Type       Member Ports
Channel
--------------------------------------------------------------------------
1 Po1(D)         LACP       Eth1/7(D)

switch (config interface 1/7)#
```

Related Commands

show interfaces port-channel summary
show interfaces port-channel compatibility-parameters
show lacp interfaces ethernet

Note

- Setting the mode to active/passive is possible only in LACP is enabled.
- The first port in the LAG decide if the LAG will be static (“on”) or LACP (“active” , “pasive”).
- All the ports in the LAG must have the same configuration, determines by the first port added to the LAG. The port with a different configuration will be rejected, for the list of dependencies refer to ‘show interfaces port-channel compatibility-parameters’

show lacp counters

show lacp counters

Displays the LACP PDUs counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin

Example	`switch (config)# show lacp counters`
	`LACPDUs Marker Marker Response LACPDUs`
	`Port Sent Recv Sent Recv Sent Recv Illegal Unknown`
	`---------------------------------------------------------------------`
	`Port-channel: 1`
	`------------------`
	`1/7 0 0 0 0 0 0 0 0`
	
	`switch (config) # switch (config)#`

Related Commands	
Note	

show lacp interfaces ethernet

show lacp interface ethernet <inf>

Displays the LACP interface configuration and status.

Syntax Description	inf	Interface number, for example “1/1”.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
Role	admin	

Example	`switch (config) # show lacp interfaces ethernet 1/4`
	`Port : 1/4`
	`-------------`
	
	`Port State = Down`
	`Channel Group : 1`
	`Pseudo port-channel = Po1`
	`LACP port-priority = 128`
	`LACP Rate = Slow`
	`LACP Activity : Passive`
	`LACP Timeout : Short`
	
	`Aggregation State : Aggregation, Defaulted,`
	
	`Port State LACP Port Priority Admin Key Oper Key Port Number Port State`
	`----------------------------------------------------------------------`
	`1/4 Down 128 1 1 0x4 0x0`
	`switch (config) #`	

Related Commands		
Note		

show lacp interfaces neighbor

show lacp interfaces neighbor

Displays the LACP interface neighbor status.

Syntax Description	N/A	
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	First version
	3.4.0000	Updated output
Role	admin	

Example

```
switch (config) # show lacp interfaces neighbor
Flags:
A - Device is in Active mode
P - Device is in Passive mode

Channel group 1 neighbors

Port 1/4
----------
Partner System ID               : 00:00:00:00:00:00
Flags                           : A
LACP Partner Port Priority      : 0
LACP Partner Oper Key           : 0
LACP Partner Port State         : 0x0

Port State Flags Decode
-----------------------
Activity : Active
Aggregation State : Aggregation, Sync, Collecting, Distributing

MLAG channel group 25 neighbors

Port 1/49
----------
Partner System ID               : 00:02:c9:fa:c4:c0
Flags                           : A
LACP Partner Port Priority      : 255
LACP Partner Oper Key           : 33
LACP Partner Port State         : 0xbc

Port State Flags Decode
-----------------------
Activity : Active
Aggregation State : Aggregation, Sync, Collecting, Distributing,

MLAG channel group 28 neighbors

Port 1/51
----------
Partner System ID               : f4:52:14:10:d8:f1
Flags                           : A
LACP Partner Port Priority      : 255
LACP Partner Oper Key           : 33
LACP Partner Port State         : 0xbc

Port State Flags Decode
-----------------------
Activity : Active
Aggregation State : Aggregation, Sync, Collecting, Distributing,

switch (config) #
```

Related Commands

Note

show lacp

show lacp

Displays the LACP global parameters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.4.0000
Role	admin

Example	`switch (config) # show lacp`
	`Port-channel Module Admin Status is enabled`
	`switch (config) #`

Related Commands	
Note	

show lacp interfaces system-identifier

show lacp interfaces {mlag-port-channel | port-channel} <instance> system-identifier

Displays the system identifier of LACP.

Syntax Description	instance	LAG or MLAG instance.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.4.0000	
Role	admin	

Example	`switch (config)# show lacp interfaces port-channel 2 system-identifier`
	`Priority: 12345`
	`MAC: 00:02:C9:AC:2A:60`
	`switch (config)#`	

Related Commands		
Note		

show interfaces port-channel

show interfaces port-channel {compatibility-parameters | load-balance | summary}

Displays port-channel parameters.

Syntax Description	compatibility-parameters	Displays the parameters that must be the same among the member ports of the port-channel interface.
	load-balance	Displays the type of load-balancing in use for port-channels.
	summary	Displays a summary of the port-channel interfaces.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4000	
Role	admin	

Example

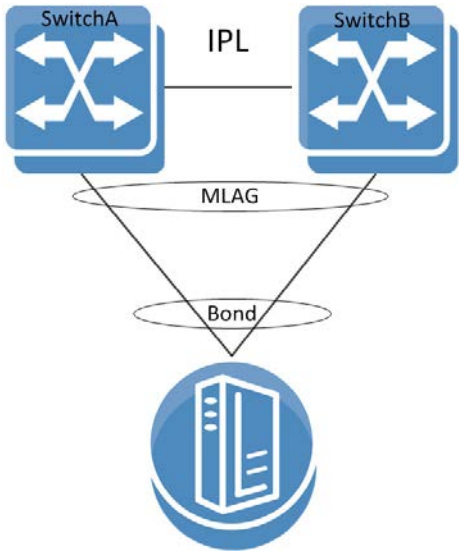
```
switch (config) # show interfaces port-channel compatibility-parameters
* Port-mode
* Speed
* MTU
* Flow Control
* Access VLAN
* Allowed VLAN list
* Flowcontrol & PFC
* Channel-group mode
* CoS parameters

Static configuration on the port should be removed:
* ACL port binding
* Static mrouter
* Static mac address
switch (config) #show interfaces port-channel load-balance
source-destination-mac

switch (config) #show interfaces port-channel summary
Flags: D- Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
U - Up (port-channel)

--------------------------------------------------------------------------------
Group Port-      Type       Member Ports
Channel
--------------------------------------------------------------------------------
switch (config) #
```

Related Commands

Note

5.3 MLAG

Figure 12: Basic MLAG Setup



All nodes in an MLAG must be of the same CPU type (i.e. PPC or x86).

Each switch configuration is independent and it is user responsibility to make sure to configure both switches similarly pertaining MLAG (e.g. MLAG port-channel VLAN membership, static MAC, ACL, etc).

A link aggregation group (LAG) is used for extending the bandwidth from a single link to multiple links and provide redundancy in case of link failure. Extending the implementation of the LAG to more than a single device provides yet another level of redundancy that extends from the link level to the node level. This extrapolation of the LAG from single to multiple switches is referred to as multi-chassis link aggregation (MLAG). MLAG is supported on Ethernet blades' internal as well as external ports.

MLAG is currently supported for only 2 switches.

A peered device (host or switch) connecting to switches running an MLAG runs a standard LAG and is unaware of the fact that the LAG connects to two separate switches.

MLAG links currently mandate disabling xSTP control protocol. However, interfaces not part of an MLAG can run any protocol independently.

The MLAG switches share an inter-peer link (IPL) between them for carrying control messages in a steady state or data packages in failure scenarios. Thus, the bandwidth of the IPL should be defined accordingly. The IPL itself can be a LAG and be constructed of either 10GbE or 40GbE links. In such a case, PFC must be configured on this IPL. Figure 13, "Basic MLAG Topology," on page 392 illustrates. The IPL serves the following purposes:

- MLAG protocol control – keepalive messages, MAC sync, MLAG port sync, etc.
- MLAG port failure – serves redundancy in case of a fallen link on one of the MLAG switches.
- Layer-3 failure – serves redundancy in case of a failed connection between the MLAG switches and the rest of the L3 network should there be one.

The MLAG protocol is made up of the following components to be expanded later:

- Keepalive
- Unicast and multicast sync
- MLAG port sync

Upgrading software of an MLAG pair can be done without consideration for master/slave roles. Switches in the same MLAG group must have the same MLNX-OS version.

When positioned at the top of rack (ToR) and connecting with a Layer-3 uplink, the MLAG pair acts as the L3 border for the hosts connected to it. To allow default gateway redundancy, both MLAG switches should be addressed by the host via the same default gateway address.

MLAG uses an IP address (VIP) that is always directed to the MLAG-VIP master node.

When running MLAG with L3, VRRP or MAGP must be deployed. For more information, refer to Section 6.6, "VRRP," on page 770 or Section 6.7, "MAGP," on page 785 respectively.

When MLAG is connected through a Layer-2 based uplink, there is no need to apply default gateway redundancy towards hosts since this function is implemented on the L2/L3 border points of the network.

The two peer switches need to carry the exact same configuration of the MLAG attributes for guaranteeing proper functionality of the MLAG.

Ensuring that both switches are configured identically is the responsibility of the user and is not monitored by the MLNX-OS software.

When working with MLAG the maximum number of MAC addresses is limited to 47,970. Without it, the number of MAC addresses would be 55,872.

When transitioning from standalone into a group or vice versa, a few seconds are required for the node state to stabilize. During that time, group features such as Gateway HA, SM HA, and MLAG commands should not be executed. To run group features, wait for the CLI prompt to turn into [standalone:master], [<group>:master] or [<group>:standby] instead of [standalone:*unknown*] or [<group>:*unknown*].

5.3.1 MLAG Keepalive and Failover

Master election in MLAG is based on the IPs of the nodes taking part of the MLAG. The master elected is that which has the higher IPL VLAN Interface.

The MLAG pair of switches periodically exchanges a keepalive message on a user configurable interval. If the keepalive message fails to arrive for three consecutive intervals the switches break into two standalone switches. In such case the remaining active switch begins to act as a standalone switch and assumes that its previously peering MLAG switch has failed.

To avoid a scenario where failure on the IPL causes both MLAG peers to assume that their peer has failed, a safety mechanism based on UDP packets running via the management plane is maintained and alerts both peers of IPL failure. In such a case of IPL failure, the slave shuts down its interfaces to avoid a split brain scenario and the master becomes a standalone switch.

5.3.2 Unicast and Multicast Sync

Unicast and multicast sync is a mechanism which syncs the unicast and multicast FDBs of the MLAG peers. It prevents unicast asymmetric traffic from loading the network with flood traffic and multicast traffic from being processed.

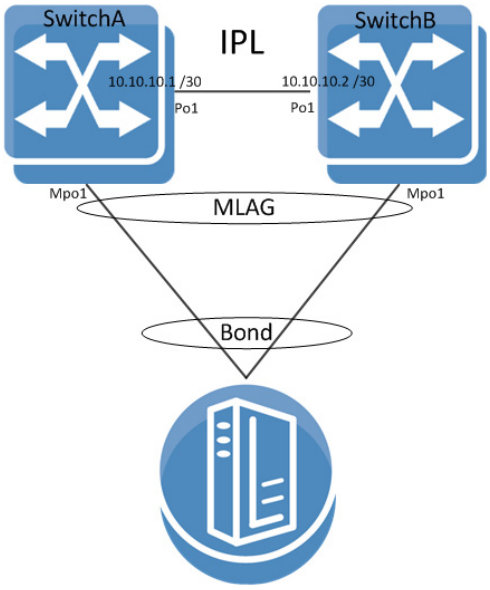
5.3.3 MLAG Port Sync

Under normal circumstances, traffic from the IPL cannot pass through the MLAG ports (the IPL is isolated from the MLAG ports). If one of the MLAG links break, the other MLAG switch opens that isolation and allows traffic from its peer through the IPL to flow via the MLAG port which accesses the destination of the fallen link.

5.3.4 MLAG Configuration

This section provides an example of how to configure two switches and a server in an MLAG setup.

Figure 13: Basic MLAG Topology



➢ ***To configure L2 MLAG:***

Prerequisites:

Step 1. Enable IP routing. Run:

```
switch (config)# ip routing
```

Step 2. (Recommended) Enable LACP in the switch. Run:

```
switch (config)# lacp
```

Step 3. Enable QoS on the switch to avoid congestion on the IPL port. Run:

```
switch (config)# dcb priority-flow-control enable force
```

Step 4. Enable the MLAG protocol commands. Run:

```
switch (config)# protocol mlag
```

Configuring the IPL:

Step 1. Create a VLAN for the inter-peer link (IPL) to run on. Run:

```
switch (config)# vlan 4000
switch (config vlan 4000)#
```

Step 2. Create a LAG. Run:

```
switch (config)# interface port-channel 1
switch (config interface port-channel 1)#
```

Step 3. Map a physical port to the LAG in active mode (LACP). Run:

```
switch (config)# interface ethernet 1/1 channel-group 1 mode active
```

Step 4. Set this LAG as an IPL. Run:

```
switch (config interface port-channel 1)# ipl 1
```

Step 5. Enable QoS on this specific interface. Run:

```
switch (config interface port-channel 1)# dcb priority-flow-control mode on force
```

Step 6. Create a VLAN interface. Run:

```
switch (config)# interface vlan 4000
switch (config interface vlan 4000)#
```

Step 7. Set an IP address and netmask for the VLAN interface.

On SwitchA, run:

```
switch (config interface vlan 4000)# ip address 10.10.10.1 /30
```

On SwitchB, run:

```
switch (config interface vlan 4000)# ip address 10.10.10.2 /30
```

Step 8. Map the VLAN interface to be used on the IPL and set the peer IP address (the IP address of the IPL port on the second switch) of the IPL peer port. IPL peer ports must be configured on the same netmask.

On SwitchA, run:

```
switch (config interface vlan 4000)# ipl 1 peer-address 10.10.10.2
```

On SwitchB, run:

```
switch (config interface vlan 4000)# ipl 1 peer-address 10.10.10.1
```

Step 9. Configure a virtual IP (VIP) for the MLAG. Run:

On SwitchA, run:

```
switch (config)# mlag-vip my-vip 10.10.10.254 /24   //mask may also be 255.255.255.0
```

On SwitchB, run:

```
switch (config)# mlag-vip my-vip
```

Creating an MLAG interface:

Step 1. Create an MLAG interface for the host. Run:

```
switch (config)# interface mlag-port-channel 1
switch (config interface mlag-port-channel 1)#
```

Step 2. Disable STP. Run:

```
switch (config interface mlag-port-channel 1)# spanning-tree port type edge
switch (config interface mlag-port-channel 1)# spanning-tree bpdufilter enable
```

Step 3. Bind an Ethernet port to the MLAG group. Run:

```
switch (config interface ethernet 1/2)# mlag-channel-group 1 mode on
```

Step 4. Create and enable the MLAG interface. Run:

```
switch (config interface mlag-port-channel 1)# no shutdown
```

STP must be disabled (`no spanning-tree`) on the MLAG switches when there is at least 1 MLAG port-channel connected to a switch and not to a host.

Enabling MLAG:

Step 1. Enable MLAG. Run:

```
switch [my-vip: master] (config mlag)# no shutdown
```

When running MLAG with L3, VRRP or MAGP must be deployed. or

- ***To verify MLAG configuration:***

Step 1. Examine MLAG configuration and status. Run:

```
switch [mellanox: master] (config)# show mlag
Admin status: Enabled
Operational status: Up
Reload-delay: 1 sec
Keepalive-interval: 30 sec
System-id: 00:02:C9:AC:2A:60

MLAG Ports Configuration Summary:
Configured: 1
Disabled:   0
Enabled:    1

MLAG Ports Status Summary:
Inactive:       0
Active-partial: 0
Active-full:    1

MLAG IPLs Summary:
ID   Group         Vlan       Operational  Local           Peer
     Port-Channel  Interface  State        IP address      IP address
-------------------------------------------------------------------
1    Po1           1          Up           10.10.10.1      10.10.10.2

Peers state Summary:
System-id          State   Hostname
----------------------------------
F4:52:14:2D:9B:88  Up      <SX2>
F4:52:14:2D:9B:08  Up       SX1
switch [mellanox: standby] (config)#
```

Step 2. Examine the MLAG summary table. Run:

```
switch [my-vip: master] (config)# show interfaces mlag-port-channel summary
Port Flags: D - Down, P - Up in port-channel (members)
MLAG Port-Channel Flags: D-Down, U-Up
                         P-Partial UP, S - suspended by MLAG

Group
Port-Channel      Type       Local Ports              Peer Ports
-------------------------------------------------------------------------
1 Mpo2(U)         Static     Eth1/2(P)                Eth1/2(P)

switch (config)#
```

Step 3. Examine the MLAG statistics. Run:

```
switch [my-vip: master] (config)# show mlag statistics
IPL 1:
Rx Heartbeat : 516
Tx Heartbeat : 516
Rx IGMP tunnel : 0
Tx IGMP tunnel : 0
RX mlag-notification: 0
TX mlag-notification: 0
Rx port-notification : 0
Tx port-notification : 0
Rx FDB sync : 0
Tx FDB sync : 0
RX LACP manager: 1
TX LACP manager: 0
switch (config)#
```

5.3.5 Commands

protocol mlag

protocol mlag
no protocol mlag

Enables MLAG functionality and unhides the MLAG commands.
The no form of the command hides the MLAG commands and deletes its database.

Syntax Description	
Default	no protocol mlag
Configuration Mode	Config
History	3.3.4500
Role	admin
Example	`switch (config) # protocol mlag` `switch (config) #`
Related Commands	
Note	• Running the no form of this command hides MLAG commands. • MLAG may be enabled without IP routing, but without IP routing an IPL vLAN interface cannot be configured and thus MLAG does not function. • MLAG may be enabled without IGMP snooping, but if IGMP snooping is disabled, multi-cast FDBs do not sync.

mlag

mlag

Enters MLAG configuration mode.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.3.4500
Role	admin
Example	`switch (config) # mlag` `switch (config mlag) #`
Related Commands	
Note	

reload-delay

reload-delay <value>
no reload-delay

Specifies the amount of time that MLAG ports are disabled after system reboot. The no form of the command resets this parameter to its default value.

Syntax Description	value	Time in seconds. Range: 0-300.
Default	30 seconds	
Configuration Mode	Config MLAG	
History	3.3.4500	
Role	admin	
Example	`switch (config mlag) # reload-delay 30` `switch (config mlag) #`	
Related Commands		
Note	• This interval allows the switch to learn the IPL topology to identify the master and sync the MAC address before opening the MLAG ports. • This parameter must be similar in all MLAG peers.	

keep-alive-interval

keep-alive-interval <value>
no keep-alive-interval

Configures the interval during which keep-alive messages are issued between the MLAG switches.
The no form of the command resets this parameter to its default value.

Syntax Description	value	Time in seconds. Range: 1-300.
Default	1 second	
Configuration Mode	Config MLAG	
History	3.3.4500	
Role	admin	
Example	`switch (config mlag) # keep-alive-interval 1` `switch (config mlag) #`	
Related Commands		
Note	This parameter must be similar in all MLAG peers.	

shutdown

shutdown
no shutdown

Enables MLAG.
The no form of the command disables MLAG.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config MLAG
History	3.3.4500
Role	admin
Example	`switch (config mlag) # no shutdown` `switch (config mlag) #`
Related Commands	
Note	This parameter must be similar in all MLAG peers.

interface mlag-port-channel

interface mlag-port-channel <if-number>
no interface mlag-port-channel <if-number>

Creates an MLAG interface.
The no form of the command deletes the MLAG interface.

Syntax Description	if-number	Integer. Interface number range: 1-1000.
Default	N/A	
Configuration Mode	Config	
History	3.3.4500	
Role	admin	
Example	`switch (config) # interface mlag-port-channel 1` `switch (config interface mlag-port-channel 1) #`	
Related Commands		
Note	• The maximum number of interfaces is 64. • The default Admin state is disabled. • Range configuration is possible on this interface. • This interface number must be the same in all the MLAG switches.	

mlag-channel-group mode

mlag-channel-group <if-number> mode {on | active | passive}
no mlag-channel-group

Binds an Ethernet port to the MLAG LAG.
The no form of the command deletes the binding.

Syntax Description	if-number	Integer. Interface number range: 1-1000.
	on	Binds to static MLAG.
	active	Sets MLAG LAG in LACP active mode.
	passive	Sets MLAG LAG in LACP passive mode.
Default	N/A	
Configuration Mode	Config Interface Ethernet	
History	3.3.4500	
Role	admin	
Example	`switch (config interface ethernet 1/1)# mlag-channel-group 1 mode on` `switch (config interface ethernet 1/1)#`	
Related Commands		
Note		

ipl

ipl <ipl-id> {gateway {a | b | c} | eth | ib} [force]
no ipl <ipl-id>

Sets this LAG as an IPL port.
The no form of the command resets this LAG as regular LAG.

Syntax Description	ipl-id	IPL ID. Only “1” IPL port is supported.
	force	Forces the change of a regular LAG to an IPL port. The user does not need to delete LAG configuration.
Default	no ipl	
Configuration Mode	Config Interface Port Channel	
History	3.3.4500	
Role	admin	
Example	`switch (config interface port-channel 1)# ipl 1` `switch (config interface port-channel 1)#`	
Related Commands		
Note	• If a LAG is set as IPL, only the commands “[no] shutdown”, “no ipl” and “no interface port-channel” become applicable. • A LAG interface set as IPL must have default LAG configuration, otherwise the set is rejected. Force option can be used.	

ipl peer-address

ipl <ipl-id> peer-address <IP-Address>
no ipl <ipl-id>

Maps a VLAN interface to be used for an IPL LAG and sets the peer IP address of the IPL peer port.
The no form of the command deletes a peer IPL LAG and unbinds this VLAN interface from the IPL function.

Syntax Description	ipl-id	IPL ID. Only “1” IPL port is supported.
	IP-Address	IPv4 address.
Default	N/A	
Configuration Mode	Config Interface VLAN	
History	3.3.4500	
Role	admin	
Example	`switch (config interface vlan 1)# ipl 1 peer-address 10.10.10.10` `switch (config interface vlan 1)#`	
Related Commands		
Note	• The subnet mask is the same subnet mask of the VLAN interface. • This VLAN interface should be used for IPL only.	

mlag-vip

mlag-vip <domain-name> [<ip-address> <masklen> | <ip-address> <subnet> [force]]
no mlag-vip

Sets the VIP domain and IP address for MLAG.
The no form of the command deletes the VIP domain and IP address.

Syntax Description	mlag-domain-name	MLAG group name.
	<ip-address> <masklen>	IP address and mask length in the format 10.10.10.10 /24. Note that a space is required between the IP address and the mask.
	<ip-address> <subnet>	IP address and mask length in the format 10.10.10.10 /24 or 255.255.255.0. Note that a space is required between the IP address and the mask.
	force	Forces the IP address if another IP is already configured.
Default	N/A	
Configuration Mode	Config	
History	3.3.4500	
Role	admin	
Example	`switch (config)# mlag-vip my-mlag-domain 10.10.10.254/24` `switch (config)#`	
Related Commands		
Note	• This IP address must be configured in one of the MLAG switches and must be in the box management subnet. • Other switches in the MLAG must join the same domain name.	

show mlag

show mlag

Displays MLAG configuration and status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.4500 3.3.5006 Updated example
Role	admin

Example	`switch (config)# show mlag`
	`Admin status: Enabled`
	`Operational status: Up`
	`Reload-delay: 1 sec`
	`Keepalive-interval: 30 sec`
	`System-id: 00:02:C9:AC:2A:60`
	
	`MLAG Ports Configuration Summary:`
	`Configured: 1`
	`Disabled:  0`
	`Enabled:  1`
	
	`MLAG Ports Status Summary:`
	`Inactive:  0`
	`Active-partial: 0`
	`Active-full:  1`
	
	`MLAG IPLs Summary:`
	`ID  Group  Vlan  Operational  Local  Peer`
	`  Port-Channel  Interface  State  IP address  IP address`
	`---------------------------------------------------------------------`
	`1  Po1  1  Up  10.10.10.1  10.10.10.2`
	
	`Peers state Summary:`
	`Peer ID  State`
	`-------------------------`
	`88:9B:2D:14:52:F4  Up`
	`switch (config) #`

Related Commands	
Note	

show mlag-vip

show mlag-vip

Displays MLAG VIP configuration and status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.4500
Role	admin

Example	`switch (config)# show mlag-vip`
	`MLAG VIP`
	`========`
	`MLAG group name: my-mlag-group`
	`MLAG VIP address: 1.1.1.1/30`
	`Active nodes: 2`
	
	`Hostname VIP-State IP Address`
	`---------- ---------- ----------`
	`SwitchA master 10.10.10.1`
	`SwitchB standby 10.10.10.2`
	`switch (config)#`

Related Commands	
Note	

show interfaces mlag-port-channel

show interfaces mlag-port-channel <if-number>

Displays the MLAG LAG configuration and status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.4500
Role	admin

Example	`switch (config)# show interfaces mlag-port-channel 1`
	`Mpo1`
	`Admin state: Enabled`
	`Operational state: Down`
	`Description: N\A`
	`Mac address: 00:00:00:00:00:00`
	`MTU: 1500 bytes (Maximum packet size 1522 bytes)`
	`Flow-control: receive off send off`
	`Actual speed: 0 Gbps`
	`Width reduction mode: Not supported Switchport mode: access`
	`Last clearing of "show interface" counters : Never`
	`60 seconds ingress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec`
	`60 seconds egress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec`
	`Rx`
	`0 packets`
	`0 unicast packets`
	`0 multicast packets`
	`0 broadcast packets`
	`0 bytes`
	`0 error packets`
	`0 discard packets`
	`Tx`
	`0 packets`
	`0 unicast packets`
	`0 multicast packets`
	`0 broadcast packets`
	`0 bytes`
	`0 discard packets`
	`switch (config)#`

Related Commands	
Note	

show interfaces mlag-port-channel summary

show interfaces mlag-port-channel summary

Displays MLAG summary table.

Syntax Description	N/A	
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4500	First version
	3.4.0000	Added notes and updated example
Role	admin	
Example		

```
switch [my-vip: standby] (config)# show interfaces mlag-port-channel
summary
Port Flags: D - Down, P - Up in port-channel (members)
MLAG Port-Channel Flags: D-Down, U-Up
                         P-Partial UP, S - suspended by MLAG

Group
Port-Channel      Type       Local Ports              Peer Ports
------------------------------------------------------------------------
1 Mpo2(U)         Static     Eth1/2(P)                Eth1/2(P)
2 Mpo3(U)         Static     Eth1/4(P)                Eth1/8(P)
3 Mpo4(U)         LACP       Eth1/15(P)               Eth1/12(P)
switch (config)#
```

Related Commands

Note

- If a cluster is not available, the column “Peer Ports” shows “N/A”. If the cluster is available but is not configured on the peer, the “Peer Ports” column shows nothing.
- If the system happens to be busy, peer ports may be unavailable and the following prompt may appear in the output: “System busy and partial information is presented - please try again later”.

show mlag statistics

show mlag statistics

Displays the MLAG IPL counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.4500 3.4.0000 Updated example
Role	admin

Example	`switch (config)# show mlag statistics`
	`IPL 1:`
	`RX Heartbeat: 439908`
	`TX Heartbeat: 439951`
	`RX IGMP tunnel: 0`
	`TX IGMP tunnel: 1`
	`RX mlag-notification: 0`
	`TX mlag-notification: 12`
	`RX port-notification: 56`
	`TX port-notification: 73`
	`RX FDB sync: 424`
	`TX FDB sync: 778`
	`RX LACP manager: 38`
	`TX LACP manager: 21`

Related Commands	
Note	

5.4 VLANs

A Virtual Local Area Network (VLAN) is an L2 segment of the network which defines a broadcast domain and is identified by a tag added to all Ethernet frames running within the domain. This tag is called a VLAN ID (VID) and can take a value of 1-4094.

Each port can have a switch mode of either:

- Access – Access port is a port connected to a host. It can accept only untagged frames, and assigns them a default configured VLAN (Port VLAN ID). On egress, traffic sent from the access port is untagged.
- Access-dcb – This mode is Mellanox specific that receives ingress untagged traffic but sends egress priority tag (VLAN ID = 0)
- Hybrid – Hybrid port is a port connected to either switches or hosts. It can receive both tagged and untagged frames and assigns untagged frames a default configured VLAN (Port VLAN ID). It receives tagged frames with VLANs of which the port is a member (these VLANs' names are allowed). On egress, traffic of allowed VLANs sent from the Hybrid port is sent tagged, while traffic sent with PVID is untagged.
- Trunk – Trunk port is a port connecting 2 switches. It accepts only tagged frames with VLANs of which the port is a member. On egress, traffic sent from the Trunk port is tagged. By default, a Trunk port is, automatically, a member on all current VLANs.

5.4.1 Configuring Access Mode and Assigning Port VLAN ID (PVID)

➢ ***To configure Access mode and assign PVID to interfaces:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Create a VLAN. Run:

```
switch (config) # vlan 6
switch (config vlan 6) #
```

Step 4. Change back to config mode. Run:

```
switch (config vlan 6) # exit
switch (config) #
```

Step 5. Enter the interface context. Run:

```
switch (config) # interface ethernet 1/36
switch (config interface ethernet 1/36) #
```

Step 6. From within the interface context, configure the interface mode to Access. Run:

```
switch (config interface ethernet 1/36) # switchport mode access
switch (config interface ethernet 1/36) #
```

Step 7. From within the interface context, configure the Access VLAN membership. Run:

```
switch (config interface ethernet 1/36) # switchport access vlan 6
switch (config interface ethernet 1/36) #
```

Step 8. Change back to config mode. Run:

```
switch (config interface ethernet 1/36) # exit
switch (config) #
```

5.4.2 Configuring Hybrid Mode and Assigning Port VLAN ID (PVID)

➢ ***To configure Hybrid mode and assign PVID to interfaces:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Create a VLAN. Run:

```
switch (config) # vlan 6
switch (config vlan 6) #
```

Step 4. Change back to config mode. Run:

```
switch (config vlan 6) # exit
switch (config) #
```

Step 5. Enter the interface context. Run:

```
switch (config) # interface ethernet 1/36
switch (config interface ethernet 1/36) #
```

Step 6. From within the interface context, configure the interface mode to Access. Run:

```
switch (config interface ethernet 1/36) # switchport mode hybrid
switch (config interface ethernet 1/36) #
```

Step 7. From within the interface context, configure the Access VLAN membership. Run:

```
switch (config interface ethernet 1/36) # switchport hybrid vlan 6
switch (config interface ethernet 1/36) #
```

Step 8. Change to config mode again. Run:

```
switch (config interface ethernet 1/36) # exit
switch (config) #
```

5.4.3 Configuring Trunk Mode VLAN Membership

➢ ***To configure Trunk mode VLAN membership:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Create a VLAN. Run:

```
switch (config) # vlan 10
switch (config vlan 10) #
```

Step 4. Change back to config mode. Run:

```
switch (config vlan 10) # exit
switch (config) #
```

Step 5. Enter the interface context. Run:

```
switch [standalone: master] (config) # interface ethernet 1/35
switch [standalone: master] (config interface ethernet 1/35) #
```

Step 6. From within the interface context, configure the interface mode to Trunk. Run:

```
switch [standalone: master] (config interface ethernet 1/35) # switchport mode trunk
switch [standalone: master] (config interface ethernet 1/35) #
```

5.4.4 Configuring Hybrid Mode VLAN Membership

➢ ***To configure Hybrid mode VLAN membership:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Create a VLAN. Run:

```
switch (config) # vlan 10
switch (config vlan 10) #
```

Step 4. Change back to config mode. Run:

```
switch (config vlan 10) # exit
switch (config) #
```

Step 5. Enter the interface context. Run:

```
switch (config) # interface ethernet 1/35
switch (config interface ethernet 1/35) #
```

Step 6. From within the interface context, configure the interface mode to Hybrid. Run:

```
switch (config interface ethernet 1/35) # switchport mode hybrid
switch (config interface ethernet 1/35) #
```

Step 7. From within the interface context, configure the allowed VLAN membership. Run:

```
switch (config interface ethernet 1/35) # switchport hybrid allowed-vlan add 10
switch (config interface ethernet 1/35) #
```

Step 8. Change to config mode again. Run:

```
switch (config interface ethernet 1/35) # exit
switch (config) #
```

5.4.5 Commands

vlan

vlan {<vlan-id> | <vlan-range>}
no vlan {<vlan-id> | <vlan-range>}

Creates a VLAN or range of VLANs, and enters a VLAN context.
The no form of the command deletes the VLAN or VLAN range.

Syntax Description	vlan-id	1-4094.
	vlan-range	Any range of VLANs.
Default	VLAN 1 is enabled by default.	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	

Example	`switch (config) # vlan 10`
	`switch (config vlan 10) # show vlan`
	
	`VLAN  Name  Ports`
	`----  ----------  ----------`
	`1  default  Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2 ...`
	`10`
	`switch (config vlan 10) #`	

Related Commands	show vlan switchport mode switchport [trunk | hybrid] allowed-vlan	
Note	Interfaces are not added automatically to VLAN unless configured with trunk or hybrid mode with “all” option turned on.	

name

name <vlan-name>
no name

Adds VLAN name.
The no form of the command deletes the VLAN name.

Syntax Description	vlan-name	40-character long string.
Default	No name available.	
Configuration Mode	Config VLAN	
History	3.1.1400	
Role	admin	

Example	`switch (config) # vlan 10`
	`switch (config vlan 10) # name my-vlan-name`
	`switch (config vlan 10) # show vlan`
	
	`VLAN Name Ports`
	`---- ----------- ----------`
	`1 default Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2, Eth1/5,`
	`Eth1/6, Eth1/7, Eth1/8, Eth1/9, Eth1/10,`
	`Eth1/11, Eth1/12, Eth1/13, Eth1/14, Eth1/15,`
	`Eth1/16, Eth1/17, Eth1/18, Eth1/19, Eth1/20,`
	`Eth1/21, Eth1/22, Eth1/23, Eth1/24, Eth1/25,`
	`Eth1/26, Eth1/27, Eth1/28, Eth1/29, Eth1/30,`
	`Eth1/31, Eth1/32, Eth1/33, Eth1/34, Eth1/35,`
	`Eth1/36, Po34, Po4096`
	`10 my-vlan-name`	

Related Commands	show vlan switchport mode switchport [trunk | hybrid] allowed-vlan	
Note	Name can not be added to a range of VLANs.	

show vlan

show vlan [id <vlan-id>]

Displays the VLAN table.

Syntax Description	vlan-id 1-4094.
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin

Example	`switch (config vlan 10) # show vlan`
	
	`VLAN Name Ports`
	`---- ----------- -------------------------------------`
	`1 default Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2 ...`
	`10 my-vlan-name`

Related Commands	show vlan switchport mode switchport [trunk | hybrid] allowed-vlan vlan
Note	

switchport mode

switchport mode {access | trunk | hybrid | access-dcb}
no switchport mode

Sets the switch port mode.
The no form of the command sets the switch port mode to access.

Syntax Description	access	Un-tagged port. 802.1q tagged traffic will be filtered. egress traffic is un-tagged.
	trunk	802.1q tagged port, un-tagged traffic will be filtered.
	hybrid	Both 802.1q tagged and un-tagged traffic is allowed on the port.
	access-dcb	Un-tagged port, egress traffic is priority tagged.
Default	access.	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.1400	
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	
Example		

```
switch (config) # interface ethernet 1/7
switch (config interface ethernet 1/7) # switchport mode access
switch (config interface ethernet 1/7) # show interfaces switchport
Interface  |    Mode    | Access vlan |        Allowed vlans
-----------|------------|-------------|--------------------------
Eth1/2      access          1
Eth1/3      access          1
Eth1/4/1    access          1
Eth1/4/2    access          1
Eth1/5      access          1
Eth1/6      access          1
....
Po34        access          1
Po4096      access          1
switch (config interface ethernet 1/7) #
```

Related Commands	show vlan show interfaces switchport switchport access vlan switchport [trunk | hybrid] allowed-vlan vlan
Note	

switchport access

switchport access vlan <vlan-id>
no switchport access vlan

Sets the port access VLAN.
The no form of the command sets the port access VLAN to 1.

Syntax Description	vlan-id	1-4094.
Default	1	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.1400	First version
	3.2.0500	Format change (removed hybrid and access-dcb options). Previous command format was: “switchport {hybrid | access-dcb | access} vlan <vlan-id>”
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	

Example

```
switch (config) # interface ethernet 1/7
switch (config interface ethernet 1/7) # switchport access vlan 10
switch (config interface ethernet 1/7) # show interfaces switchport
Interface  |    Mode    | Access vlan |        Allowed vlans
-----------|------------|-------------|--------------------------
Eth1/2      access          1
Eth1/3      access          1
Eth1/4/1    access          1
Eth1/4/2    access          1
Eth1/5      access          1
Eth1/6      access          1
Eth1/7      access          10
....
Po4096      access          1
switch (config interface ethernet 1/7) #
```

Related Commands	show vlan show interfaces switchport switchport mode switchport [trunk | hybrid] allowed-vlan vlan
Note	This command is not applicable for interfaces with port mode trunk. only one option (“access”, “access-dcb” or “hybrid”) is applicable to configure on the port, depends on the switchport mode of the port.

switchport {hybrid, trunk} allowed-vlan

switchport {hybrid, trunk} allowed-vlan {<vlan> | add <vlan> | remove <vlan> all | except <vlan> | none}

Sets the port allowed VLANs.

Syntax Description	vlan	VLAN ID (1-4094) or VLAN range.
	add	Adds VLAN or range of VLANs.
	remove	Removes VLANs or range of VLANs.
	all	Adds all VLANs in available in the VLAN table. New VLANs added to the VLAN table are added automatically.
	except	Adds all VLANs expect this VLAN or VLAN range.
	none	Removes all VLANs.
Default	N/A	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.1400	
Role	admin	

Example

```
switch (config) # interface ethernet 1/7
switch (config interface ethernet 1/7) # switchport hybrid allowed-vlan
all
switch (config interface ethernet 1/7) #show interfaces switchport
Interface  |    Mode    | Access vlan |        Allowed vlans
-----------|------------|-------------|--------------------------
Eth1/2      access          1
Eth1/3      access          1
Eth1/4/1    access          1
Eth1/4/2    access          1
Eth1/5      access          1
Eth1/6      access          1
Eth1/7      hybrid          1           1, 10
....
Po34        access          1
Po4096      access          1
switch (config interface ethernet 1/7) #
```

Related Commands	show vlan show interfaces switchport switchport access vlan switchport mode vlan
Note	This command is not applicable for interfaces with port mode access or access-dcb.

show interface switchport

show interface switchport

Displays all interface switch port configurations.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin

Example	`switch (config) #show interfaces switchport`
	`Interface  |    Mode    | Access vlan |        Allowed vlans`
	`-----------|------------|-------------|--------------------------`
	`Eth1/2      access          1`
	`Eth1/3      access          1`
	`Eth1/4/1    access          1`
	`Eth1/4/2    access          1`
	`Eth1/5      access          1`
	`Eth1/6      access          1`
	`Eth1/7      hybrid          1           1, 10`
	`....`
	`Po34        access          1`
	`Po4096      access          1`
	`switch (config)#`

Related Commands	show vlan switchport access vlan switchport mode vlan
Note	

5.5 MAC Address Table

5.5.1 Configuring Unicast Static MAC Address

You can configure static MAC addresses for unicast traffic. This feature improves security and reduces unknown unicast flooding.

➢ ***To configure Unicast Static MAC address:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Run the command `mac-address-table static unicast <destination mac address> vlan <vlan identifier(1-4094)> interface ethernet <slot>/ <port>`.

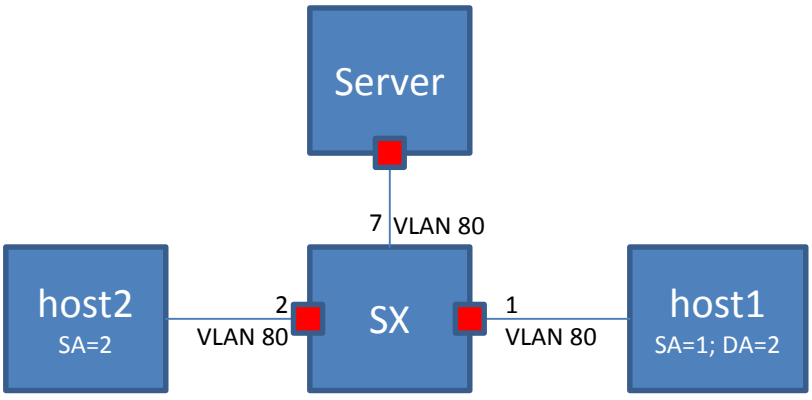
```
switch (config) # mac-address-table static unicast 00:11:22:33:44:55 vlan 1 interface ethernet 0/1
```

5.5.2 MAC Learning Considerations

MAC learning may be disabled using the command `mac-learning disable` which is beneficial in the following situations:

- To prevent denial-of-service attacks
- To manage the available MAC address table space by controlling which interfaces can learn MAC addresses
- To duplicate to a dedicated server (port7) all the packets that one host (host1; port1) sends to another (host2; port2), like in port mirroring. To accomplish this, MAC learning is disabled on port2. In this case the FDB does not obtain the MAC address of host2. Also, to prevent broadcast to every port, it is possible to configure a VLAN (VLAN 80) which ports 1, 2 and 7 are member of.

Figure 14: MAC Learning Disable Example Case



5.5.3 Commands

mac-address-table aging-time

mac-address-table aging-time <age>
no mac-address-table aging-time

Sets the maximum age of a dynamically learnt entry in the MAC address table.
The no form of the command resets the aging time of the MAC address table to its default.

Syntax Description	age	10-1000000 seconds.
Default	300	
Configuration Mode	Config	
History	3.1.0600	
Role	admin	

Example	`switch (config) # mac-address-table aging-time 50`
	`switch (config) # show mac-address-table aging-time`
	
	`Mac Address Aging Time: 50`
	
	`switch (config) #`	

Related Commands	show mac-address-table show mac-address-table aging time	
Note		

mac-address-table static

mac-address-table static <mac address> vlan <vlan> interface <if-type> <if-number>
no mac-address-table static <mac address> vlan <vlan> interface <if-type> <if-number>

Configures a static MAC address in the forwarding database.
The no form of the command deletes a configured static MAC address from the forwarding database.

Syntax Description	mac address	Destination MAC address.
	vlan	VLAN ID or VLAN range.
	if-type	Ethernet or port-channel interface type.
	if-number	The interface number (i.e. 1/1, 3).
Default	No static MAC addresses available in default.	
Configuration Mode	Config	
History	3.1.0600	
Role	admin	

Example

```
switch (config) # mac-address-table static aa:aa:aa:aa:aa:aa vlan 1
interface ethernet 1/7
switch (config) # show mac-address-table

Switch ethernet-default

Vlan    Mac Address          Type     Interface
----    -----------          ----     ------------
1       aa:aa:aa:aa:aa:aa   static     Eth1/7
Number of unicast:      1
Number of multicast:    0
switch (config) #
```

Related Commands

show mac-address-table
mac-address-table aging time

Note

The no form of the command will not clear a dynamic MAC address. Dynamic MAC addresses are cleared using the “clear mac-address-table dynamic” command.

mac-learning disable

mac-learning disable
no mac-learning disable

Disables MAC-address learning.
The no form of the command enables MAC-address learning.

Syntax Description	N/A
Default	Enabled
Configuration Mode	Config Interface Ethernet Config Interface Port Channel
History	3.1.0600
Role	admin
Example	`switch (config interface ethernet 1/1) # mac-learning disable`
Related Commands	
Note	• When adding a port to a LAG, the port needs to be aligned with the LAG's configuration • When removing a port from a LAG, the port remains in whichever configuration the LAG is in • Disabling MAC learning is not supported on a local analyzer port. • Disabling MAC learning is not supported on an IPL LAG.

clear mac-address-table dynamic

clear mac-address-table dynamic

Clear the dynamic entries in the MAC address table.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0600
Role	admin
Example	`switch (config) # clear mac-address-table dynamic` `switch (config) #`
Related Commands	mac-address-table aging-time mac-address-table static show mac-address-table
Note	This command does not clear the MAC addresses learned on the mgmt0 port. Static entries are deleted using the “no mac-address-table static” command.

show mac-address-table

show mac-address-table [address <mac-address> | interface ethernet <if-number> | vlan [<vlan> | range <range>] | unicast | multicast]

Displays the static and dynamic unicast and multicast MAC addresses for the switch. Various of filter options available.

Syntax Description	mac-address	Filter the table to a specific MAC address.
	if-number	Filter the table to a specific interface.
	vlan	Filter the table to a specific VLAN number (1-4094).
	range	Filter the table to a range of VLANs.
	unicast	Filter the table to a unicast addresses only.
	multicast	Filter the table to a multicast addresses only.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0600	
	3.3.4500	Updated Example
Role	admin	
Example		

```
switch (config) # show mac-address-table

Switch ethernet-default

Vlan    Mac Address         Type     Interface
----    -----------         ----     ------------
1       00:00:00:00:00:01   Static   Po5
1       00:00:3D:5C:FE:16   Dynamic  Eth1/1
1       00:00:3D:5D:FE:1B   Dynamic  Eth1/2
Number of unicast:      2
Number of multicast:    0
switch (config) #
```

Related Commands	mac-address-table static clear mac-address-table
Note	

show mac-address-table aging-time

show mac-address-table aging-time

Displays the MAC address table aging time.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0600
Role	admin

Example	`switch (config) # mac-address-table aging-time 300`
	`switch (config) # show mac-address-table aging-time`
	
	`Mac Address Aging Time: 300`
	
	`switch (config) #`

Related Commands	mac-address-table aging-time mac-address-table static clear mac-address-table
Note	MAC addresses learned on the mgmt0 is not shown by this command.

5.6 Spanning Tree

The operation of Rapid Spanning Tree Protocol (RSTP) provides for rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN. The RSTP component avoids this delay by calculating an alternate root port, and immediately switching over to the alternate port if the root port becomes unavailable. Thus, using RSTP, the switch immediately brings the alternate port to forwarding state, without the delays caused by the listening and learning states. The RSTP component conforms to IEEE standard 802.1D 2004.

RSTP enhancements is a set of functions added to increase the volume of RSTP in Mellanox switches. It adds a set of capabilities related to the behavior of ports in different segments of the network. For example: the required behavior of a port connected to a non-switch entity, such as host, is to converge quickly, while the required behavior of a port connected to a switch entity is to converge based on the RSTP parameters.

Additionally, it adds security issues on a port and switch basis, allowing the operator to determine the state and role of a port or the entire switch should an abnormal event occur. For example: If a port is configured to be root-guard, the operator will not allow it to become a root-port under any circumstances, regardless of any BPDU that will have been received on the port.

5.6.1 Port Priority and Cost

When two ports on a switch are part of a loop, the STP port priority and port path cost configuration determine which port on the switch is put in the forwarding state and which port is put in the blocking state.

To configure port priority use the following command:

```
switch (config interface etherent <inf>)# spanning-tree port-priority <0-240>
```

To configure port path cost use the following command:

```
switch (config interface etherent <inf>)# spanning-tree cost <1-200000000>
```

5.6.2 Port Type

Port type has the following configuration options:

- **edge –** is not assumed to be converged by the RSTP learning/forwarding mechanism. It converges to forwarding quickly.

It is recommended to configure the port type for all ports connected to hosts as edge ports.

- **normal –** is assumed to be connected to a switch, thus it tries to be converged by the RSTP learning/forwarding. However, if it does not receive any BPDUs, it is operationally moved to be edge.
- **network –** is assumed to be connected to a switch. If it does not receive any BPDUs, it is moved to discarding state.

Each of these configuration options is mutually exclusive.

Port type is configured using the command spanning-tree port type. It may be applied globally on the switch (Config) level, which configures all switch interfaces. Another option is to configure ports individually by entering the interface's configuration mode.

- Global configuration:

```
switch (config)# spanning-tree port type {edge , normal , network} default
```

- Interface configuration:

```
switch (config interface etherent <inf>)# spanning-tree port type {edge , normal, net-
work}
```

5.6.3 BPDU Filter

Using BPDU filter prevents the CPU from sending/receiving BPDUs on specific ports.

BPDU filtering is configured per interface. When configured, the port does not send any BPDUs and drops all BPDUs that it receives. To configure BPDU filter, use the following command:

```
switch (config interface etherent <inf>)# spanning-tree bpdufilter {enable , disable}
```

Configuring BPDU filtering on a port connected to a switch can cause bridging loops because the port filters any BPDU it receives and goes to forwarding state.

5.6.4 Loop Guard

Loop guard is a feature that prevents loops in the network.

When a blocking port in a redundant topology transitions to the forwarding state (accidentally), an STP loop occurs. This happens when BPDUs are no longer received by one of the ports in a physically redundant topology.

Loop guard is useful in switched networks where devices are connected point-to-point. A designated bridge cannot disappear unless it sends an inferior BPDU or brings the link down on a point-to-point connection.

The loop guard configuration is only allowed on “network” port type.

If loop guard is enabled and the port does not receive BPDUs, the port is put into an inconsistent state (blocking) until the port starts to receive BPDUs again. A port in the inconsistent state does not transmit BPDUs. If BPDUs are received again, loop guard alters its inconsistent state condition. STP converges to a stable topology without the failed link or bridge after loop guard isolates the failure.

Disabling loop guard moves all loop-inconsistent ports to listening state.

To configure loop guard use the following command:

```
switch (config interface etherent <inf>)# spanning-tree guard loop
```

5.6.5 Root Guard

Configuring root guard on a port prevents that port from becoming a root port. A port put in root-inconsistent (blocked) state if an STP convergence is triggered by a BPDU that makes that port a root port. The port is unblocked after the port stops sending BPDUs.

To configure loop guard use the following command:

```
switch (config interface etherent <inf>)# spanning-tree guard root
```

5.6.6 MSTP

Spanning Tree Protocol (STP) is a mandatory protocol to run on L2 Ethernet networks to eliminate network loops and the resulting broadcast storm caused by these loops. Multiple STP (MSTP) enables the virtualization of the L2 domain into several VLANs, each governed by a separate instance of a spanning tree which results in a network with higher utilization of physical links while still keeping the loop free topology on a logical level.

Up to 64 MSTP instances can be defined in the switch. Up to 64 VLANs can be mapped to a single MSTP instance. MSTP instance 0 (the default instance) may have all possible VLANs (1-4094) mapped to it.

For MSTP network design over Mellanox L2 VMS, please refer to Mellanox Virtual Modular Switch Reference Guide.

5.6.7 Commands

spanning-tree

spanning-tree
no spanning-tree

Globally enables the spanning tree feature.
The no form disables the spanning tree feature.

Syntax Description	N/A
Default	Spanning tree is enabled.
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	switch (config) # no spanning-tree switch (config) #
Related Commands	show spanning-tree
Note	

spanning-tree (timers)

spanning-tree [forward-time <time in secs> | hello-time <time in secs> | max-age <time in secs>]
no spanning-tree [forward-time | hello-time | max-age]

Sets the spanning tree timers.
The no form of the command sets the timer to default.

Syntax Description	forward-time	Controls how fast a port changes its spanning tree state from Blocking state to Forwarding state. Parameter range: 4-30 seconds.
	hello-time	Determines how often the switch broadcasts its hello message to other switches when it is the root of the spanning tree. Parameter range: 1-2 seconds.
	max-age	Sets the maximum age allowed for the Spanning Tree Protocol information learnt from the network on any port before it is discarded. Parameter range: 6-40 seconds.
Default	forward-time: 15 seconds hello-time:2 seconds max-age: 20 seconds	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # spanning-tree forward-time` `switch (config) #`	
Related Commands	show spanning-tree	
Note	The following formula applies on the spanning tree timers: 2*(ForwardTime -1)>=MaxAgeTime >= 2*(Hello Time + 1)	

spanning-tree port type (default global)

spanning-tree port type <port-type> default
no spanning-tree port type default

Configures all switch interfaces as edge/network/normal ports. These ports can be connected to any type of device.
The no form of the command disables the spanning tree operation.

Syntax Description	port-type	• Edge - Assumes all ports are connected to hosts/servers. • Network - Assumes all ports are connected to switches and bridges. • Normal - the port type (Edge or Network) determines according to the spanning tree operational mode.
Default	Normal	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # spanning-tree port type edge default` `switch (config) #`	
Related Commands	show spanning-tree	
Note		

spanning-tree priority

spanning-tree priority <bridge-priority>
no spanning-tree priority

Sets the spanning tree bridge priority.
The no form of the command sets the bridge priority to default.

Syntax Description	bridge-priority	Sets the bridge priority for the spanning tree. Its value must be in steps of 4096, starting from 0. Only the following values are applicable: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.
Default	32786	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # spanning-tree priority 4096` `switch (config) #`	
Related Commands	show spanning-tree	
Note		

spanning-tree port-priority

spanning-tree port-priority <priority>
no spanning-tree port-priority

Configures the spanning-tree interface priority.
The no form of the command returns configuration to its default.

Syntax Description	priority	Spanning tree interface priority. The possible values are: 0, 16, 32,48, 64, 80, 96, 112, 128,144, 160, 176, 192, 208, 224, 240.
Default	128	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	

Example	`switch (config) # interface ethernet 1/1`
	`switch (config interface ethernet 1/1) # spanning-tree port-priority 16`
	`switch (config interface ethernet 1/1) #`	

Related Commands	show spanning-tree	
Note		

spanning-tree cost

spanning-tree cost <port cost>
no spanning-tree cost

Configures the interface cost of the spanning tree.
The no form of the command returns configuration to its default.

Syntax Description	port cost	Sets the spanning tree cost of an interface. Value range is 0-200000000.
Default	The default cost is derived from the speed. 1Gbps 20000 10Gbps 2000 40Gbps 500 56Gbps 357	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	

Example	`switch (config) # interface ethernet 1/1`
	`switch (config interface ethernet 1/1) # spanning-tree cost 1000`
	`switch (config interface ethernet 1/1) #`	

Related Commands	show spanning-tree	
Note	• LAG default cost is calculated by dividing the port speed by the number of active links in UP state. For example: if there were 4 links in the LAG out of which only two are in UP state, assuming the port speed is 10Gbps, the LAG cost will be 2000/2 = 1000. • When configuring the cost for a LAG, the cost will be fixed to this configuration, no matter what the number of active links (UIP state) in the LAG is • Unstable network may cause the LAG cost to change dynamically assuming the cost parameter is not configured for anything else other than default	

spanning-tree port type

spanning-tree port type <port type>
no spanning-tree port type

Configures spanning-tree port type
The no form of the command returns configuration to default.

Syntax Description	port type	Sets the spanning-tree port type. The port type parameter has four options: • Default (globally defined) • Edge • Normal • Network In case there is no change of this parameter, the configuration will be taken from the global default port type.
Default	Globally defined by the command “spanning-tree port type <port-type> default”	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	

Example	`switch (config) # interface ethernet 1/1`
	`switch (config interface ethernet 1/1) # spanning-tree port type edge`
	`switch (config interface ethernet 1/1) #`	

Related Commands	show spanning-tree	
Note		

spanning-tree guard

spanning-tree guard {loop | root}
no spanning-tree guard {loop | root}

Configures spanning-tree guard.
The no form of the command returns configuration to default.

Syntax Description	loop	Enables loop-guard on the interface. If the loop-guard is enabled, upon a situation where the interface fails to receive BPDUs the switch will not egress data traffic on this interface.
	root	Enables root-guard on the interface. If root-guard is enabled on the interface, the interface will never be selected as root port.
Default	loop-guard and loop-guard are disabled.	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	

Example	`switch (config) # interface ethernet 1/1`
	`switch (config interface ethernet 1/1) # spanning-tree guard root`
	`switch (config interface ethernet 1/1) #`	

Related Commands	show spanning-tree	
Note		

spanning-tree bpdufilter

spanning tree bpdufilter {disable | enable}
no spanning tree bpdufilter

Configures spanning-tree BPDU filter on the interface. The interface will ignore any BPDU that it receives and will not send PDBUs, The STP state on the port will move to the forwarding state.
The no form of the command returns the configuration to default.

Syntax Description	disable	Disables the BPDU filter on this port.
	enable	Enables the BPDU filter on this port.
Default	BPDU filter is disabled.	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.0000	
Role	admin	

Example	`switch (config) # interface ethernet 1/1`
	`switch (config interface ethernet 1/1) # spanning-tree bpdufilter enable`
	`switch (config interface ethernet 1/1) #`	

Related Commands	show spanning-tree	
Note	This command can be used when the switch is connected to hosts.	

clear spanning-tree counters

clear spanning-tree counters

Clears the spanning-tree counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	`switch (config) # clear panning-tree counters` `switch (config) #`
Related Commands	show spanning tree
Note	

show spanning-tree

show spanning-tree [detail | interface <type> <number>]

Displays spanning tree information.

Syntax Description	detail	Displays detailed spanning-tree configuration and statistics.
	interface <type> <number>	Displays the running state for a specific interface. Options for “type”: ethernet or port-channel. Options for “number”: <slot/port> or <number>.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show spanning-tree`
	
	`Switch ethernet-default`
	
	`Spanning tree protocol is enabled rstp`
	
	`Spanning tree force version:2`
	`Root ID`
	`  Priority 32768`
	`  Address 00:02:c9:5c:61:70`
	`  This bridge is the root`
	`  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec`
	`Bridge ID`
	`  Priority 32768`
	`  Address  00:02:c9:5c:61:70`
	`  Hello Time 2 sec Max Age 20 sec Forward Delay  15 sec`
	
	`Interface  Role  Sts  Cost  Prio  Type`
	`----  ----  -----  ----  ----  ----`
	`switch (config) #`	

Related Commands	clear spanning-tree counters spanning-tree	
Note		

spanning-tree mst max-hops

spanning-tree mst max-hops <max-hops>
no spanning-tree mst max-hops

Specifies the max hop value inserts into BPDUs that sent out as the root bridge. The no form of the command sets the parameter to its default value.

Syntax Description	max-hops	Max hop value. The range is 6-40.
Default	20	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config)# spanning-tree mst max-hops 20` `switch (config)#`	
Related Commands		
Note	The max hop setting determines the number of bridges in an MST region that a BPDU can traverse before it is discarded.	

spanning-tree mst priority

spanning-tree mst <mst-instance> priority <priority>
no spanning-tree mst <mst-instance> priority

Configures the specified instance's priority number.
The no form of the command sets the parameter to its default value.

Syntax Description	mst-instance	MST instance. Range is 1-64.
	priority	MST instance port priority. Possible values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
Default	32768	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config)# spanning-tree mst 1 priority 32768` `switch (config)#`	
Related Commands		
Note	The bridge priority is the four most significant digits of the bridge ID, which is used by spanning tree algorithms to select the root bridge and choose among redundant links. Bridge ID numbers range from 0-65535 (16 bits); bridges with smaller bridge IDs are elected over other bridges.	

spanning-tree mst vlan

spanning-tree mst <mst-instance> vlan <vlan-range>
no spanning-tree mst <mst-instance> vlan <vlan-range>

Maps a VLAN or a range of VLANs into an MSTP instance.
The no form of the command unmaps a VLAN or a range of VLANs from MSTP instances.

Syntax Description	mst-instance	MST instance. Range is 1-64.
	vlan <vlan-range>	A single VLAN or a a range of VLANs. The format is <vlan> or <from-vlan>-<to-vlan>.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config)# spanning-tree mst 1 vlan 10-20` `switch (config)#`	
Related Commands		
Note		

spanning-tree mst revision

spanning-tree mst revision <number>
no spanning-tree mst revision

Configures the MSTP revision number.
The no form of the command sets the parameter to its default value.

Syntax Description	number	The MST revision number. Range is 0-65535.
Default	0	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config)# spanning-tree mst revision 1` `switch (config)#`	
Related Commands		
Note	The revision number is one of three parameters, along with the MST name and VLAN-to-instance map, that identify the switch's MST region.	

spanning-tree mst name

spanning-tree mst name <name>
no spanning-tree mst name

Configures the MSTP name.
The no form of the command sets the parameter to its default value.

Syntax Description	name	MST name: Up to 32 characters.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config)# spanning-tree mst name my-mst` `switch (config)#`	
Related Commands		
Note	The name is one of three parameters, along with the MST revision number and VLAN-to-instance map, that identifies the switch's MST region.	

spanning-tree mst root

spanning-tree mst <mst-instance> root <role>
no spanning-tree mst <mst-instance> root

Changes the bridge priority for the specified MST instance to the following values:
- Primary – 8192
- Secondary – 16384

The no form of the command sets the parameter to its default value.

Syntax Description	mst-instance	MSTP instance. Possible range is 1-64.
	role	Values: “primary” or “secondary”.
Default	primary	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config)# spanning-tree mst name my-mst` `switch (config)#`	
Related Commands		
Note	The root command is a way to automate a system configuration while ‘playing’ with the priority field. The priority field granularity may be too explicit for some users in case you wish to have 2 levels of priority (primary and secondary). So by default all the switches get the same priority and while using the root option you can get the role of master and backup by setting the priority field to a predefined value.	

spanning-tree mode

spanning-tree mode {rst | mst}
no spanning-tree mode

Changes the spanning tree mode.
The no form of the command sets the parameter to its default value.

Syntax Description	mst	Multiple spanning tree.
	rst	Rapid spanning tree.
Default	rst	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config)# spanning-tree mode mst` `switch (config)#`	
Related Commands		
Note		

spanning-tree mst port-priority

spanning-tree mst {mst-instance} port-priority <priority>
no spanning-tree mode

Changes the spanning tree mode.
The no form of the command sets the parameter to its default value.

Syntax Description	mst-instance	MST instance. Range is 1-64.
	priority	MST instance port priority. Valid values are: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 and 240.
Default	rst	
Configuration Mode	Config Interface Port Channel	
History	3.3.4150	
Role	admin	

Example	`switch (config interface ethernet 1/1)# spanning-tree mst 1 port-priority 32768`
	`switch (config interface port-channel 1)# spanning-tree mst 1 port-priority 32768`
	`switch (config)#`	

Related Commands		
Note		

spanning-tree mst cost

spanning-tree mst {mst-instance} cost <cost-value>
no spanning-tree mode

Configures the cost per MSTP instance.
The no form of the command sets the parameter to its default value.

Syntax Description	mst-instance	MST instance. Range is 1-64.
	cost-value	MST instance port cost. Range is 0-200000000.
Default	2000 for 10Gb/s, 500 for 40Gb/s, 20000 for 1Gb/s, 357 for 56Gb/s	
Configuration Mode	Config Interface Port Channel	
History	3.3.4150	
Role	admin	

Example	`switch (config interface ethernet 1/1)# spanning-tree mst 1 cost 4000`
	`switch (config interface port-channel 1)# spanning-tree mst 1 cost 4000`
	`switch (config)#`	

Related Commands		
Note		

show spanning-tree

show spanning-tree [detail | interface {ethernet <slot>/<port> | port-channel <port-channel>} | mst [<instance> interface {ethernet <slot>/<port> | port-channel <port-channel>} | details | interface {ethernet <slot>/<port> | port-channel <port-channel>}] | root]

Displays spanning-tree information for a switch.

Syntax Description	detail	Displays detailed spanning-tree information on a switch.
	interface {ethernet <slot>/<port> | port-channel <port-channel>}	Displays running state for the specified interface.
	mst [<instance> interface {ethernet <slot>/<port> | port-channel <port-channel>} | details | interface {ethernet <slot>/<port> | port-channel <port-channel>}	Displays basic multi-spanning-tree information of a specific switch or a specific interface.
	root	Displays root multi-spanning-tree information of a specific switch.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4150	
Role	admin	

Example	`switch (config) # show spanning-tree root`
	`Instance  Priority  MAC addr  Root Cost  Hello Time Max Age  FWD Dly  Root Port`
	`MST0  32768  00:02:c9:71:ed:40  500  2  20  15  Eth1/20`
	`MST1  32768  00:02:c9:71:f0:c0  0  2  20  15  -`
	`MST2  0  00:02:c9:71:f0:c0  0  2  20  15  -`
	`MST3  32768  00:02:c9:71:f0:c0  0  2  20  15  -`
	`switch (config) #`	

Related Commands		
Note		

5.7 OpenFlow

MLNX-OS supports OpenFlow 1.0. OpenFlow is a network protocol that facilitates direct communication between network systems via Ethernet. Software Defined Networks (SDN) allows a centralist management of network equipment. OpenFlow allows the SDN controller to manage SDN equipment. The OpenFlow protocol allows communication between the OpenFlow controller and OpenFlow agent.

OpenFlow is useful to manage switches and allow applications running on the OpenFlow controller to have access to the switch's datapath and provide functionality such as flow steering, security enhancement, traffic monitoring and more.

The OpenFlow controller communicates with the OpenFlow switch over secured channel using OpenFlow protocol.

An OpenFlow switch contains a flow table which contains flows inserted by the OpenFlow controller. And the OpenFlow switch performs packet lookup and forwarding according to those rules.

Mellanox OpenFlow switch implementation is based on the hybrid model, allowing the coexistence of an OpenFlow pipeline and a normal pipeline. In this model, a packet is forwarded according to OpenFlow configuration, if such configuration is matched with the packet parameters. Otherwise, the packet is handled by the normal (regular forwarding/routing) pipeline.

The OpenFlow specification defines:

> "OpenFlow-hybrid switches support both OpenFlow operation and normal Ethernet switching operation, i.e. traditional L2 Ethernet switching, VLAN isolation, L3 routing (IPv4 routing, IPv6 routing...), ACL and QoS processing. Those switches must provide a classification mechanism outside of OpenFlow that routes traffic to either the OpenFlow pipeline or the normal pipeline. For example, a switch may use the VLAN tag or input port of the packet to decide whether to process the packet using one pipeline or the other, or it may direct all packets to the OpenFlow pipeline."

Utilizing the built-in capabilities of the hybrid switch/router is the main benefit of the hybrid mode. It increases network performance and efficiency – faster processing of new flows as well as lower load on the controllers. The hybrid switch processes non-OpenFlow data through its local management plane and achieve better efficiency and use of resources, compared to the pure OpenFlow switch.

5.7.1 Flow Table

The flow table contains flows which are used to perform packet lookup, modification and forwarding. Each flow has a 12 tuple key. The key is used in order to classify a packet into a certain flow. The key contains the flowing fields: ingress port, source MAC, destination MAC, EtherType, VLAN ID, PCP, source IP, destination IP, IP protocol, IP ToS bits, TCP/UDP source port and TCP/UDP destination port.

The flow key can have a specific value for each field or wildcard which signals to the switch to ignore this part of the key.

Each packet passes through the flow table once a match is found; the switch performs the actions configured to the specific flow by the OpenFlow controller.

Upkeeping a flow table enables the switch to forward incoming traffic with a simple lookup on its flow table entries. OpenFlow switches perform a check for matching entries on, or ignore using a wildcard, specific fields of the ingress traffic. If the entry exists, the switch performs the action associated with that flow entry. Packets without a flow entry match are forwarded according to the normal pipeline (hybrid switch).

Every flow entry contains one of the following parameters:

1. Header fields for matching purposes with each entry containing a specific value or a wildcard which could match all entries.
2. Matching packet counters which are useful for statistical purposes, in order to keep track of the number of packets.
3. Actions which specify the manner in which to handle the packets of a flow which can be any of the following:
   a. Forwarding the packet
   b. Dropping the packet
   c. Forwarding the packet to the OpenFlow controller
   d. Modifying the VLAN, VLAN priority (PCP), and/or stripping the VLAN header

The flow table supports up to 1000 flows.

5.7.2 Configuring OpenFlow

➢ ***To run OpenFlow on a switch:***

Step 1. Unlock the OpenFlow CLI commands. Run:

```
switch (config) # protocol openflow
```

Step 2. Configure interfaces to be managed by OpenFlow. Run:

```
switch (config) # interface ethernet 1/1-1/4 openflow mode hybrid
```

Step 3. Configure the OpenFlow controller IP and TCP port. Run:

```
switch (config) # openflow controller-ip 10.209.0.205 tcp-port 6633
```

Step 4. (Optional) Verify the OpenFlow configuration. Run:

```
switch (config) # show openflow
OpenFlow version: OF VERSION 1.0
Table size: 1000, 0 in use
Active controller ip: 10.209.0.205 port: 6633
Connection status: HANDSHAKE_COMPLETE (CONNECTED)
Forward-to-controller: ospf lldp arp-unicast arp-broadcast (all)
Enabled ports:  Eth1/1      Eth1/2      Eth1/3      Eth1/4
switch (config) #
```

To be able to configure the switch using the controller, you should see the following line in the output:

Connection status must be: HANDSHAKE_COMPLETE (CONNECTED).

5.7.3 Commands

protocol openflow

protocol openflow
no protocol openflow

Unhides the OpenFlow commands.
The no form of the command hides the OpenFlow commands.

Syntax Description	N/A
Default	no protocol openflow
Configuration Mode	Config
History	3.3.4200
Role	admin
Example	`switch (config) # protocol openflow` `switch (config) #`
Related Commands	
Note	

openflow description

openflow description <string>

Sets the OpenFlow description.

Syntax Description	string	Free string.
Default	N/A	
Configuration Mode	Config	
History	3.3.4302	
Role	admin	

Example	`switch (config) # openflow description OF-switch-104`
	`switch (config) # show openflow detail`
	`OpenFlow version: OF VERSION 1.0`
	`Table size: 1000, 0 in use`
	`Active controller ip: 10.209.1.39 port: 6633`
	`Connection status: HANDSHAKE_COMPLETE (CONNECTED)`
	`Forward-to-controller: ospf lldp arp-unicast arp-broadcast (all)`
	`Enabled ports: Eth1/10 Eth1/11 Eth1/13 Eth1/19`
	`Echo period: 10 sec`
	`Keep alive period: 30 sec`
	`Messages in (last session): 86290`
	`Messages out (last session): 47984`
	`Disconnect count: 0`
	`Openflow description: OF-switch-104`
	`Datapath ID: 00:00:00:02:c9:a8:e3:50`
	`Not supporting buffering`
	`Not supporting emergency flows`
	`Not supporting port statistics`
	`Not supporting IP reassemble`
	`Supporting spanning tree`
	`Not supporting queue statistics`
	`switch (config) #`	

Related Commands		
Note		

openflow mode hybrid

openflow mode hybrid
no openflow mode

Enables OpenFlow on the port.
The no form of the command returns the port to its default state.

Syntax Description	N/A
Default	no openflow mode
Configuration Mode	Config Interface Ethernet
History	3.3.4200
Role	admin
Example	`switch (config interface etherent 1/1)# openflow mode hybrid` `switch (config interface etherent 1/1)#`
Related Commands	
Note	

controller-ip

controller-ip <ip-address> [tcp-port <port-number>]
no controller-ip <ip-address> tcp-port

Sets the OpenFlow controller's IP & TCP port.
The no form of the command sets the parameter to its default.

Syntax Description	ip-address	The IPv4 address of the OpenFlow controller.
	tcp-port <port-number>	Sets the TCP port number of the OpenFlow controller.
Default	0.0.0.0; TCP port 6633	
Configuration Mode	Config OpenFlow	
History	3.3.4200	
Role	admin	
Example	`switch (config openflow) # controller-ip 10.10.10.10 tcp-port 6633` `switch (config openflow) #`	
Related Commands		
Note		

datapath-id

datapath-id <value>
no datapath-id

Sets a specific identifier for the switch with which the controller is communicating. The no form of the command resets the parameter to its default value.

Syntax Description	value	The most significant 16 bits of the agent data-path ID. Range is 0x0000-0xFFFF in hexa.
Default	0x0000	
Configuration Mode	Config OpenFlow	
History	3.3.4200	
Role	admin	
Example	`switch (config openflow) # datapath-id 0x1234` `switch (config openflow) #`	
Related Commands		
Note		

forward-to-controller

forward-to-controller {[ospf] [lldp] [arp-unicast] [arp-broadcast] all | none}

Forwards the selected traffic types to the controller from all the ports on which Open-Flow enabled.

Syntax Description	ospf	Forwards OSPF traffic to the controller.
	lldp	Forwards LLDP traffic to the controller.
	arp-unicast	Forwards ARP-unicast traffic to the controller.
	arp-broadcast	Forwards ARP-broadcast traffic to the controller.
	all	Forwards all traffic types to the controller.
	none	Forwards no traffic to the controller.
Default	None	
Configuration Mode	Config OpenFlow	
History	3.3.4200	
Role	admin	
Example	`switch (config openflow) # forward-to-controller all` `switch (config openflow) #`	
Related Commands		
Note		

show openflow

show openflow [detail | tables | flows <id>]

Displays general information about the OpenFlow protocol configuration.

Syntax Description	detail	Displays detailed information about the OpenFlow protocol.
	tables	Displays information about the OpenFlow tables (size, type, etc.).
	flows <id>	Displays specific flows inside the OpenFlow tables. ID may be a range (e.g. 1-10).
	statistics	Displays OpenFlow statistics.
Default	None	
Configuration Mode	Any Command Mode	
History	3.3.4200	
	3.3.4302	Removed flow-id parameter Added “flows” and “statistics” parameters
Role	admin	
Example		

```
switch (config openflow) # show openflow flows 2

Flow id: 2
priority:       1
hard timeout:   infinite
idle timeout:   0 sec
match:
  ingress interface:            Eth1/18
  source Ethernet address:      11:22:33:44:55:66
  destination Ethernet address: 77:88:aa:bb:cc:fe
  Ethernet type:                0x800
  VLAN ID:                      308
  PCP:                          4
  SIP:                          1.1.1.1
  DIP:                          2.2.2.2
  Dport:                        1790
  Protocol:                     86
  TOS:                          120
actions:
  output controller
statistics:
  0 packets,  0 bytes

switch (config openflow) #
```

Related Commands	
Note	

5.8 IGMP Snooping

Only IGMP Snooping v1 and v2 are supported.

The Internet Group Multicast Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. The host joins a multicast-group by sending a join request message towards the network router, and responds to queries sent from the network router by dispatching a join report.

A given port can be either manually configured to be a router-port or it can be dynamically manifested when having received a query, hence, the network router is connected to this port. All IGMP Snooping Control packets received from hosts (joins/leaves) are forwarded to the router-port, and the router-port updates its multicast-group data-base accordingly. Each dynamically learnt multicast group will be added to all of the router-ports on the switch.

As many as 5K multicast groups can be created on the switch.

5.8.1 Configuring IGMP Snooping

You can configure IGMP snooping to establish multicast group memberships.

➢ ***To configure IGMP snooping:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Enable IGMP snooping globally. Run:

```
switch (config) # ip igmp snooping
switch (config) #
```

Step 4. Enable IGMP snooping on a VLAN. Run:

```
switch (config) # vlan 2
switch (config vlan 2) # ip igmp snooping
```

5.8.2 Defining a Multicast Router Port on a VLAN

You can define a Multicast Router (MRouter) port on a VLAN in one of the following methods:

➢ ***To change the Interface Switchport to Trunk:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Enable IGMP snooping globally. Run:

```
switch (config) # ip igmp snooping
switch (config) #
```

Step 4. Change the interface switchport mode of the port (the interface is member of VLAN 1 by default). Run:

```
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) # switchport mode trunk
```

Step 5. Change back to config mode. Run:

```
switch (config interface ethernet 1/1) # exit
switch (config) #
```

Step 6. Define the MRouter port on the VLAN. Run:

```
switch (config) # vlan 2
switch (config vlan 2) # ip igmp mrouter interface ethernet 1/1
switch (config vlan 2) #
```

➢ ***To change the Interface Switchport to Hybrid:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Enable IGMP snooping globally. Run:

```
switch (config) # ip igmp snooping
switch (config) #
```

Step 4. Create a VLAN. Run:

```
switch (config) # vlan 200
switch (config vlan 200) #
```

Step 5. Change back to config mode. Run:

```
switch (config vlan 200) # exit
switch (config) #
```

Step 6. Change the interface switchport mode of the port (the interface is member of VLAN 1 by default). Run:

```
switch (config) # interface ethernet 1/36
switch (config interface ethernet 1/36) # switchport mode hybrid
```

Step 7. Attach the VLAN to the port's interface. Run:

```
switch (config interface ethernet 1/36) # switchport mode hybrid allowed-vlan 200
switch (config interface ethernet 1/36) #
```

Step 8. Change to config mode again. Run:

```
switch (config interface ethernet 1/36) # exit
switch (config) #
```

Step 9. Define the MRouter port on the VLAN. Run:

```
switch (config) # vlan 200
switch (config vlan 200) # ip igmp mrouter interface ethernet 1/36
switch (config vlan 200) #
```

5.8.3 IGMP Snooping Querier

IGMP Snooping Querier compliments the IGMP snooping functionality. IGMP Snooping Querier is used to support IGMP snooping in a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed. When IGMP Snooping Querier is enabled, IGMP queries are sent out periodically by the switch through all ports in the VLAN and to which hosts wishing to receive IP multicast traffic respond with IGMP report messages. IGMP Snooping Querier must be used in conjunction with IGMP snooping as IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

➢ ***To configure IGMP Snooping Querier:***

Step 1. Enable the IGMP snooping on the switch. Run:

```
switch (config) # ip igmp snooping
```

Step 2. Enable the IGMP snooping querier on a specific VLAN. Run:

```
switch (config) # vlan 10
switch (config vlan 10)# ip igmp snooping querier
```

Step 3. Set the query interval time. Run:

```
switch (config vlan 10)# igmp snooping querier query-interval 25
```

Step 4. (Optional) Verify the IGMP snooping querier configuration. Run:

```
switch (config vlan 10)# show ip igmp snooping querier
VLAN 10   IGMP Querier Present   query-interval: 125   address: 1.1.1.2   version: 2
switch (config vlan 10)#
```

5.8.4 Commands

ip igmp snooping (admin)

ip igmp snooping
no ip igmp snooping

Enables IGMP snooping globally or per VLAN.
The no form of the command disables IGMP snooping globally or per VLAN.

Syntax Description	N/A
Default	IGMP snooping is disabled, globally and per VLAN.
Configuration Mode	Config Config VLAN
History	3.1.1400
Role	admin

Example	`switch (config) # ip igmp snooping`
	`switch (config) # vlan 10`
	`switch (config vlan 10) # ip igmp snooping`
	`switch (config vlan 10) # exit`
	`switch (config) # show ip igmp snooping`
	
	`IGMP snooping global configuration:`
	
	`IGMP snooping globally enabled`
	`IGMP snooping operationally enabled`
	`Proxy-reporting globally disabled`
	`Last member query interval is 1 seconds`
	`Mrouter timeout is 125 seconds`
	`Port purge timeout is 260 seconds`
	`Report suppression interval is 5 seconds`
	
	`switch (config vlan 10) # show ip igmp snooping vlan 10`
	
	`Vlan 10 configuration parameters:`
	`IGMP snooping is enabled`
	`IGMP version is V2`
	`Snooping switch is acting as Non-Querier`
	`mrouter static port list: none`
	`mrouter dynamic port list: none`
	`switch (config vlan 10) # vlan 10`
	`switch (config vlan 10) #`

Related Commands	show ip igmp snooping
Note	IGMP snooping has global admin state, and per VLAN admin state. Both states need to be enabled in order to enable the IGMP snooping on a specific VLAN.

ip igmp snooping (config)

ip igmp snooping {last-member-query-interval <1-25> | proxy reporting mrouter-timeout <60-600> | port-purge-timeout <130-1225> | report-suppression-interval <1-25>}

no ip igmp snooping {last-member-query-interval | proxy reporting | mrouter-timeout | report-suppression-interval}

Configures IGMP global parameters.
The no form of the command resets the IGMP global parameters to default.

Syntax Description	last-member-query-interval <1-25>	Sets the time period (in seconds) with which the general queries are sent by the IGMP quarrier. After time-out expiration the port will be removed from the multicast group.
	proxy reporting	Enables proxy reporting
	mrouter-timeout <60-600>	Sets the IGMP snooping router port purge time-out after which the port gets deleted if no IGMP router control packets are received. The default value is 125 seconds.
	port-purge-timeout <130-1225>	Sets the IGMP snooping port purge time interval after which the port gets deleted if no IGMP reports are received.
	report-suppression-interval <1-25>	Sets the IGMP snooping report-suppression time interval for which the IGMPv2 report messages for the same group will not get forwarded onto the router ports. The default value is 5 seconds.
Default	last-member-query-interval – 1 second proxy reporting is disabled mrouter-timout – 125 port-purge-timeout – 260 seconds report-suppression-interval – 5 seconds	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	

Example	`switch (config) # ip igmp snooping report-suppression-interval 3`
	`switch (config) # show ip igmp snooping`
	
	`IGMP snooping global configuration:`
	
	`IGMP snooping globally enabled`
	`IGMP snooping operationally enabled`
	`Proxy-reporting globally disabled`
	`Last member query interval is 1 seconds`
	`Mrouter timeout is 125 seconds`
	`Port purge timeout is 260 seconds`
	`Report suppression interval is 3 seconds`
	
	`switch (config) #`

Related Commands	ip igmp snooping (admin) show ip igmp snooping
Note	

ip igmp snooping fast-leave

ip igmp snooping fast-leave
no ip igmp snooping fast-leave

Enables fast leave processing on a specific interface.
The no form of the command disables fast leave processing on a specific interface.

Syntax Description	N/A
Default	Normal-leave is enabled.
Configuration Mode	Config Interface Ethernet Config Interface Port Channel
History	3.1.1400 3.3.4500 Added MLAG port-channel configuration mode
Role	admin

Example	`switch (config interface ethernet 1/1) # ip igmp snooping fast-leave`
	`switch (config interface ethernet 1/1) # show ip igmp snooping inter-faces`
	`interface leave-mode`
	`---------- ------------`
	`Eth1/1 Fast`
	`Eth1/2 Normal`
	`Eth1/3 Normal`
	`...`
	`switch (config interface ethernet 1/1) #`

Related Commands	show ip igmp snooping interfaces
Note	

ip igmp snooping static-group

ip igmp snooping static-group <IP address> interface <type> <number>
no ip igmp snooping static-group <IP address> interface <type> <number>

Creates a static multicast group and attaches a port to a specified group.
The no form of the command deletes the interface from the multicast group.

Syntax Description	Ip address	Multicast IP address <224.x.x.x - 239.255.255.255>
	interface <type> <number>	Attach the group to a specific interface. type - ethernet or port-channel
Default	No static groups are configured.	
Configuration Mode	Config VLAN	
History	3.1.1400	
Role	admin	

Example	`switch (config)# vlan 1`
	`switch (config vlan 1) # ip igmp snooping static-group 230.0.0.1 interface ethernet 1/1`
	`switch (config vlan 1) # show ip igmp snooping groups`
	`Vlan ID Group St/Dyn Ports`
	`-------- ------------ ------- -------`
	`1 230.0.0.1 St Eth1/1`
	`Total Num of Dynamic Group Addresses 0`
	`Total Num of Static Group Addresses 1`
	`switch (config vlan 1) #`	

Related Commands	show ip igmp snooping groups	
Note	If the deleted interface is the last port, it deletes the entire multicast group.	

ip igmp snooping mrouter

ip igmp snooping mrouter interface <type> <number>
no ip igmp snooping mrouter interface <type> <number>

Creates a static multicast router port on a specific VLAN, on a specific interface. The no form of the command removes the static multicast router port from a specific VLAN.

Syntax Description	interface <type> <number>	Attaches the group to a specific interface. type - ethernet or port-channel.
Default	No static mrouters are configured.	
Configuration Mode	Config VLAN	
History	3.1.1400	
Role	admin	

Example	`switch (config)# vlan 1`
	`switch (config vlan 1) # ip igmp snooping mrouter interface ethernet 1/1`
	`switch (config vlan 1) # show ip igmp snooping mrouter`
	`Vlan Ports`
	`-------- ------------`
	`1 Eth1/1(static)`
	`switch (config vlan 1) #`	

Related Commands	show ip igmp snooping mrouter	
Note	The multicast router port can be created only if IGMP snooping is enabled both globally and on the VLAN.	

ip igmp snooping unregistered multicast

ip igmp snooping unregistered multicast <options>
no ip igmp snooping unregistered multicast

Sets the behavior of the snooping switch for unregistered multicast traffic. The no form of the command sets it default.

Syntax Description	options	• flood • forward-to-mrouter-ports
Default	flood	
Configuration Mode	Config	
History	3.2.0500	
Role	admin	

Example	`switch (config) # ip igmp snooping unregisted multicast flood`
	`switch (config) # show ip igmp snooping`
	
	`IGMP snooping global configuration:`
	
	`IGMP snooping globally enabled`
	`IGMP snooping operationally enabled`
	`Proxy-reporting globally disabled`
	`Last member query interval is 1 seconds`
	`Mrouter timeout is 125 seconds`
	`Port purge timeout is 260 seconds`
	`Report suppression interval is 5 seconds`
	`IGMP snooping unregistered multicast: flood`
	`switch (config) #`	

Related Commands	show ip igmp snooping	
Note		

ip igmp snooping querier

ip igmp snooping querier
no ip igmp snooping querier

Enables the IGMP Snooping Querier on a VLAN.
The no form of the command disables the IGMP Snooping Querier on a VLAN.

Syntax Description	N/A
Default	Disable
Configuration Mode	Config VLAN
History	3.3.4200
Role	admin
Example	`switch (config vlan 1)# ip igmp snooping querier` `switch (config vlan 1)#`
Related Commands	igmp snooping querier query-interval show ip igmp snooping querier
Note	

igmp snooping querier query-interval

igmp snooping querier query-interval <time>
no igmp snooping querier query-interval

Configures the query interval.
The no form of the command rests the parameter to its default.

Syntax Description	time	Time interval between queries (in seconds).
Default	125 seconds	
Configuration Mode	Config VLAN	
History	3.3.4200	
Role	admin	
Example	`switch (config vlan 1)# igmp snooping querier query-interval 20` `switch (config vlan 1)#`	
Related Commands	igmp snooping querier query-interval show ip igmp snooping querier	
Note		

show ip igmp snooping

show ip igmp snooping

Displays IGMP snooping information for all VLANs or a specific VLAN.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin

Example	`switch (config) # show ip igmp snooping`
	
	`IGMP snooping global configuration:`
	
	`IGMP snooping globally enabled`
	`IGMP snooping operationally enabled`
	`Proxy-reporting globally disabled`
	`Last member query interval is 1 seconds`
	`Mrouter timeout is 125 seconds`
	`Port purge timeout is 260 seconds`
	`Report suppression interval is 3 seconds`
	`IGMP snooping unregistered multicast: flood`
	
	`switch (config) #`

Related Commands	
Note	

show ip igmp snooping groups

show ip igmp snooping groups

Displays per VLAN the list of multicast groups attached (static or dynamic allocated) per port.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin

Example	`switch (config) # show ip igmp snooping groups`
	`Vlan ID  Group  St/Dyn  Ports`
	`--------  ------------  -------  -------`
	`1  230.0.0.1  St  Eth1/1`
	`Total Num of Dynamic Group Addresses 0`
	`Total Num of Static Group Addresses 1`
	`switch (config) #`

Related Commands	
Note	

show ip igmp snooping vlan

show ip igmp snooping vlan {<vlan/vlan-range> | all}

Displays IGMP configuration per VLAN or VLAN range.

Syntax Description	vlan/vlan range	Displays IGMP VLAN configuration per specific VLAN or VLAN range.
	all	Display IGMP VLAN configuration on all VLAN.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
Role	admin	

Example	`switch (config) # show ip igmp vlan 1`
	`Vlan 1 configuration parameters:`
	`  IGMP snooping is enabled`
	`  IGMP version is V2`
	`  Snooping switch is acting as Non-Querier`
	`  mrouter static port list: Eth1/1`
	`  mrouter dynamic port list: none`
	`switch (config) #`	

Related Commands		
Note		

show ip igmp snooping mrouter

show ip igmp snooping mrouter

Displays IGMP snooping multicast router information.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin

Example	`switch (config) # show ip igmp snooping mrouter`
	`Vlan Ports`
	`-------- ------------`
	`1 Eth1/1(static)`
	`switch (config) #`

Related Commands	
Note	

show ip igmp snooping interfaces

show ip igmp snooping interfaces

Displays IGMP snooping interface information.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin

Example	`switch (config) # show ip igmp snooping interfaces`
	`interface  leave-mode`
	`-----------  ------------`
	`1/1  Normal`
	`1/2  Normal`
	`1/3  Normal`
	`1/4  Fast`
	`...`
	`switch (config) #`

Related Commands	
Note	

show ip igmp snooping statistics

show ip igmp snooping statistics

Displays IGMP snooping statistical counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin

Example	`switch (config) # show ip igmp snooping statistics`
	`Snooping Statistics for VLAN 1`
	`  General queries received : 0`
	`  Group specific queries received : 0`
	`  V1/V2 reports received : 0`
	`  V1/V2 reports transmitted : 0`
	`  Leave messages received : 0`
	`  Group specific queries transmitted: 0`
	`  Leave messages transmitted: 0`
	`  Unsuccessful joins received count Per Vlan: 0`
	`  Active/Successful joins received count Per Vlan: 0`
	`  Active Groups count: 0`
	`  Packets dropped: 0`
	`switch (config) #`

Related Commands	
Note	

show ip igmp snooping querier

show ip igmp snooping querier [vlan <num>]

Displays running IGMP snooping querier configuration on the VLANs.

Syntax Description	vlan <num>	Displays the IGMP snooping querier configuration running on the specified VLAN.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4200	
Role	admin	

Example	`switch (config) # show ip igmp snooping querier vlan 10`
	`Vlan 1  IGMP Querier Present  query-interval: 20  address: 1.1.1.2  version: 2`
	`switch (config) #`	

Related Commands		
Note		

5.9 Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 LAN. The protocol is formally defined in IEEE 802.1AB.

5.9.1 Configuring LLDP

➢ ***To configure the LLDP on the switch:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Enable LLDP globally on the switch. Run:

```
switch (config) # lldp
switch (config) #
```

Step 4. Enable LLDP per interface. Run:

```
switch (config interface ethernet 1/1) # lldp receive
switch (config interface ethernet 1/1) # lldp transmit
```

Step 5. Show LLDP local information. Run:

```
switch (config) # show lldp local

LLDP is Enabled

Local global configuration
Chassis sub type: macAddress (4)
Chassis id: 00:11:22:33:44:55
System Name: "switch-111111"
System Description: my-system-description
Supported capabilities: B
Supported capabilities enabled: B
```

Step 6. Show LLDP remote information. Run:

```
switch (config)# show lldp interfaces ethernet 1/1 remote

Ethernet 1/1
Remote Index: 1
Remote chassis id: 00:11:22:33:44:55 ; chassis id subtype: mac
Remote port-id: ethenret 1/2; port id subtype: local
Remote port description: ethernet 1/2
Remote system name: remote-system
Remote system description: remote-system-description
Remote system capabilities supported: B ; B
```

5.9.2 DCBX

Data Center Bridging (DCB) is an enabler for running the Ethernet network with lossless connectivity using priority-based flow control and enhanced transmission selection. DCBx (exchange)

compliments the DCB implementation by offering a dynamic protocol that communicates DCB attributes between peering endpoint.

5.9.3 Commands

lldp

lldp
no lldp

Enables LLDP globally.
The no form of the command disables the LLDP.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.2.0300
Role	admin
Example	`switch (config)# lldp` `switch (config)#`
Related Commands	show lldp local
Note	

lldp reinit

lldp reinit <seconds>
no lldp reinit

Sets the delay in seconds from enabling the LLDP on the port until re-initialization will be attempted.
The no form of the command sets the parameter to default.

Syntax Description	seconds	1-10
Default	2	
Configuration Mode	Config	
History	3.2.0300	
Role	admin	
Example	`switch (config)# lldp reinit 10` `switch (config)#`	
Related Commands	show lldp timers	
Note		

lldp timer

lldp timer <seconds>
no lldp timer

Sets the LLDP interval at which LLDP frames are transmitted. (lldpMessageTxInterval)
The no form of the command sets the parameter to default.

Syntax Description	seconds	5-32768
Default	30	
Configuration Mode	Config	
History	3.2.0300	
Role	admin	
Example	`switch (config)# lldp timer 10` `switch (config)#`	
Related Commands	show lldp timers	
Note		

lldp tx-delay

lldp tx-delay <seconds>
no lldp tx-delay

Indicates the delay in seconds between successive LLDP frame transmissions
The no form of the command sets the parameter to default.

Syntax Description	seconds	1-8192
Default	2	
Configuration Mode	Config	
History	3.2.0300	
Role	admin	
Example	`switch (config)# lldp tx-delay 10` `switch (config)#`	
Related Commands	show lldp timers	
Note	The recommended value for the tx-delay is set by the following formula: 1 <= lldp tx-delay <= (0.25 * lldp timer)	

lldp tx-hold-multiplier

lldp tx-hold-multiplier <seconds>
no lldp tx-hold-multiplier

The time-to-live value expressed as a multiple of the lldpMessageTxInterval object. The no form of the command sets the parameter to default.

Syntax Description	seconds	1-8192
Default	2	
Configuration Mode	Config	
History	3.2.0300	
Role	admin	
Example	`switch (config)# lldp tx-hold-multiplier 10` `switch (config)#`	
Related Commands	show lldp timers	
Note	The actual time-to-live value used in LLDP frames, can be expressed by the following formula: TTL = min(65535, (lldpMessageTxInterval * lldpMessageTxHoldMultiplier)) For example, if the value of lldpMessageTxInterval is '30', and the value of lldpMessageTxHoldMultiplier is '4', then the value '120' is encoded in the TTL field in the LLDP header.	

lldp {receive | transmit}

lldp {receive | transmit}
no lldp {receive | transmit}

Enables LLDP to be received or transmitted on this port.
The no form of the command disables the LLDP to be received or transmitted on this port.

Syntax Description	N/A
Default	Enabled for receive and Trasmit.
Configuration Mode	Config Interface Ethernet
History	3.2.0300
Role	admin

Example	`switch (config interface ethernet 1/1)# lldp receive`
	`switch (config interface ethernet 1/1)# lldp transmit`
	`switch (config interface ethernet 1/1)#`

Related Commands	show lldp interface
Note	The LLDP is disabled by default (globally)

lldp tlv-select

lldp tlv-select {[dcbx] [dcbx-cee] [port-description] [sys-name] [sys-description] [sys-capababilities] [management-address] [none] all}

Sets the LLDP basic TLVs to be transmitted on this port.

Syntax Description	dcbx	Enables LLDP-DCBX TLVs.
	dcbx-cee	Enables LLDP-DCBX CEE TLVs.
	port-description	LLDP port description TLV.
	sys-name	LLDP system name TLV.
	sys-description	LLDP system description TLV.
	sys-capabilities	LLDP system capabilities TLV.
	management-address	LLDP management address TLV.
	all	all above TLVs.
	none	None of the above TLVs.
Default	all	
Configuration Mode	Config Interface Ethernet	
History	3.2.0300	Initial revision
	3.3.0000	Added “none” parameter
	3.3.4302	Added “dcbx” parameter
	3.3.4402	Added “dcbx-cee” parameter
Role	admin	
Example	`switch (config interface ethernet 1/1)# lldp tlv-select port-description sys-name` `switch (config interface ethernet 1/1)#`	
Related Commands	show lldp interface	
Note		

dcb application-priority

dcb application-priority <selector> <protocol> <priority>

Adds an application to the application priority table.

Syntax Description	selector	Protocol field in hexa notation (e.g. '0x8906' for FCoE, '0x8914' for FIP).
	protocol	Has 4 options: 1. ethertype 2. tcp-sctp 3. udp-dccp 4. tcp-sctp-udp-dccp
	priority	Range: 0-7.
Default	No applications are available. The table is empty.	
Configuration Mode	Config	
History	3.3.4200	
Role	admin	
Example	`switch (config-if)# dcb application-priority ethertype 3 0x8906` `switch (config-if)#`	
Related Commands	show lldp interface	
Note		

show lldp local

show lldp local

Shows LLDP local information.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0300
Role	admin

Example	`switch (config)# show lldp local`
	
	`LLDP is Enabled`
	
	`Local global configuration`
	
	`Chassis sub type: macAddress (4)`
	`Chassis id: 0002C9030046AF00`
	`System Name: my-switch`
	`System Description: SX1036`
	`Supported capabilities: B,R`
	`Supported capabilities enabled: B`
	
	`switch (config)#`

Related Commands	
Note	

show lldp interface

show lldp interface [ethernet <inf>]

Shows LLDP local interface table information.

Syntax Description	inf	Interface number (e.g. 1/1).
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.2.0300	First version
	3.3.4200	Updated example
	3.3.4402	Updated example
Role	admin	
Example		

```
switch (config)# show lldp interface ethernet 1/1

TLV flags:
PD: port-description, SN: sys-name, SD: sys-description, SC: sys-capa-
bilities, MA: management-address, ETS-C: ETS-Configuration, ETS-R: ETS-
Recommendation, AP: Application Priority, PFC: Priority Flow Control,
CEE: Converged Enhanced Ethernet DCBX version

Interface    Receive    Transmit    Notification    TLVs
-------------------------------------------------------------------------
eth1/1       Enable     Enable      Enable          PD,SN,SD,SC,MA,PFC,CEE
eth1/2       Disable    Disable     Enable          PD,SN,SD,MA,AP
eth1/3       Enable     Disable     Disable         PD,SD,SC,ETS-R,AP,PFC
...

switch (config)#
```

Related Commands	
Note	

show lldp interfaces ethernet <inf> remote

show lldp interfaces ethernet <inf> remote

Shows LLDP remote interface table information.

Syntax Description	inf	Local interface number (e.g. 1/1).
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.2.0300	First version
	3.3.4200	Updated output
Role	admin	

Example

```
switch (config)# show lldp interfaces ethernet <number> Ethernet <port-number> // example "Ethernet 1/1"
Latest LLDPDU received on <date> // e.g. date: "Thu Feb 14 12:08:29 2013" - new field
Remote Index:
Remote chassis id: <byte array> ; chassis id subtype: <sub-type>
Remote port-id: <byte array> ; port id subtype: <sub-type>
Remote port description: <byte array>
Remote system name: <byte array>
Remote system description: < byte array>
Remote system capabilities supported: <enum parced as defined in the MIB> ; enable <enum parced as defined in the
MIB>
Management Table //theoretially remote can send more then one management address (Future) RemoteIndex Subtype Address
ifSubtype ifId OID
1 ipV4(1) 10.10.10.10 ifIndex(2) 1(mgmt0) <Oid>
1 ipV4(1) 10.10.10.11 ifIndex(3) 2(mgmt1) <Oid>
Unknown TLVs Table //(Future) Type Info
------------------------------
<integer> <byte-array>
<integer> <byte-array>
Organizationally-Defined Information Table // (Future) OUI subtype Index DefInfo
------------------------------------------------------------
<byte-array> <integer> <integer> <byte-array>
<byte-array> <integer> <integer> <byte-array>
Remote PFC configuration // new section Willing: {enabled, disabled}
MACsec: {enabled, disabled}
Number of supported traffic classes: 4 // range is 1-8
PFC enabled on priorities: 5 7 // it could be "0 1 2 3 4 5 6 7" or " 1 3 7" or "None"
WARNING: peer PFC configuration does not match the local PFC configuration // This warning should appear only if the
local and remote PFC configuration don't match!
Remote ETS configuration // new section Willing: {enabled, disabled}
CBS: {enabled, disabled}
Number of supported traffic classes: 3 // range is 1-8
WARNING: peer ETS configuration does not match the local ETS configuration // This warning should appear only if the
local and remote ETS configuration don't match!
Priority assignment table: Priority TC
--------------
0
0
1
0
2
1
3
1
4
2
5
2
6
3
7
3
Traffic class bandwidth table // (No need to have the recommended TC - ETS-Recommended TLV)
TC Bandwidth TSA
----------------------------
Page 43 of 354
0 25% tsaStrictPriority(0) // we are expecting either 0 or 2 as answers.
```

Related Commands

Note

show lldp timers

show lldp timers

Shows LLDP timers configuration

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0300
Role	admin

Example	`switch (config)# show lldp timers`
	`msg-tx-interval:30`
	`tx-delay:2`
	`tx-hold:4`
	`tx-reinit-delay:2`
	`switch (config)#`

Related Commands	
Note	

show lldp statistics global

show lldp statistics global

Shows LLDP global statistics

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0300
Role	admin

Example	`switch (config)# show lldp timers`
	`Remote Table Last Change Time : 10300`
	`Remote Table Inserts : 5`
	`Remote Table Deletes : 0`
	`Remote Table Drops : 0`
	`Remote Table Ageouts : 0`
	`switch (config)#`

Related Commands	
Note	

show lldp statistics [interface ethernet <inf>]

show lldp statistics [interface ethernet <inf>]

Shows LLDP interface statistics

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0300
Role	admin

Example	`switch (config)# show lldp statistics ethernet 1/1`
	`Interface Frames In In TLVs TLVs Ageout Out`
	`Discarded Errors Total Discarded Unrecognize Frames`
	`---`
	`Eth 1/1 0 0 10 0 0 0 0`
	`switch (config)#`

Related Commands	
Note	

show dcb application-priority

show dcb application-priority

Displays application priority admin table.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.4200
Role	admin

Example	`switch (config)# show dcb application-priority`
	
	`Application priority configuration`
	
	`Selector  Protocol  Priority`
	`----------------------------`
	`Ethertype  0x8906  3`
	`Ethertype  0x8914  3`
	
	`switch (config)#`

Related Commands	
Note	

5.10 Quality of Service (QoS)

5.10.1 Priority Flow Control and Link Level Flow Control

Priority Flow Control (PFC) provides an enhancement to the existing pause mechanism in Ethernet. The current Ethernet pause option stops all traffic on a link. PFC creates eight separate virtual links on the physical link and allows any of these links to be paused and restarted independently, enabling the network to create a no-drop class of service for an individual virtual link. PFC has 8 possible priorities (3 bits in VLAN header). Each priority can be mapped to one of 4 possible queues in the ingress.

The PFC software offers the following features:

- Provides per-priority enabling or disabling of flow control
- Transmits PFC-PAUSE frames when the receive threshold for a particular traffic class is reached
- Provides the management capability for an administrator to configure the flow control properties on each port of the switch
- Keeps flow control disabled for all priorities on all ports by default
- Allows an administrator to enable or disable flow control per port and per priority level
- Supports flow control only on physical ports, not on logical interfaces such as tunnels or interfaces defined by sharing a physical port in multiple virtual switch contexts
- Uses the configured threshold values to set up the queue buffer spaces accordingly in the datapath
- Provides hardware abstraction layer callouts for the following:
  - Enabling or disabling of flow control on each port for each priority
  - Configuring the queue depth for each priority on each port
- Provides trace logs for execution upon error conditions and for any event notifications from the hardware or datapath. These trace logs are a useful aid in troubleshooting.
- Allows the administrator to configure the minimum and maximum threshold values for flow control. These configurations are applied globally on all ports and priorities.

Priority Based Flow Control (PFC) provides an enhancement to the existing pause flow control mechanism as described in 802.1X.

➢ ***To enable PFC globally:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Enable PFC globally on the switch. Run:

```
switch (config) # dcb priority-flow-control enable
This action might cause traffic loss while shutting down a port with priority-flow-con-
trol mode on
Type 'yes' to confirm  enable pfc globally: yes
```

➢ ***To enable PFC per priority:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Enable PFC globally on the switch. Run:

```
switch (config) # dcb priority-flow-control enable
# dcb priority-flow-control enable
This action might cause traffic loss while shutting down a port with priority-flow-con-
trol mode on
Type 'yes' to confirm  enable pfc globally: yes
switch (config) #
```

Step 4. Choose the desirable priority you want to enable using the command `dcb priority-flow-control priority <pri[0..7]> enable`.

```
switch (config) # dcb priority-flow-control priority 5 enable
```

➢ ***To enable PFC per interface:***

Step 1. Log in as admin.

Step 2. Change to config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Enable PFC globally on the switch. Run:

```
switch (config) # dcb priority-flow-control enable
```

Step 4. Choose the desirable priority you want to enable using the command `dcb priority-flow-control priority <pri[0..7]> enable`

```
switch (config) # dcb priority-flow-control 5 enable
```

Step 5. Change to Interface mode. Run:

```
switch (config) #
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) #
```

Step 6. Enable PFC for the specific interface:

```
switch (config interface ethernet 1/1) # dcb priority-flow-control mode on
```

5.10.2 Enhanced Transmission Selection (ETS)

Enhanced Transmission Selection (ETS) provides a common management framework for assignment of bandwidth to traffic classes, for weighted round robin (WRR) scheduling. If a traffic class does not use all the bandwidth allocated to it, other traffic classes can use that available bandwidth. This allows optimal utilization of the network capacity while prioritizing and providing the necessary resources.

The ETS feature has the following attributes:

- ETS global admin:
  - Enable (default) – scheduling mode is WRR according to the configured bandwidth-per-traffic class
  - Disable – scheduling mode is Strict Priority (SP)

- Bandwidth percentage for each traffic class: By default each traffic class gets an equal share

The default mapping of priority to traffic classes (per interface) is as follows:

- Priority 0,1 mapped to TC 0
- Priority 2,3 mapped to TC 1
- Priority 4,5 mapped to TC 2
- Priority 6,7 mapped to TC 3

TC0 and TC3 are lossy TCs, while TC1 and TC2 can be lossless as well as lossy. It is possible but not recommended to map PFC enabled priorities (lossless traffic) to those TC0 or TC3.

ETS is enabled by default (scheduling is WRR).

➢ ***To set the scheduling mode to Strict Priority:***

Step 1. Run the command `dcb ets disable`.

```
switch (config) # no dcb ets enable
```

➢ ***To configure the WRR bandwidth percentage:***

Step 1. Make sure ETS feature is enabled. Run:

```
switch (config) # dcb ets enable
```

Step 2. Choose the WRR bandwidth rate and distribution.

By default the WRR distribution function is equal 25% per TC. Changing the WRR bandwidth rate will cause a change in the distribution function, for example if you wish to schedule more traffic on TC-0, TC-1, TC-2 while reducing the amount of traffic sent on TC-3, run the command `dcb ets tc bandwidth`.

```
switch (config) # dcb ets tc bandwidth 30 30 30 10
# show dcb ets

ETS enabled

TC        Bandwidth
--------------------------
0         30%
1         30%
2         30%
3         10%

Number of Traffic Class: 4
switch (config) #
```

Traffic class priorities are <0-3>, where 0 is the lowest and 3 is the highest.

The sum of all traffic class bandwidth value (in percentage) should be 100, otherwise the command fails.

Step 3. Run the command `show dcb ets` to verify the configuration.

```
switch (config) # show dcb ets
ETS enabled

TC        Bandwidth
-------------------------
0         30%
1         30%
2         10%
3         30%

Number of Traffic Class: 4
switch (config) #
```

5.10.3 Commands

5.10.3.1 Enhanced Transmission Selection (ETS)

dcb ets enable

dcb ets enable
no dcb ets enable

Sets the switch egress scheduling mode to be weighted round robin.
The no form of the command sets the switch egress scheduling mode to be strict priority.

Syntax Description	N/A
Default	ETS is enabled.
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config)# dcb ets enable`
	`switch (config)# show dcb ets`
	
	`ETS enabled`
	
	`TC  Bandwidth`
	`--------------------------`
	`0  25%`
	`1  25%`
	`2  25%`
	`3  25%`
	
	`Number of Traffic Class: 4`
	
	`switch (config) #`

Related Commands	show dcb ets
Note	

dcb ets tc bandwidth

dcb ets tc bandwidth <tc-0> <tc-1> <tc-2> <tc-3>
no dcb ets tc bandwidth

Configures the bandwidth limit of the traffic class.
The no form of the command sets the bandwidths per traffic class back to its default.

Syntax Description	`tc-i` 0-100.
Default	25% per traffic class.
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config)# dcb ets tc bandwidth 20 20 30 30`
	`switch (config) # show dcb ets`
	
	`ETS enabled`
	
	`TC Bandwidth`
	`--------------------------`
	`0 20%`
	`1 20%`
	`2 30%`
	`3 30%`
	
	`Number of Traffic Class: 4`
	
	`switch (config) #`

Related Commands	show dcb ets
Note	The sum of all traffic class bandwidth must be equal to 100.

vlan map-priority

vlan map priority <priority> traffic-class <tc>
no vlan map priority <priority>

Maps an VLAN user priority to a traffic class.
The no form of the command sets the mapping back to default.

Syntax Description	N/A
Default	Priority 0,1 mapped to tc 0. Priority 2,3 mapped to tc 1. Priority 4,5 mapped to tc 2. Priority 6,7 mapped to tc 3.
Configuration Mode	Config Interface Ethernet
History	3.1.0000
Role	admin
Example	`switch (config interface ethernet 1/1) # vlan map-priority 1 traffic-class 2` `switch (config interface ethernet 1/1) #`
Related Commands	`show dcb ets interface`
Note	

show dcb ets

show dcb ets

Displays ETS configuration and operational data.

Syntax Description	
Default	ETS is enabled.
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin

Example	`switch (config)# show dcb ets`
	
	`ETS enabled`
	
	`TC Bandwidth`
	`--------------------------`
	`0 25%`
	`1 25%`
	`2 25%`
	`3 25%`
	
	`Number of Traffic Class: 4`
	
	`switch (config) #`

Related Commands	
Note	

show dcb ets interface

show dcb ets interface <type> <number>

Displays ETS configuration and operational data, per interface.

Syntax Description	type	ethernet or port-channel
	number	interface number, i.e. 1/1
Default	ETS is enabled.	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example

```
switch (config)# show dcb ets interface ethernet 1/1

ETS Port Mode             :ON MODE
ETS Oper State            :INIT STATE
ETS State Machine Type    :Assymetric
-----------------------------------------------
ETS Local Port Info
-----------------------------------------------
TC bandwidth table
-----------------------------------------------
TC        Bandwidth        RecomBandwidth
-----------------------------------------------
0         25%         25%
1         25%         25%
2         25%         25%
3         25%         25%

priority assignment table
--------------------------------------
Priority     TC
--------------------------------------
0          0
1          0
2          1
3          1
4          2
5          2
6          3
7          3

Number of Traffic Class: 4


Willing Status:  Disable
-----------------------------------------------
ETS Admin Port Info
-----------------------------------------------
TC        Bandwidth        RecomBandwidth
-----------------------------------------------
0         30%         30%
1         30%         30%
2         30%         30%
3         10%         10%

-----------------------------------------------
ETS Remote Port Info
-----------------------------------------------
No Remote Entry is Present
-----------------------------------------------
switch (config) #
```

Related Commands

Note

5.10.3.2 Priority Flow Control (PFC)

dcb priority-flow-control enable

dcb priority-flow-control enable
no dcb priority-flow-control enable

Enables PFC globally on the switch.
The no form of the command globally disables PFC on the switch.

Syntax Description	N/A
Default	PFC is disabled.
Configuration Mode	Config
History	3.1.0000 Initial revision 3.3.0000 Output update
Role	admin

Example	`switch (config)# dcb priority-flow-control enable`
	`This action might cause traffic loss while shutting down a port with priority-flow-control mode on`
	`Type 'yes' to confirm enable pfc globally: yes`
	`switch (config)# show dcb priority-flow-control`
	
	`PFC enabled`
	`Priority Enabled List    :`
	`Priority Disabled List   :0 1 2 3 4 5 6 7`
	
	`TC     Lossless`
	`---    ----------`
	`0           N`
	`1           Y`
	`2           Y`
	`3           N`
	
	`Interface      PFC admin        PFC oper`
	`------------   --------------   -------------`
	`1/1              Disabled         Disabled`
	`1/2              Disabled         Disabled`
	`1/3              Disabled         Disabled`
	`1/4              Disabled         Disabled`
	`...`
	`switch (config) #`

Related Commands	show dcb priority-flow-control
Note	This command asks the user to approve traffic loss because there might be interfaces with dcb mode on, that will be shutdown.

dcb priority-flow-control priority

dcb priority-flow-control priority <prio> enable
no dcb priority-flow-control priority <prio> enable

Enables PFC per priority on the switch.
The no form of the command disables PFC per priority on the switch.

Syntax Description	prio 0-7.
Default	PFC is disabled for all priorities.
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	
Related Commands	show dcb priority-flow-control
Note	

```
switch (config)# dcb priority-flow-control priority 0 enable
switch (config)# show dcb priority-flow-control

PFC enabled
Priority Enabled List    : 0
Priority Disabled List   : 1 2 3 4 5 6 7

TC     Lossless
---    ----------
0           N
1           Y
2           Y
3           N


Interface      PFC admin        PFC oper
------------   --------------   -------------
1/1              Disabled         Disabled
1/2              Disabled         Disabled
1/3              Disabled         Disabled
1/4              Disabled         Disabled
...
switch (config) #
```

dcb priority-flow-control mode on

dcb priority-flow-control mode on [force]
no dcb priority-flow-control mode

Enables PFC per interface.
The no form of the command disables PFC per interface.

Syntax Description	force	Force command implementation.

Default

PFC is disabled for all interfaces.

Configuration Mode

Config Interface Ethernet
Config Interface Port Channel
Config Interface MLAG Port Channel

History

3.1.0000	
3.3.4500	Added MLAG port-channel configuration mode

Role

admin

Example

```
switch (config interface ethernet 1/1) # dcb priority-flow-control mode
on
switch (config interface ethernet 1/1) # show dcb priority-flow-control

PFC enabled
Priority Enabled List    : 0
Priority Disabled List   : 1 2 3 4 5 6 7

TC     Lossless
---    ----------
0           N
1           Y
2           Y
3           N


Interface      PFC admin        PFC oper
------------   --------------   -------------
1/1              On               Enabled
1/2              Disabled         Disabled
1/3              Disabled         Disabled
1/4              Disabled         Disabled
...
switch (config) #
```

Related Commands

show dcb priority-flow-control

Note

show dcb priority-flow-control

show dcb priority-flow-control [interface <type> <inf>] [detail]

Displays DCB priority flow control configuration and status.

Syntax Description	type	• ethernet • port-channel
	inf	The interface number.
	detail	Adds details information to the show output.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	
Example		

```
switch (config interface ethernet 1/1) # show dcb priority-flow-control

PFC enabled
Priority Enabled List    : 0
Priority Disabled List   : 1 2 3 4 5 6 7

TC     Lossless
---    ----------
0           N
1           Y
2           Y
3           N


Interface      PFC admin        PFC oper
------------   --------------   -------------
1/1              On               Enabled
1/2              Disabled         Disabled
1/3              Disabled         Disabled
1/4              Disabled         Disabled
...
switch (config) #
```

Related Commands	
Note	

5.11 Access Control List

An Access Control List (ACL) is a list of permissions attached to an object, to filter or match switches packets. When the pattern is matched at the hardware lookup engine, a specified action (e.g. permit/deny) is applied. The rule fields represent flow characteristics such as source and destination addresses, protocol and VLAN ID.

ACL support currently allows actions of *permit* or *deny* rules, and supports only ingress direction. ACL search pattern can be taken from either L2 or L3 fields, e.g L2/L3 source and destination addresses, protocol, VLAN ID and priority or TCP port.

5.11.1 Configuring Access Control List

Access Control List (ACL) is configured by the user and is applied to a port once the ACL search engine matches search criteria with a received packet.

➢ ***To configure ACL:***

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

```
switch > enable
switch # configure terminal
```

Step 3. Create a MAC / IPv4 ACL (access-list) entity.

```
switch (config) mac access-list mac-acl
switch (config mac access-list mac-acl) #
```

Step 4. Add a MAC / IP rules to the appropriate access-list.

```
switch (config mac access-list mac-acl)seq-number 10 deny 0a:0a:0a:0a:0a:0a mask
ff:ff:ff:ff:ff:ff any vlan 6 cos 2 protocol 80
switch (config mac access-list mac-acl) #
```

Step 5. Bind the created access-list to an interface (slot/port or port-channel).

```
switch (config)
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) # mac port access-group mac-acl
```

5.11.2 ACL Actions

An ACL action is a set of actions can be activated in case the packet hits the ACL rule.

➢ ***To modify the VLAN tag of the egress traffic as part of the ACL "permit" rule:***

Step 1. Create access-list action profile:

a. Create an action access-list profile using the command `access-list action <action-profile-name>`

b. Add rule to map a VLAN using the command `vlan-map <vlan-id>` within the action profile configuration mode

Step 2. Create an access-list and bind the action rule:

a. Create an access-list profile using the command `ipv4/mac access-list`

b. Add access list rule using the command `deny/permit (action <action profile name>)`

Step 3. Bind the access-list to an interface using the command `ipv4/mac port access-group`

```
Create an action profile and add vlan mapping action:
switch (config)#access-list action my-action
switch (config access-list action my-action) # vlan-map 20
switch (config access-list action my-action) #exit

Create an access list and bind rules:
switch (config)# mac access-list my-list
switch (config mac access-list my-list)# permit any any action my-action
switch (config mac access-list my-list)# exit

Bind an access-list to a port:
Switch (config)# interface ethernet 1/1
Switch (config interface ethernet 1/1)# mac port access-group my-list
```

5.11.3 Commands

ipv4/mac access-list

{ipv4 | mac} access-list <acl-name>
no {ipv4 | mac} access-list <acl-name>

Creates a MAC or IPv4 ACL and enter the ACL configuration mode.
The no form of the command deletes the ACL.

Syntax Description	ipv4 | mac	IPv4 or MAC – access list.
	acl-name	User defined string for the ACL.
Default	No ACL available by default.	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	
Example	`switch (config)# mac access-list my-mac-list` `switch (config mac access-list my-mac-list)#`	
Related Commands	ipv4/port access-group	
Note		

ipv4/mac port access-group

{ipv4 | mac} port access-list <acl-name>
no {ipv4 | mac} port access-list <acl-name>

Binds an ACL to the interface.
The no form of the command unbinds the ACL from the interface.

Syntax Description	ipv4 | mac	IPv4 or MAC – access list.
	acl-name	ACL name.
Default	No ACL is bind by default.	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
History	3.1.1400	
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	
Example	`switch (config interface ethernet 1/1) # mac port access-group my-list` `switch (config interface ethernet 1/1) #`	
Related Commands	ipv4/mac access-list	
Note	The access control list should be defined prior to the binding action.	

deny/permit (MAC ACL rule)

[seq-number <sequence-number>] {deny|permit} {any | <source-mac> [mask <mac>]} {any |<destination-mac> [mask <mac>]} [protocol <protocol>] [cos <cos-value>] [vlan <vlan-id> | vlan-mask <vlan-mask>] [action <action-id>] no <sequence-number>

Creates a rule for MAC ACL.
The no form of the command deletes a rule from the MAC ACL.

Syntax Description	sequence-number	Optional parameter to set a specific sequence number for the rule. The range is:1-500.
	deny | permit	Determines the type of the rule, denies or permits action.
	{any | <source-mac> [mask <mac>]}	Sets source MAC and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the source MAC.
	{any | <destination-mac> [mask <mac>]}	Sets destination MAC and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the destination MAC.
	protocol	Sets the Ethertype filed value from the MAC address. Possible range is: 0x0000-0xffff.
	cos-value	Sets the COS (priority bits) field, possible range is: 0-7.
	vlan-id	Sets the VLAN ID field, possible range is 0-4095.
	vlan-mask <vlan-mask>	Sets VLAN group. Range: 0x0000-0x0FFF.
	action	Action name (free string).
Default	No rule is added by default to access control list. Default sequence number is in multiple of 10.	
Configuration Mode	Config MAC ACL	
History	3.1.1400	
	3.3.4500	Added vlan-mask parameter
Role	admin	
Example	`switch (config mac access-list my-list) # seq-number 10 deny 0a:0a:0a:0a:0a:0a mask ff:ff:ff:ff:ff:ff any vlan 6 cos 2 protocol 80` `switch (config mac access-list my-list) #`	
Related Commands	ipv4/mac access-list ipv4/mac port access-group	
Note		

deny/permit (IPv4 ACL rule)

[seq-number <sequence-number>] {permit | deny} ip {<source-ip> [mask <ip>] | [any]} {<dest-ip> [mask <ip>] | [any]} [action <action-id>]
no <sequence-number>

Creates a rule for IPv4 ACL.
The no form of the command deletes a rule from the IPv4 ACL.

Syntax Description	sequence-number	Optional parameter to set a specific sequence number for the rule. The range is:1-500.
	deny | permit	Determines the type of the rule, deny or permit action. Valid mask values fall in the range 0-255.
	{any | <source-ip> [mask <ip>]}	Sets source IP and optionally sets a mask for that IP address. The “any” option causes the rule to not check the source IP. Valid mask values fall in the range 0-255.
	{any | <destination-ip> [mask <ip>]}	Sets destination IP and optionally sets a mask for that MAC. The “any” option causes the rule to not check the destination MAC.
Default	No rule is added by default to access control list. Default sequence number is in multiple of 10.	
Configuration Mode	Config IPv4 ACL	
History	3.1.1400	First version
	3.3.4302	Updated syntax description of mask <ip> parameter
Role	admin	
Example	`switch (config ipv4 access-list my-list) # seq-number 51 deny ip 1.1.1.1 mask 123.12.13.53 45.45.45.0 mask 123.132.21.123` `switch (config ipv4 access-list my-list) #`	
Related Commands	ipv4/mac access-list ipv4/mac port access-group	
Note		

deny/permit (IPv4 TCP/UDP ACL rule)

[seq-number <sequence-number>] {permit | deny} {tcp | udp} {<source-ip> [mask <ip>] | [any]} {<dest-ip> [mask <ip>]| [any]} [eq-source <port-number>] [eq-destination <port-number>] [action <action-id>]
no <sequence-number>

Creates a rule for IPv4 UDP/TCP ACL.
The no form of the command deletes a rule from the ACL.

Syntax Description	sequence-number	Optional parameter to set a specific sequence number for the rule. The range is:1-500.
	deny | permit	Determines the type of the rule, deny or permit action.
	tcp | udp	UDP or TCP rule transport type.
	{any | <source-ip> [mask <ip>]}	Sets source IP and optionally sets a mask for that IP address. The “any” option will cause the rule not to check the source IP.
	{any | <destination-ip> [mask <ip>]}	Sets destination IP and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the destination MAC.
	[eq-source <port-number>]	TCP/UDP source port number. Range is 0-65535.
	[eq-destination <port-number>]	TCP/UDP destination port number. Range is 0-65535.
Default	No rule is added by default to access control list. Default sequence number is in multiple of 10.	
Configuration Mode	Config IPv4 ACL	
History	3.1.1400	
Role	admin	
Example	`switch (config ipv4 access-list my-list) # seq-number 10 deny tcp any any eq-source 1200` `switch (config ipv4 access-list my-list) #`	
Related Commands	ipv4/mac access-list ipv4/mac port access-group	
Note		

access-list action

access-list action <action-profile-name>
no access-list action <action-profile-name>

Creates access-list action profile and entering the action profile configuration mode. The no form of the command deletes the action profile.

Syntax Description	action-profile-name given name for the profile.
Default	N/A
Configuration Mode	Config
History	3.2.0230
Role	admin

Example	`switch (config)# access-list action my-action`
	`switch (config access-list action my-action)# show access-list action my-action`
	`Access-list Action my-action`
	`Mapped_Vlan_ID |Mapped_port |Counter_set |Policer_ID |`
	`==========================================================`
	`N/A |N/A |N/A |N/A |`
	`switch (config access-list action my-action)#`

Related Commands	
Note	

vlan-map

vlan-map <vlan-id>
no vlan-map

Adds action to map a new VLAN to the packet (in the ingress port or VLAN).
The no form of the command removes the action to map a new VLAN.

Syntax Description	vlan-id 0-4095.
Default	N/A
Configuration Mode	Config
History	3.2.0230
Role	admin

Example	`switch (config access-list action my-action)# vlan-map 10`
	`switch (config access-list action my-action)# show access-list action my-action`
	`Access-list Action my-action`
	`Mapped_Vlan_ID |Mapped_port |Counter_set |Policer_ID |`
	`==========================================================`
	`10 |N/A |N/A |N/A |`
	`switch (config access-list action my-action)#`

Related Commands	
Note	

show access-list action

show access-list action {<action-profile-name> | summary}

Displays the access-list action profiles summary.

Syntax Description	action-profile-name	Filter the table according to the action profile name.
	summary	Display summary of the action list.
Default	N/A	
Configuration Mode	Config	
History	3.2.0230	
Role	admin	
Example	witch (config access-list action my-action)# show access-list action my-action Access-list Action my-action Mapped_Vlan_ID |Mapped_port |Counter_set |Policer_ID | ========== 10 |N/A |N/A |N/A | switch (config access-list action my-action)#	
Related Commands		
Note		

show mac/ipv4 access-lists

show [mac |ipv4 |] access-lists <access-list-name>

Displays the list of rules for the MAC/IPv4 ACL.

Syntax Description	ipv4 | mac	IPv4 or MAC - access list.
	access-list-name	ACL name.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
History	3.3.4500	Updated output
Role	admin	

Example	`switch (config mac access-list my-list) # show mac access-lists my-list`
	`mac access-list my-list`
	`seq-number|p/d  |smac |dmac |protocol|cos  |vlan |vlan-mask|action|`
	`==========================================================================`
	`10        |deny  |any  |any  |0800    |3    |3    |0x0FFF   |none  |`
	`20        |deny  |any  |any  |80      |2    |6    |0x0000   |none  |`
	`30        |deny  |any  |any  |any     |any  |any  |0x0ACB   |none  |`
	`40        |deny  |any  |any  |any     |any  |any  |N/A      |none  |`
	`switch (config mac access-list my-list) #`	

Related Commands	deny/permit (MAC ACL rule) deny/permit (IPv4 ACL rule) deny/permit (IPv4 TCP/UDP ACL rule) ipv4/mac access-list ipv4/mac port access-group	
Note		

show mac/ipv4 access-lists summary

show [mac |ipv4 |] access-lists summary

Displays the summary of number of rules per ACL, and the interfaces attached.

Syntax Description	ipv4 | mac	IPv4 or MAC - Access list
	access-list-name	ACL name
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
Role	admin	

Example	`switch (config) # show mac access-lists summary`
	`mac access-list my-list`
	`Total ACEs Configured: 2`
	`Configured on interfaces:`
	`Ethernet 1/1`
	`Ethernet 1/2`
	`switch (config) #`	

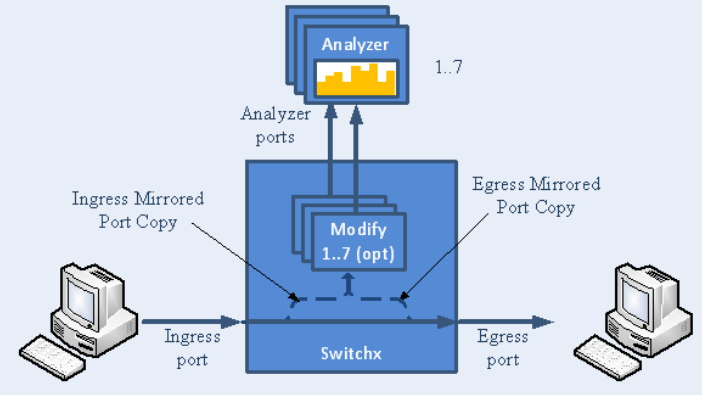
Related Commands	deny/permit (MAC ACL rule) deny/permit (IPv4 ACL rule) deny/permit (IPv4 TCP/UDP ACL rule) ipv4/mac access-list ipv4/mac port access-group	
Note		

5.12 Port Mirroring

Port mirroring enables data plane monitoring functionality which allows the user to send an entire traffic stream for testing. Port mirroring sends a copy of packets of a port's traffic stream, called "mirrored port", into an analyzer port. Port mirroring is used for network monitoring. It can be used for intrusion detection, security breaches, latency analysis, capacity and performance matters, and protocol analysis.

Figure 15 provides an overview of the mirroring functionality.

Figure 15: Overview of Mirroring Functionality

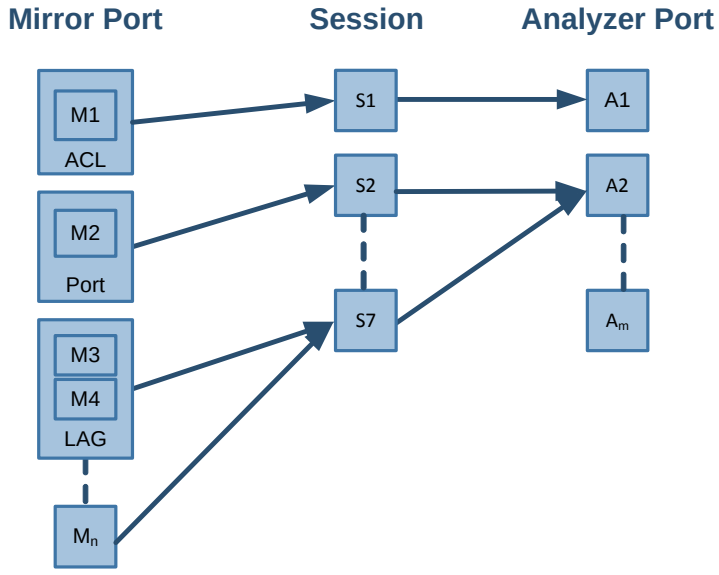


There is no limitation on the number of mirroring sources and more than a single source can be mapped to a single analyzer destination.

5.12.1 Mirroring Sessions

Port mirroring is performed by configuring mirroring sessions. A session is an association of a mirror port (or more) and an analyzer port.

Figure 16: Mirror to Analyzer Mapping



A mirroring session is a monitoring configuration mode that has the following parameters:

Table 22 - Mirroring Parameters

Parameter	Description	Access
Source interface(s)	List of source interfaces to be mirrored.	RW
Destination interface	A single analyzer port through which all mirrored traffic egress.	RW
Header format	The format and encapsulation of the mirrored traffic when sent to analyzer.	RW
Truncation	Enabling truncation segments each mirrored packet to 64 bytes.	RW
Congestion control	Controls the behavior of the source port when destination port is congested.	RW
Admin state	Administrative state of the monitoring session.	RW

5.12.1.1 Source Interface

The source interface (mirror port) refers to the interface from which the traffic is monitored. Port mirroring does not affect the switching of the original traffic. The traffic is simply duplicated and sent to the analyzer port. Traffic in any direction (either ingress, egress or both) can be mirrored.

There is no limitation on the number of the source interfaces mapped to a mirroring session.

Ingress and egress traffic flows of a specific source interface can be mapped to two different sessions.

LAG

The source interface can be a physical interface or a LAG.

Port mirroring can be configured on a LAG interface but not on a LAG member. When a port is added to a mirrored LAG it inherits the LAG's mirror configuration. However, if port mirroring configuration is set on a port, that configuration must be removed prior to adding the port to a LAG interface.

When a port is removed from a LAG, the mirror property is switched off for that port.

Control Protocols

All control protocols captured on the mirror port are forwarded to the analyzer port in addition to their normal treatment. For example LACP, STP, and LLDP are forwarded to the analyzer port in addition to their normal treatment by the CPU.

Exceptions to the behavior above are the packets that are being handled by the MAC layer, such as pause frames.

5.12.1.2 Destination Interface

The destination interface is an analyzer port is one to which mirrored traffic is sent. The mirrored packets, are duplicated, optionally modified and sent to the analyzer port. The SwitchX® platform supports up to 7 analyzer ports where any mirror port can be mapped to any analyzer port and more than a single mirror port can be mapped to a single analyzer port.

Packets can be forwarded to any destination using the command `destination interface`.

The analyzer port supports status and statistics as any other port.

LAG

The destination interface cannot be a member of LAG when the header format is local.

Control Protocols

The destination interface may also operate in part as a standard port, receiving and sending out non-mirrored traffic. When the header format is configured as a local port, ingress control protocol packets that are received by the local analyzer port get discarded.

Advanced MTU Considerations

The analyzer port, like its counterparts, is subject to MTU configuration. It does not send packets longer than configured.

When the analyzer port sends encapsulated traffic, the analyzer traffic has additional headers and therefore longer frame. The MTU must be configured to support the additional length, otherwise, the packet is truncated to the configured MTU.

The system on the receiving end of the analyzer port must be set to handle the egress traffic. If it is not, it might discard it and indicate this in its statistics (packet too long).

5.12.1.3 Header Format

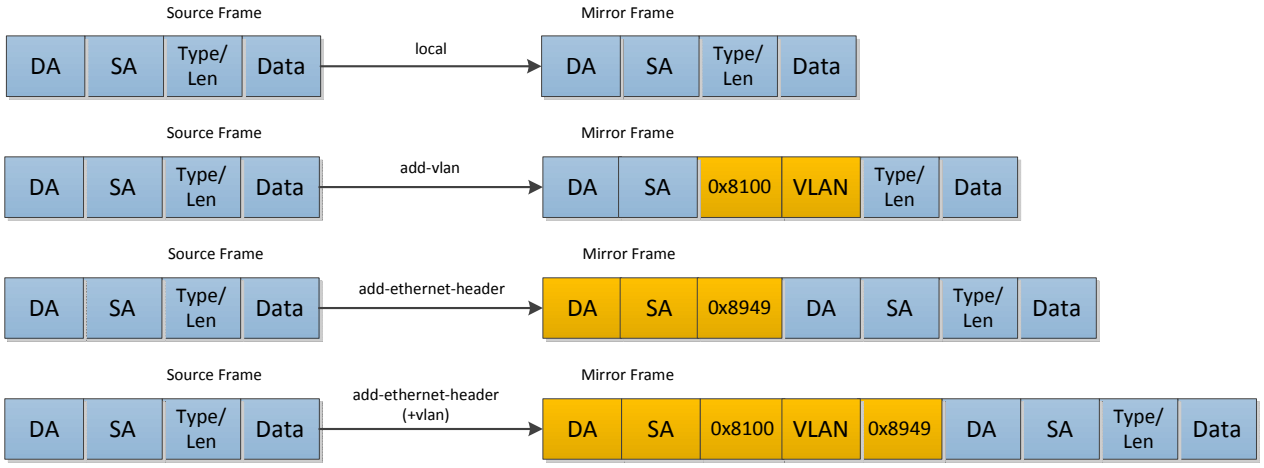
Ingress traffic from the source interface can be manipulated in several ways depending on the network layout using the command `header-format`.

If the analyzer system is directly connected to the destination interface, then the only parameters that can be configured on the port are the MTU, speed and port based flow control. Priority flow control is not supported is this case. However, if the analyzer system is indirectly connected to the destination interface, there are two options for switching the mirrored data to the analyzer system:

- A VLAN tag may be added to the Ethernet header of the mirrored traffic
- An Ethernet header can be added with include a new destination address and VLAN tag

It must be taken into account that adding headers increases packet size.

Figure 17: Header Format Options



5.12.1.4 Congestion Control

The destination ports might receive pause frames that lead to congestion in the switch port. In addition, too much traffic directed to the analyzer port (for example 40GbE mirror port is directed into 10G analyzer port) might also lead to congestion.

In case of congestion:

- When best effort mode is enabled on the analyzer port, SwitchX drops excessive traffic headed to the analyzer port using tail drop mechanism, however, the regular data (mirrored data heading to its original port) does not suffer from a delay or drops due to the analyzer port congestion.
- When the best effort mode on the analyzer port is disabled, the SwitchX does not drop the excessive traffic. This might lead to buffer exhaustion and data path packet loss.

The default behavior in congestion situations is to drop any excessive frames that may clog the system.

ETS, PFC and FC configurations do not apply to the destination port.

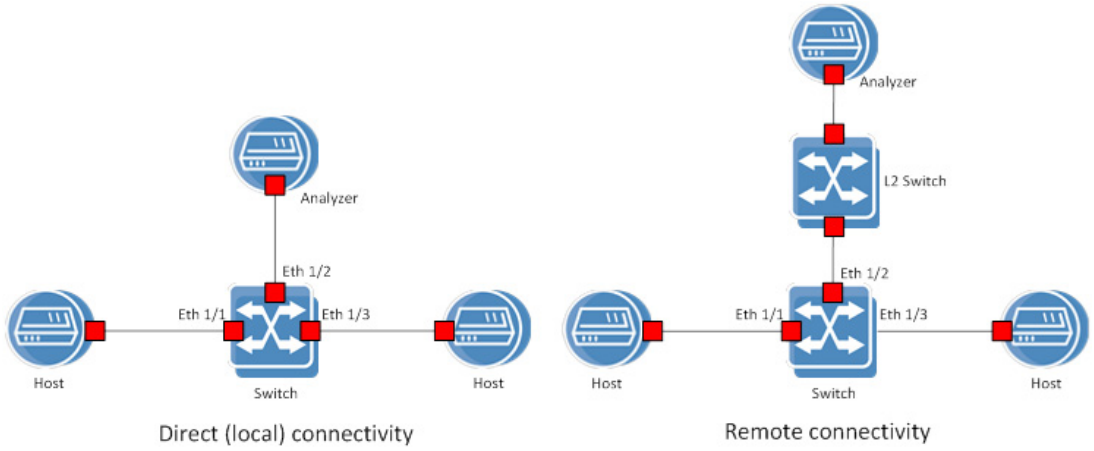
5.12.1.5 Truncation

When enabled, the system can truncate the mirrored packets into smaller 64-byte packets (default) which is enough to capture the packets' L2 and L3 headers.

5.12.2 Configuring Mirroring Sessions

Figure 18 presents two network scenarios with direct and remote connectivity to the analyzer equipment. Direct connectivity is when the analyzer is connected to the analyzer port of the switch. In this case there is no need for adding an L2 header to the mirrored traffic. Remote connectivity is when the analyzer is indirectly connected to the analyzer port of the switch. In this situation, adding an L2 header may be necessary depending on the network's setup.

Figure 18: Mirroring Session



➢ ***To configure a mirroring session:***

Step 1. Create a session. Run:

```
switch (config) # monitor session 1
```

This command enters a monitor session configuration mode. Upon first implementation the command also creates the session.

Step 2. Add source interface(s). Run:

```
switch (config monitor session 1) # add source interface ethernet 1/1 direction both
```

Step 3. Add destination interface. Run:

```
switch (config monitor session 1) # destination interface ethernet 1/2
```

Step 4. (Optional) Set header format. Run:

```
switch (config monitor session 1) # header-format add-ethernet-header destination-mac
00:0d:ec:f1:a9:c8 add-vlan 10 priority 5 traffic-class 2
```

For remote connectivity use the header formats `add-vlan` or `add-ethernet-header`. For local connectivity, use `local`.

Step 5. (Optional) Truncate the mirrored traffic to 64-byte packets. Run:

```
switch (config monitor session 1) # truncate
```

Step 6. (Optional) Set congestion control. Run:

```
switch (config monitor session 1) # congestion pause-excessive-frames
```

The default for this command is to drop excessive frames. The `pause-excessive-frames` option uses flow control to regulate the traffic from the source interfaces.

If the option `pause-excessive-frame` is selected, make sure that flow control is enabled on **all** source interfaces on the ingress direction of the monitoring session using the command `flowcontrol` in the interface configuration mode.

Step 7. Enable the session. Run:

```
switch (config monitor session 1) # no shutdown
```

5.12.3 Verifying Mirroring Sessions

- ***To verify the attributes of a specific mirroring session:***

```
switch (config) # show monitor session 1
Admin: Enable
Status: Up
Truncate: Enable
Destination interface: eth1/2
Congestion type: pause-excessive-frames
Header format: add-ethernet-header
                  - traffic class 2
                  - vlan 10
                  - priority 5
                  - destination-mac 00:0d:ec:f1:a9:c8

Source interfaces
Interface  direction
-------------------------
eth1/1     both
```

- ***To verify the attributes of running mirroring sessions:***

```
switch (config) # show monitor session summary
Session  Admin        Status     Mode       Destination    Source
1        Enable       Up         add-eth    eth1/2         eth1/1(b)
2        Disable      Down       add-vlan   eth1/2         eth1/8(i), po1(e)
3        Enable       Up         add-eth    eth1/5         eth1/18(e)
7        Disable      Down       local
```

5.12.4 Commands

5.12.4.1 Config

monitor session

monitor session <session-id>
no monitor session <session-id>

Creates session and enters monitor session configuration mode upon using this command for the first time.
The no form of the command deletes the session.

Syntax Description	session-id	The monitor session ID. The range is 1-7.
Default	N/A	
Configuration Mode	Config	
History	3.3.3500	
Role	admin	
Example	`switch (config)# monitor session 1` `switch (config monitor session 1)#`	
Related Commands		
Note		

5.12.4.2 Config Monitor Session

destination interface

destination interface <type> <number> [force]
no destination interface

Sets the egress interface number.
The no form of the command deletes the destination interface.

Syntax Description	interface <type> <number>	Sets the interface type and number (e.g. ethernet 1/2)
	force	The user does not need to shutdown the port prior the operation.
Default	no destination interface	
Configuration Mode	Config Monitor Session	
History	3.3.3500	First version
	3.3.4100	Added force argument
Role	admin	
Example	`switch (config monitor session 1) # destination interface ethernet 1/2` `switch (config monitor session 1)#`	
Related Commands		
Note		

shutdown

shutdown
no shutdown

Disables the session.
The no form of the command enables the session.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config Monitor Session
History	3.3.3500
Role	admin
Example	`switch (config monitor session 1) # no shutdown` `switch (config monitor session 1)#`
Related Commands	
Note	

add source interface

add source interface <type> <number> direction <d-type>
no source interface <type> <number>

Adds a source interface to the mirrored session.
The no form of the command deletes the source interface.

Syntax Description	interface <type> <number>	Configures interface as “ethernet” or “port-channel”.
	direction <d-type>	Configures the direction of the mirrored traffic. The options are as follows: • egress – sets the egress traffic to be monitored • ingress – sets the ingress traffic to be monitored • both – sets egress and ingress traffic to be monitored
Default	N/A	
Configuration Mode	Config Monitor Session	
History	3.3.3500	
Role	admin	
Example	`switch (config monitor session 1) # add source interface ethernet 1/1 direction both` `switch (config monitor session 1)#`	
Related Commands		
Note	If mirroring is configured in one direction (e.g. ingress) on an interface and then is configured in the other direction (e.g. egress), then the ultimate setting is “both”.	

header-format

header-format {local [traffic-class <tc>] | add-vlan <vlan-id> [priority <prio>] [traffic-class <tc>] | add-ethernet-header destination-mac <mac-address> [add-vlan <vlan-id> [priority <prio>]] [traffic-class <tc>]}
no header-format

Sets the header format of the mirrored traffic.
The no form of the command resets the parameter values back to default.

Syntax Description	local	The mirrored header of the frame is not changed.
	traffic-class <tc>	Changes the egress traffic class of the frame. Range is 0-3.
	add-vlan <vlan-id>	An 802.1q VLAN tag is added to the frame.
	priority <prio>	The priority to be added to the Ethernet header. Range is 0-7.
	add-ethernet-header	Adds an Ethernet header to the mirrored frame.
	destination-mac	The destination MAC address of the added Ethernet frame.
Default	no-change vlan 1 priority 0 traffic-class 0	
Configuration Mode	Config Monitor Session	
History	3.3.3500	
Role	admin	
Example	`switch (config monitor session 1) # header-format add-ethernet-header destination-mac 00:0d:ec:f1:a9:c8 add-vlan 10 priority 5 traffic-class 2` `switch (config monitor session 1)#`	
Related Commands		
Note	If add-ethernet-header is used, the source MAC address is the one attached to the switch.	

truncate

truncate
no truncate

Truncates the mirrored frames to 64-byte packets.
The no form of the command disables truncation.

Syntax Description	N/A
Default	no truncate
Configuration Mode	Config Monitor Session
History	3.3.3500
Role	admin
Example	`switch (config monitor session 1) # truncate` `switch (config monitor session 1)#`
Related Commands	
Note	This command applies for all sessions on the same analyzer port.

congestion

congestion [drop-excessive-frames | pause-excessive-frames]
no congestion

Sets the system's behavior when congested
The no form of the command disables truncation.

Syntax Description	drop-excessive-frames	Drops excessive frames.
	pause-excessive-frames	Pauses excessive frames.
Default	drop-excessive-frames	
Configuration Mode	Config Monitor Session	
History	3.3.3500	
	3.3.4000	Added Syntax Description.
Role	admin	
Example	`switch (config monitor session 1) # congestion pause-excessive-frames` `switch (config monitor session 1)#`	
Related Commands		
Note	This command applies for all sessions on the same analyzer port.	

5.12.4.3 Show

show monitor session

show monitor session <session-id>

Displays monitor session configuration and status.

Syntax Description	session-id	The monitor session ID. Range is 1-7.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.3500	
Role	admin	

Example	`switch (config) # show monitor session 1`
	`Admin: Enable`
	`Status: Up`
	`Truncate: Enable`
	`Destination interface: eth1/2`
	`Congestion type: pause-excessive-frames`
	`Header format: add-ethernet-header`
	`- traffic class 2`
	`- vlan 10`
	`- priority 5`
	`- destination-mac 00:0d:ec:f1:a9:c8`
	`Source interfaces`
	`Interface direction`
	`------------------------`
	`eth1/1 both`
	`switch (config) #`	

Related Commands		
Note		

show monitor session summary

show monitor session summary

Displays monitor session configuration and status summary.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.3500
Role	admin

Example	`switch (config) # show monitor session summary`
	`Session  Admin   Status  Mode      Destination  Source`
	`1        Enable  Up      add-eth   eth1/2       eth1/1(b)`
	`2        Disable Down    add-vlan  eth1/2       eth1/8(i), po1(e)`
	`3        Enable  Up      add-eth   eth1/5       eth1/18(e)`
	`7        Disable Down    local`
	`switch (config) #`

Related Commands	
Note	

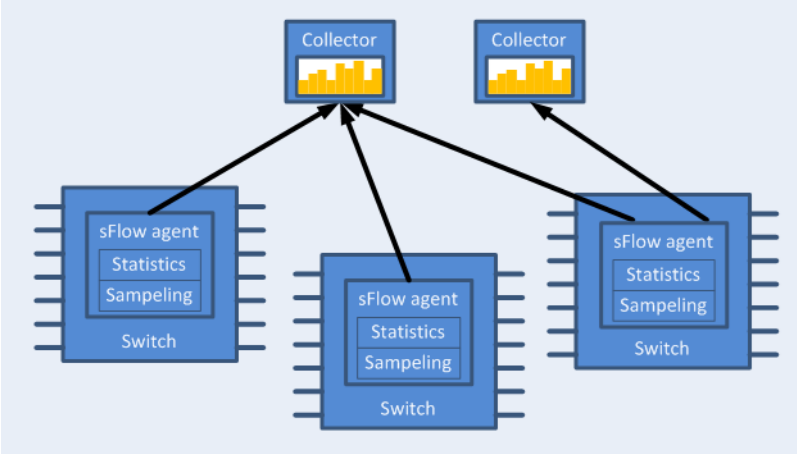
5.13 sFlow

sFlow (ver. 5) is a procedure for statistical monitoring of traffic in networks. MLNX-OS supports an sFlow sampling mechanism (agent), which includes collecting traffic samples and data from counters. The sFlow datagrams are then sent to a central collector.

The sampling mechanism must ensure that any packet going into the system has an equal chance of being sampled, irrespective of the flow to which it belongs. The sampling mechanism provides the collector with periodical information on the amount (and load) of traffic per interface by loading the counter samples into sFlow datagrams.

The sFlow packets are encapsulated and sent in UDP over IP. The UDP port number that is used is the standard 6343 by default.

Figure 19: sFlow Functionality Overview



5.13.1 Flow Samples

The sFlow agent samples the data path packet based.

Truncation and sampling rate are the two parameters that influence the flow samples. In case of congestion the flow samples can be truncated to a predefined size before it is being assigned to the CPU. The truncation can be set to any value between 64 to 256 bytes with the default being 128 bytes. Furthermore, the sampling rate may also be adjust as required.

5.13.2 Statistical Samples

The sFlow agent samples interface counters time based. Polling interval is configurable to any value between 5-3600 seconds with the default being 20 seconds.

The following statistics are gathered by the CPU:

Table 23 - List of Statistical Counters

Counter	Description
Total packets	The number of packets that pass through sFlow-enabled ports.
Number of flow samples	The number of packets that are captured by the sampling mecha-nism.
Number of statistic samples	The number of statistical samples.

Table 23 - List of Statistical Counters

Counter	Description
Number of discarded samples	The number of samples that were discarded.
Number of datagrams	The number of datagrams that were sent to the collector.

5.13.3 sFlow Datagrams

The sFlow datagrams contain flow samples and statistical samples.

The sFlow mechanism uses IP protocol, therefore if the packet length is more than the interface MTU, it becomes fragmented by the IP stack. The MTU may also be set manually to anything in the range of 200-9216 bytes. The default is 1400 bytes.

5.13.4 Sampled Interfaces

sFlow must be enabled on physical or LAG interfaces that require sampling. When adding a port to a LAG, sFlow must be disabled on the port. If a port with enabled sFlow is configured to be added to a LAG, the configuration is rejected. Removing a port from a LAG disables sFlow on the port regardless of the LAG's sFlow status.

5.13.5 Configuring sFlow

➢ ***To configure the sFlow agent:***

Step 1. Unlock the sFlow commands. Run:

```
switch (config) # protocol sflow
```

Step 2. Enable sFlow on the system. Run:

```
switch (config) # sflow enable
```

Step 3. Enter sFlow configuration mode. Run:

```
switch (config) # sflow
switch (config sflow) #
```

Step 4. Set the central collector's IP. Run:

```
switch (config sflow) # collector-ip 10.10.10.10
```

Step 5. Set the agent-ip used in the sFlow header. Run:

```
switch (config sflow) # agent-ip 20.20.20.20
```

Step 6. (Optional) Set the sampling rate of the mechanism. Run:

```
switch (config sflow) # sampling-rate 16000
```

This means that one every 16000 packet gets collected for sampling.

Step 7. (Optional) Set the maximum size of the data path sample. Run:

```
switch (config sflow) # max-sample-size 156
```

Step 8. (Optional) Set the frequency in which counters are polled. Run:

```
switch (config sflow) # counter-poll-interval 19
```

Step 9. (Optional) Set the maximum size of the datagrams sent to the central collector. Run:

```
switch (config sflow) # max-datagram-size 1500
```

Step 10. Enable the sFlow agent on the desired interfaces. Run:

```
switch (config interface ethernet 1/1)# sflow enable
switch (config interface port-channel 1)# sflow enable
```

5.13.6 Verifying sFlow

- ***To verify the attributes of the sFlow agent:***

```
switch (config)# show sflow

sflow protocol enabled
sflow enabled
sampling-rate 16000
max-sampled-size 156
counter-poll-interval 19
max-datagram-size 1500
collector-ip 10.10.10.10
collector-port 6343
agent-ip 20.20.20.20

Interfaces
Ethernet: eth1/1
Port-channel: po1

Statistics:
Total Packets: 2000
Number of flow samples: 1200
Number of samples discarded: 0
Number of statistic samples: 800
Number of datagrams: 300
```

5.13.7 Commands

5.13.7.1 Config

protocol sflow

protocol sflow
no protocol sflow

Unhides the sFlow commands.
The no form of the command deletes sFlow configuration and hides the sFlow commands.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.3500
Role	admin
Example	`switch (config) # protocol sflow` `switch (config) #`
Related Commands	
Note	

sflow enable (global)

sflow enable
no sflow enable

Enables sFlow in the system.
The no form of the command disables sFlow without deleting the configuration.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.3500
Role	admin
Example	`switch (config) # sflow enable` `switch (config) #`
Related Commands	
Note	

sflow

sflow

Enters sFlow configuration mode.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.3.3500
Role	admin
Example	`switch (config) # sflow` `switch (config sflow) #`
Related Commands	
Note	

5.13.7.2 Config sFlow

sampling-rate

sampling-rate <rate>
no sampling-rate

Sets sFlow sampling ratio.
The no form of the command resets this parameter to its default value.

Syntax Description	rate	Sets the number of packets passed before selecting one for sampling. The range is 4000-16777215. Zero disables sampling.
Default	16000	
Configuration Mode	Config sFlow	
History	3.3.3500	
Role	admin	
Example	`switch (config sflow) # sampling-rate 16111` `switch (config sflow) #`	
Related Commands		
Note		

max-sample-size

max-sample-size <packet-size>
no max-sample-size

Sets the maximum size of sampled packets by sFlow.
The no form of the command resets the parameter to its default value.

Syntax Description	packet-size	The sampled packet size. The range is 64-256 bytes.
Default	128 bytes	
Configuration Mode	Config sFlow	
History	3.3.3500	
Role	admin	
Example	`switch (config sflow) # max-sample-size 165` `switch (config sflow) #`	
Related Commands		
Note	Sampled payload beyond the configured size is discarded.	

counter-poll-interval

counter-poll-interval <seconds>
no counter-poll-interval

Sets the sFlow statistics polling interval.
The no form of the command resets the parameter to its default value.

Syntax Description	seconds	The sFlow statistics polling interval in seconds. Range is 5-3600 seconds. Zero disables the statistic polling.
Default	20 seconds	
Configuration Mode	Config sFlow	
History	3.3.3500	
Role	admin	
Example	`switch (config sflow) # counter-poll-interval 30` `switch (config sflow) #`	
Related Commands		
Note		

max-datagram-size

max-datagram-size <packet-size>
no max-datagram-size

Sets the maximum sFlow packet size to be sent to the collector.
The no form of the command resets the parameter to its default value.

Syntax Description	packet-size	The packet size of the packet being sent to the collector. The range is 200-9216 bytes.
Default	1400 bytes	
Configuration Mode	Config sFlow	
History	3.3.3500	
Role	admin	
Example	`switch (config sflow) # max-datagram-size 9216` `switch (config sflow) #`	
Related Commands		
Note	This packet contains the data sample as well as the statistical counter data.	

collector-ip

collector-ip <ip-address> [udp-port <udp-port-number>]
no collector-ip [<ip-address> udp-port]

Sets the collector's IP.
The no form of the command resets the parameters to their default values.

Syntax Description	ip-address	The collector IP address.
	udp-port <udp-port-number>	Sets the collector UDP port number.
Default	ip-address: 0.0.0.0 udf-port-number: 6343	
Configuration Mode	Config sFlow	
History	3.3.3500	
Role	admin	
Example	`switch (config sflow) # collector-ip 10.10.10.10` `switch (config sflow) #`	
Related Commands		
Note		

agent-ip

agent-ip {<ip-address> | interface [ethernet <slot/port> | port-channel <channel-group>] | <if-name> | loopback <number> | vlan <id>}
no agent-ip

Sets the IP address associated with this agent.
The no form of the command resets the parameters to their default values.

Syntax Description	interface	Configures a specific ethernet/port-channel interface's agent IP.
	if-name	Interface name (e.g. mgmt0, mgmt1).
	ip-address	The sFlow agent's IP address (i.e. the source IP of the packet).
	loopback <number>	Loopback interface number. Range: 1-32.
	vlan <id>	Interface VLAN. Range: 1-4094.
Default	ip-address: 0.0.0.0	
Configuration Mode	Config sFlow	
History	3.3.3500	
	3.3.5200	Updated "interface" parameters
Role	admin	
Example	`switch (config sflow) # agent-ip 20.20.20.20` `switch (config sflow) #`	
Related Commands		
Note	The IP address here is used in the sFlow header.	

clear counters

clear counters

Clears sFlow counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config sFlow
History	3.3.3500
Role	admin
Example	`switch (config sflow) # clear counters` `switch (config sflow) #`
Related Commands	
Note	

sflow enable (interface)

sflow enable
no sflow enable

Enables sFlow on this interface.
The no form of the command disables sFlow on the interface.

Syntax Description	N/A
Default	disable no view-port-channel member
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel
History	3.3.3500 3.3.4500 Added MLAG port-channel configuration mode
Role	admin

Example	`switch(config interface ethernet 1/1)# sflow enable`
	`...`
	`switch(config interface port-channel 1)# sflow enable`

Related Commands	
Note	

5.13.7.3 Show

show sflow

show sflow

Displays sFlow configuration and counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.3500
Role	admin

Example	`switch (config)# show sflow`
	`sflow protocol enabled`
	`sflow enabled`
	`sampling-rate 16000`
	`max-sampled-size 156`
	`counter-poll-interval 19`
	`max-datagram-size 1500`
	`collector-ip 10.10.10.10`
	`collector-port 6343`
	`agent-ip 20.20.20.20`
	`Interfaces`
	`Ethernet: eth1/1`
	`Port-channel: po1`
	`Statistics:`
	`Total Packets: 2000`
	`Number of flow samples: 1200`
	`Number of samples discarded: 0`
	`Number of statistic samples: 800`
	`Number of datagrams: 300`

Related Commands	
Note	

5.14 Transport Applications

5.14.1 RDMA over Converged Ethernet (RoCE)

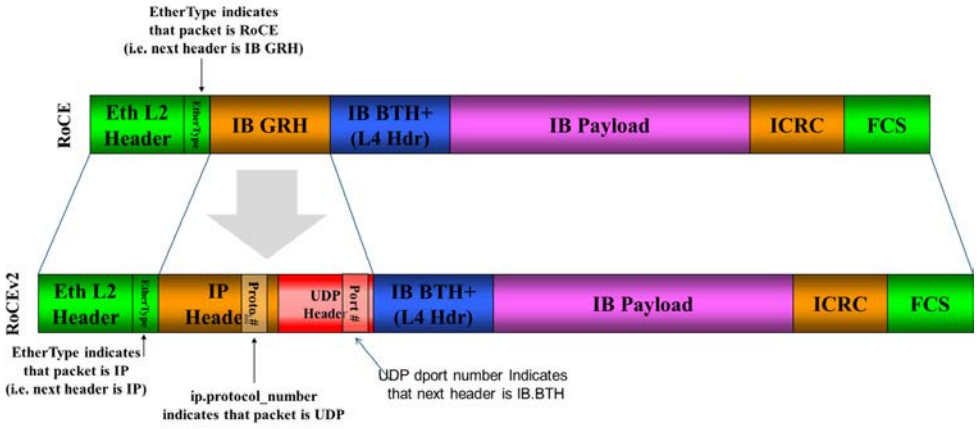
5.14.1.1 RoCE Overview

Remote Direct Memory Access (RDMA) is the remote memory management capability that allows server to server data movement directly between application memory without any CPU involvement. RDMA over Converged Ethernet (RoCE) is a mechanism to provide this efficient data transfer with very low latencies on loss-less Ethernet networks. With advances in data center convergence over reliable Ethernet, ConnectX® EN with RoCE uses the proven and efficient RDMA transport to provide the platform for deploying RDMA technology in mainstream data center application at 10GigE and 40GigE link-speed. ConnectX® EN with its hardware offload support takes advantage of this efficient RDMA transport (InfiniBand) services over Ethernet to deliver ultra-low latency for performance-critical and transaction intensive applications such as financial, database, storage, and content delivery networks. RoCE encapsulates IB transport and GRH headers in Ethernet packets bearing a dedicated ether type. While the use of GRH is optional within InfiniBand subnets, it is mandatory when using RoCE. Applications written over IB verbs should work seamlessly, but they require provisioning of GRH information when creating address vectors. The library and driver are modified to provide mapping from GID to MAC addresses required by the hardware.

5.14.1.1.1IP Routable (RoCEv2)

A straightforward extension of the RoCE protocol enables traffic to operate in layer 3 environments. This capability is obtained via a simple modification of the RoCE packet format. Instead of the GRH used in RoCE, routable RoCE packets carry an IP header which allows traversal of IP L3 Routers and a UDP header that serves as a stateless encapsulation layer for the RDMA Transport Protocol Packets over IP.

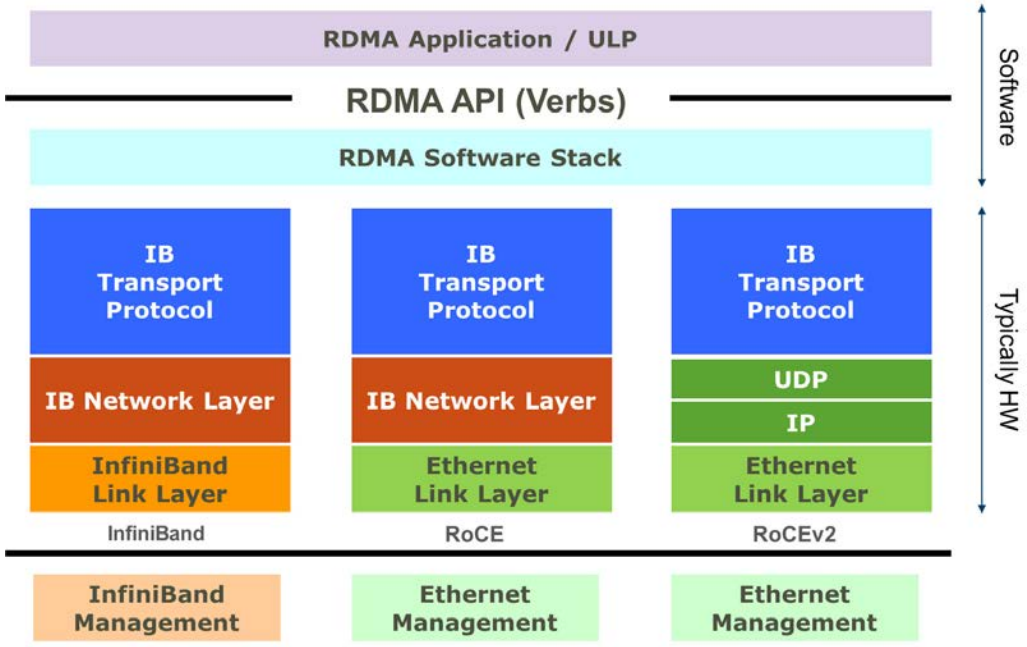
Figure 20: RoCEv2 and RoCE Frame Format Differences



The proposed RoCEv2 packets use a well-known UDP destination port value that unequivocally distinguishes the datagram. Similar to other protocols that use UDP encapsulation, the UDP source port field is used to carry an opaque flow-identifier that allows network devices to implement packet forwarding optimizations (e.g. ECMP) while staying agnostic to the specifics of the protocol header format.

Furthermore, since this change exclusively affects the packet format on the wire, and due to the fact that with RDMA semantics packets are generated and consumed below the AP applications can seamlessly operate over any form of RDMA service (including the routable version of RoCE as shown in Figure 2), in a completely transparent way[1].

Figure 21: RoCEv2 Protocol Stack



5.14.1.2 RoCE Configuration

In order to function reliably, RoCE requires a form of flow control. While it is possible to use global flow control, this is normally undesirable, for performance reasons.

The normal and optimal way to use RoCE is to use Priority Flow Control (PFC). To use PFC, it must be enabled on all endpoints and switches in the flow path.

In the following section we present instructions to configure PFC on Mellanox ConnectX™ cards. There are multiple configuration steps required, all of which may be performed via PowerShell. Therefore, although we present each step individually, you may ultimately choose to write a PowerShell script to do them all in one step. Note that administrator privileges are required for these steps.

For further information, please refer to the following URL:

http://blogs.technet.com/b/josebda/archive/2012/07/31/deploying-windows-server-2012-with-smb-direct-smb-over-rdma-and-the-mellanox-connectx-3-using-10gbe-40gbe-roce-step-by-step.aspx

5.14.1.2.1Prerequisites

The following are the driver's prerequisites in order to set or configure RoCE:

- ConnectX®-3 and ConnectX®-3 Pro firmware version 2.30.3000 or higher

1. Standard RDMA APIs are IP based already for all existing RDMA technologies

- All InfiniBand verbs applications which run over InfiniBand verbs should work on RoCE links if they use GRH headers.
- Set HCA to use Ethernet protocol:
  Display the Device Manager and expand “System Devices”.

5.14.1.2.2Configuring Windows Host

Since PFC is responsible for flow controlling at the granularity of traffic priority, it is necessary to assign different priorities to different types of network traffic.

As per RoCE configuration, all ND/NDK traffic is assigned to one or more chosen priorities, where PFC is enabled on those priorities.

Configuring Windows host requires configuring QoS.

5.14.1.2.2.1 Using Global Pause Flow Control (GFC)

➢ ***To use Global Pause Flow Control (GFC) mode, disable QoS and Priority:***

```
PS $ Disable-NetQosFlowControl
PS $ Disable-NetAdapterQos
```

5.14.1.3 Configuring SwitchX® Based Switch System

➢ ***To enable RoCE, the SwitchX should be configured as follows:***

- Ports facing the host should be configured as access ports, and either use global pause or Port Control Protocol (PCP) for priority flow control
- Ports facing the network should be configured as trunk ports, and use Port Control Protocol (PCP) for priority flow control

For further information on how to configure SwitchX, please refer to SwitchX User Manual.

5.14.1.4 Configuring Arista Switch

Step 1. Set the ports that face the hosts as trunk.

```
(config)# interface et10
(config-if-Et10)# switchport mode trunk
```

Step 2. Set VID allowed on trunk port to match the host VID.

```
(config-if-Et10)# switchport trunk allowed vlan 100
```

Step 3. Set the ports that face the network as trunk.

```
(config)# interface et20
(config-if-Et20)# switchport mode trunk
```

Step 4. Assign the relevant ports to LAG.

```
(config)# interface et10
(config-if-Et10)# dcbx mode ieee
(config-if-Et10)# speed forced 40gfull
(config-if-Et10)# channel-group 11 mode active
```

Step 5. Enable PFC on ports that face the network.

```
(config)# interface et20
(config-if-Et20)# load-interval 5
(config-if-Et20)# speed forced 40gfull
```

```
(config-if-Et20)# switchport trunk native vlan tag
(config-if-Et20)# switchport trunk allowed vlan 11
(config-if-Et20)# switchport mode trunk
(config-if-Et20)# dcbx mode ieee
(config-if-Et20)# priority-flow-control mode on
(config-if-Et20)# priority-flow-control priority 3 no-drop
```

5.14.1.4.1Using Global Pause Flow Control (GFC)

- ***To enable GFC on ports that face the hosts, perform the following:***

```
(config)# interface et10
(config-if-Et10)# flowcontrol receive on
(config-if-Et10)# flowcontrol send on
```

5.14.1.4.2Using Priority Flow Control (PFC)

- ***To enable PFC on ports that face the hosts, perform the following:***

```
(config)# interface et10
(config-if-Et10)# dcbx mode ieee
(config-if-Et10)# priority-flow-control mode on
(config-if-Et10)# priority-flow-control priority 3 no-drop
```

5.14.1.5 Configuring Router (PFC only)

The router uses L3's DSCP value to mark the egress traffic of L2 PCP. The required mapping, maps the three most significant bits of the DSCP into the PCP. This is the default behavior, and no additional configuration is required.

5.14.1.5.1Copying Port Control Protocol (PCP) between Subnets

The captured PCP option from the Ethernet header of the incoming packet can be used to set the PCP bits on the outgoing Ethernet header.

5.14.1.6 Configuring the RoCE Mode

Configuring the RoCE mode requires the following:

- RoCE mode is configured per-driver and is enforced on all the devices in the system

The supported RoCE modes depend on the firmware installed. If the firmware does not support the needed mode, the fallback mode would be the maximum supported RoCE mode of the installed NIC.

RoCE mode can be enabled and disabled via PowerShell.

- ***To enable RoCE using the PowerShell:***

- Open the PowerShell and run:

```
Set-MlnxDriverCoreSetting –RoceMode 1
```

- ***To enable RoCEv2 using the PowerShell:***

- Open the PowerShell and run:

```
Set-MlnxDriverCoreSetting –RoceMode 2
```

- ***To disable any version of RoCE using the PowerShell:***

  Open the PowerShell and run:

```
Set-MlnxDriverCoreSetting –RoceMode 0
```

- ***To check current version of RoCE using the PowerShell:***

Step 1. Open the PowerShell and run:

```
Get-MlnxDriverCoreSetting
```

Step 2. Example output:

```
Caption               : DriverCoreSettingData 'mlx4_bus'
Description           : Mellanox Driver Option Settings
.
.
.
RoceMode              : 0
```

6 IP Routing

6.1 General

6.1.1 IP Interfaces

MLNX-OS supports 3 types of IP interfaces.

- VLAN interface
- Loopback interface
- Router ports

VLAN interface is a logical IPv4 interface created per subnet over a specific 802.1Q VLAN ID. If two hosts from two different subnets need to communicate (via the IP layer), the network administrator needs to configure two interface VLANs, one for each of the subnets. The user may configure up to 64 VLAN interfaces.

Each interface VLAN has the following attributes:

- Admin state
- Operational state
- MAC address
- IP address and mask
- MTU
- Description
- Set of counters

Loopback interface is a logical software entity where traffic transmitted to this interface is immediately received on the sending end.

Router port is a regular switch port configured to operate as an L3 interface. Router ports are assigned an IP address and all L3 commands become applicable to them.

Once configured, router ports no longer partake in the bridging activities of the switch and VLANs configured on them are separate from the pool allocated for the switch ports.

6.1.1.1 Commands

switchport

switchport [force]
no switchport [force]

Configures the Ethernet interface as a regular switchport.
The no form of the command configures the Ethernet interface as a router port.

Syntax Description	force	Forces configuration even if the interface's admin state is enabled.
Default	N/A	
Configuration Mode	Config	
History	3.3.5200	
Role	admin	
Example	`switch (config interface ethernet 1/10)# no switchport force`	
Related Commands		
Note		

encapsulation dot1q vlan

encapsulation dot1q vlan <vlan-id> [force]
no encapsulation dot1q vlan [force]

Enables L2 802.1Q encapsulation of traffic on a specified router port in a VLAN. The no form of the command disables L2 802.1Q encapsulation of traffic on a specified router port in a VLAN.

Syntax Description	vlan-id	Enables L2 802.1Q encapsulation of traffic on a router port in a VLAN.
	force	Forces admin state down.
Default	N/A	
Configuration Mode	Config Interface Ethernet	
History	3.3.5200	
Role	admin	
Example	`switch (config interface ethernet 1/10)# encapsulation dot1q vlan 10`	
Related Commands		
Note		

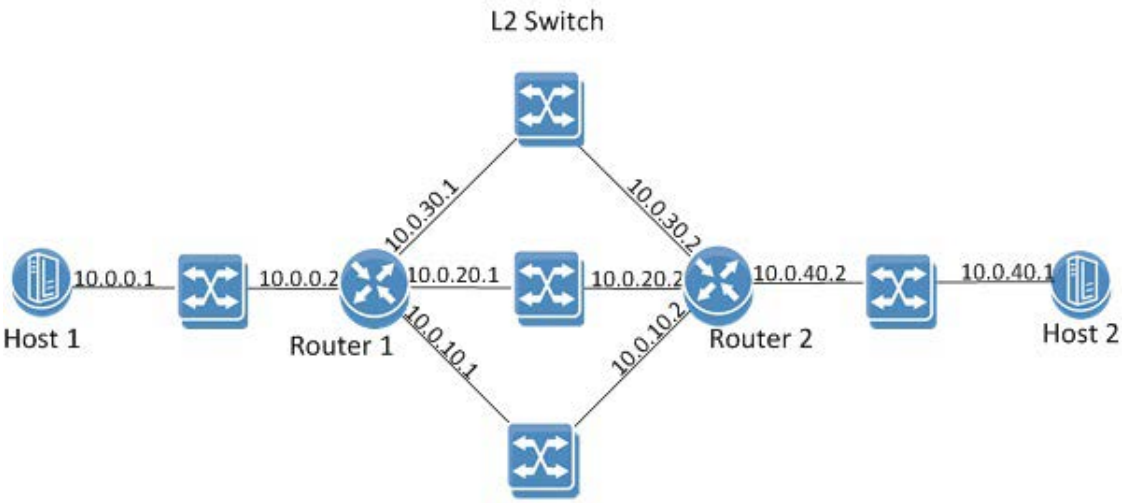
6.1.2 Equal Cost Multi-Path Routing (ECMP)

Equal-cost multi-path routing (ECMP) is a routing strategy where next-hop packet forwarding to a single destination can occur over multiple paths.

In Figure 22, routers R1 and R2 can both access each of their router peer networks. Router R1 routing table for 10.0.40/24 will contain the following routes:

- 10.0.10.2
- 10.0.20.2
- 10.0.30.2

Figure 22: ECMP



The load balancing function of the ECMP is configured globally on the system.

Hash algorithm can be symmetric or asymmetric. In symmetric hash functions bidirectional flows between routes will follow the same path, while in asymmetric hash functions, bidirectional traffic can follow different paths in both directions.

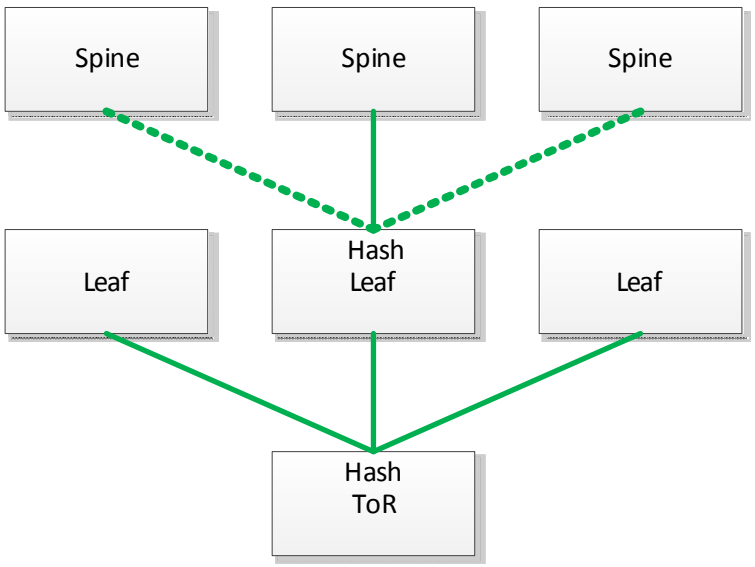
The following load balancing types are supported:

- Source IP & Port – source IP (SIP) and source UDP/TCP port: If the packet is not UDP/TCP, only SIP is used for the hash calculation. This is an asymmetric hash function.
- Destination IP & Port – destination IP (DIP) and destination UDP/TCP port: If the packet is not UDP/TCP, only DIP is used for the hash calculation. This is an asymmetric hash function.
- Source and Destination IP & Port – destination and source IP, as well as destination and source UDP/TCP port: If the packet is not UDP/TCP, only SIP/DIP are used for the hash calculation. This is a symmetric hash function.
- Traffic Class: Load balance based on the traffic class assigned to the packet. This is an asymmetric hash function.
- All (default): all above fields are part of the hash calculations. This is a symmetric hash function.

6.1.2.1 Hash Functions

It is advised that LAG and ECMP hash function configuration over more than one hop is different. If the same hash function is used over two hops, all the traffic sorted from one hop to following one will arrive already having the same characteristics, which will render the next hash function useless. For example, configure load-balancing on the first hop based on source IP while on the next hop based on destination IP.

Figure 23: Multiple Hush Functions



6.1.3 IPv4 Routing Mode

The resources available for IPv4 routing are as follows:

- number of IPv4 neighbors – 2048
- number of IPv4 unicast routes – 4096
- number of IPv4 multicast routes – 672

Prior to upgrading to this software release the user must align the number of configured multicast routes to number defined above.

6.1.4 Creating an IP Interface

Preconditions:

- An L3 license must be installed on your system (UPGR-xxxx-GW)
- A VLAN must be created using the command `vlan <vlan-id>`
- There must be at least one interface attached to this VLAN (to do so, run the `switchport` command in the interface configuration mode)
- There must be at least one interface in the operational state “UP”

➢ ***To create an IP interface:***

Step 1. Create a VLAN interface using the command `interface vlan <vlan-id>`.

Step 2. Apply an IP address and a network mask to the interface using the `ip address` command.

```
switch (config)# vlan 10
switch (config vlan 10)# exit
switch (config)# interface ethernet 1/1
switch (config interface ethernet 1/1)#switchport mode access
switch (config interface ethernet 1/1)#exit
switch (config)# show interface etherent status  // making sure there is a
                                                    port in UP state
Port                  Operational state          Speed                 Nego-
tiation
----                   -----------------          -----                  ----
-------
Eth1/1                 Up                         40 Gbps                No-
Negotiation
…
switch (config)#interface vlan 10
switch (config interface vlan)#ip address 10.10.10.10 /24
switch (config interface vlan)#show interface vlan 10

Vlan 10
 Admin state: Enabled
 Operational state: UP
 Mac Address: 00:02:c9:5d:e0:f0
  Internet Address: 10.10.10.10/24
  Broadcast address: 10.10.10.255
  MTU: 1500 bytes
  Description: my-ip-interface
  Counters: disabled
switch (config interface vlan)#
```

6.1.5 Commands

6.1.5.1 General

ip routing

ip routing
no ip routing

Enables L3 capabilities: IP router interfaces, static routing and routing protocols.
The no form of the command disables L3 capabilities, however does not delete the L3 configuration.

Syntax Description	N/A
Default	IP routing is disabled
Configuration Mode	Config
History	3.2.0230
Role	admin
Example	`switch (config) # ip routing` `switch (config) #`
Related Commands	interface vlan show ip routing
Note	• This command requires L3 license (i.e.LIC-1036-L3) • Disabling the command does not remove the feature configuration

show ip routing

show ip routing

Displays IP routing admin state.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0230
Role	admin

Example	`switch (config) # show ip routing`
	`IP routing: enabled`
	`switch (config) #`

Related Commands	ip routing
Note	

6.1.5.2 Interface VLAN

interface vlan

interface vlan <vlan-id>
no interface vlan <vlan-id>

Creates a VLAN interface and enters the interface VLAN configuration mode. The no form of the command deletes the VLAN interface.

Syntax Description	vlan-id	A numeric range of 1-4094
Default	N/A	
Configuration Mode	Config	
History	3.2.0230	
Role	admin	

Example	`switch (config) # interface vlan 10`
	`switch (config interface vlan 10) # show interfaces vlan 10`
	
	`Vlan 10`
	`  Admin state: Enabled`
	`  Operational state: Down (no up member port)`
	`  Mac Address: 00:02:c9:5d:e0:f0`
	`  Internet Address: 0.0.0.0/0`
	`  Broadcast address: 255.255.255.255`
	`  MTU: 1522 bytes`
	`  Description: N/A`
	`switch (config interface vlan 10) #`	

Related Commands	ip routing vlan <vlan-id> switchport mode switchport access show interfaces vlan	
Note	• Make sure the VLAN was created, using the command “vlan <vlan-id>” in the global configuration mode • The VLAN must be assigned to one of the L2 interfaces. To do so, run the command “swichport ...” • At least one interface belong to that VLAN must be in UP state	

ip address

ip address <ip-address> <mask>
no ip address <ip-address> <mask>

Enters user-defined description for the interface.

Syntax Description	ip-address	IPv4 address
	mask	There are two possible ways to the mask: • /length (i.e. /24) • Network address (i.e. 255.255.255.0)
Default	0.0.0.0/0	
Configuration Mode	Config Interface VLAN	
History	3.2.0230	
Role	admin	

Example	`switch (config interface vlan 10) # ip address 10.10.10.10 /24`
	`switch (config interface vlan 10) # show interfaces vlan 10`
	
	`Vlan 10`
	`  Admin state: Enabled`
	`  Operational state: Down (no up member port)`
	`  Mac Address: 00:02:c9:5d:e0:f0`
	`  Internet Address: 10.10.10.10/24`
	`  Broadcast address: 10.10.10.255`
	`  MTU: 1522 bytes`
	`  Description: my-ip-interface`
	`switch (config) #`	

Related Commands	interface vlan	
Note		

counters

counters
no counters

Enables counters gathering on the IP interface.
The no form of the command disables counters gathering on the IP interface.

Syntax Description	N/A
Default	counters are disabled.
Configuration Mode	Config Interface VLAN
History	3.2.0230
Role	admin

Example	`switch (config) # interface vlan 10`
	`switch (config interface vlan 10) # counters`
	`switch (config interface vlan 10) # show interfaces vlan 10`
	
	`Vlan 10`
	`  Admin state: Enabled`
	`  Operational state: Down (no up member port)`
	`  Mac Address: 00:02:c9:5d:e0:f0`
	`  Internet Address: 0.0.0.0/0`
	`  Broadcast address: 255.255.255.255`
	`  MTU: 1522 bytes`
	`  Description: N/A`
	
	`RX`
	`  0  Unicast frames`
	`  0  Multicast frames`
	`  0  Unicast octets`
	`  0  Multicast octets`
	`  0  Error frames`
	`  0  Error octets`
	`TX`
	`  0  Unicast frames`
	`  0  Multicast frames`
	`  0  Unicast octets`
	`  0  Multicast octets`
	
	`switch (config) #`

Related Commands	interface vlan
Note	• Enabling counters for the router interface adds delay to the traffic stream • There are maximum of 16 counter sets

description

description <string>
no description

Enters a description for the interface.
The no form of the command sets the description to default.

Syntax Description	string	User defined string
Default	“”	
Configuration Mode	Config Interface VLAN	
History	3.2.0230	
Role	admin	

Example	`switch (config interface vlan 10) #description my-ip-interface`
	`switch (config interface vlan 10) #show interfaces vlan 10`
	
	`Vlan 10`
	`  Admin state: Enabled`
	`  Operational state: Down (no up member port)`
	`  Mac Address: 00:02:c9:5d:e0:f0`
	`  Internet Address: 0.0.0.0/0`
	`  Broadcast address: 255.255.255.255`
	`  MTU: 1522 bytes`
	`  Description: my-ip-interface`
	
	`switch (config) #`	

Related Commands	interface vlan	
Note		

mtu

mtu <size> [force]
no mtu

Sets the MTU for the interface.
The no form of the command sets the MTU to default.

Syntax Description	size	1518-9216.
	force	Forces command implementation.
Default	1522	
Configuration Mode	Config Interface VLAN	
History	3.2.0230	
Role	admin	

Example	`switch (config interface vlan 10)# mtu 9216`
	`switch (config interface vlan 10 # show interfaces vlan 10`
	
	`Vlan 10`
	`  Admin state: Enabled`
	`  Operational state: Down (no up member port)`
	`  Mac Address: 00:02:c9:5d:e0:f0`
	`  Internet Address: 10.10.10.10/24`
	`  Broadcast address: 10.10.10.255`
	`  MTU: 9216 bytes`
	`  Description: my-ip-interface`
	`switch (config interface vlan 10)#`	

Related Commands	interface vlan	
Note		

shutdown

	shutdown **no shutdown** Disables the interface. The no form of the command enables the interface.
Syntax Description	N/A
Default	The interface is enabled.
Configuration Mode	Config Interface VLAN
History	3.1.0000
Role	admin

Example	`switch (config interface vlan 20) # shutdown`
	`switch (config interface vlan 20) # show interfaces vlan 20`
	
	`Vlan 20`
	`  Admin state: Disabled`
	`  Operational state: Down (admin down)`
	`  Mac Address: 00:02:c9:5d:e0:f0`
	`  Internet Address: 0.0.0.0/0`
	`  Broadcast address: 255.255.255.255`
	`  MTU: 1522 bytes`
	`  Description: N/A`
	`switch (config interface vlan 20) #`

Related Commands	interface vlan
Note	

clear counters

clear counters

Clears the interface counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config Interface VLAN
History	3.2.0230
Role	admin
Example	`switch (config interface vlan 10) # clear counters` `switch (config interface vlan 10) #`
Related Commands	interface vlan counters
Note	

show interfaces vlan

show interfaces vlan [<vlan-ID> | status]

Displays the interface VLAN configuration and status per VLAN or as a summarized list.

Syntax Description	vlan-id	A numeric range of 1-4094
	status	Displays a summarized status table.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.2.0230	
	3.3.4000	Added ARP timeout to the output example.
Role	admin	

Example

```
switch (config) # show interfaces vlan status

Interface         Description       State
---------         -----------       ------
Vlan1             N/A               Up
Vlan10            my-ip-interface   Down
Vlan11            N/A               Up
Vlan12            N/A               Up
Vlan13            N/A               Up
Vlan14            N/A               Up
Vlan20            N/A               Down
switch (config) # show interfaces vlan 10

Vlan 10
  Admin state: Enabled
  Operational state: Down (no up member port)
  Mac Address: 00:02:c9:5d:e0:f0
  MTU: 1522 bytes
  Arp timeout: 240 seconds
  Description: N/A

RX
  0                   Unicast frames
  0                   Multicast frames
  0                   Unicast octets
  0                   Multicast octets
  0                   Error frames
  0                   Error octets
TX
  0                   Unicast frames
  0                   Multicast frames
  0                   Unicast octets
  0                   Multicast octets

switch (config) #
```

Related Commands	interface vlan
Note	Byte counters count octets starting from the IP header field, it doesn't count the L2 header (MAC, VLAN) and FCS length.

6.1.5.3 Loopback Interface

interface loopback

interface loopback <id>
no interface loopback <id>

Creates a loopback interface and enters the interface configuration mode.
The no form of the command deletes the interface.

Syntax Description	id	A numeric range of 1-32
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # interface loopback 10` `switch (config interface loopback 10) #`	
Related Commands		
Note	• Up to 32 loopback interfaces can be configured. • Within the loopback configuration mode, you can configure description and ip-address. • MTU cannot be configured on the loopback interface.	

ip address

ip address <ip-address> <mask>
no ip address <ip-address> <mask>

Enters user-defined description for the interface.

Syntax Description	ip-address	IPv4 address.
	mask	There are two possible ways to the mask: • /length – only /32 is possible • Network address (i.e. 255.255.255.0)
Default	0.0.0.0/0	
Configuration Mode	Config Interface Loopback	
History	3.3.5006	
Role	admin	
Example	`switch (config interface loopback 10) # ip address 10.10.10.10 /32`	
Related Commands	interface loopback	
Note		

description

description <string>
no description

Enters a description for the interface.
The no form of the command sets the description to default.

Syntax Description	string	User defined string.
Default	“”	
Configuration Mode	Config Interface Loopback	
History	3.3.5006	
Role	admin	
Example	`switch (config interface loopback 10) #description my-ip-interface`	
Related Commands	interface loopback	
Note		

show interfaces loopback

show interface loopback <id>

Shows the attribute of the interface loopback.

Syntax Description	id	A numeric range of 1-32
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	

Example	`switch (config) # show interfaces loopback 2`
	
	`Loopback 2`
	`  Internet Address: 2.2.2.2/32`
	`  Broadcast address: 2.2.2.2`
	`  MTU: 1500 bytes`
	`  Description: my-loopback`
	`switch (config) #`	

Related Commands		
Note	•	

6.1.5.4 Routing and ECMP

ip route

ip route <IP prefix> <netmask> <next hop IP address>
no ip route <IP prefix> <netmask> <next hop IP address>

Sets a static route.
The no form of the command deletes the static route

Syntax Description	IP address	IPv4 address
	netmask	There are two possible ways to the mask: • /length (i.e. /24) • Network address (i.e. 255.255.255.0)
	next hop IP address	IPv4 address of the next hop.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ip route 10.10.10.0 /24 172.28.2.4`
	`switch (config) # show ip route`
	`Destination Mask Gateway Interface Source`
	`default 0.0.0.0 172.28.0.1 mgmt0 DHCP`
	`10.10.10.0 255.255.255.0 172.28.2.4 mgmt0 static`
	`172.28.0.0 255.255.0.0 0.0.0.0 mgmt0 direct`
	`1.0.0.0 255.255.255.0 0.0.0.0 Vlan11 direct`
	`2.0.0.0 255.255.255.0 0.0.0.0 Vlan12 direct`
	`3.0.0.0 255.255.255.0 0.0.0.0 Vlan13 direct`
	`4.0.0.0 255.255.255.0 0.0.0.0 Vlan14 direct`
	`8.8.8.0 255.255.255.0 0.0.0.0 Vlan1 direct`
	`7.7.7.0 255.255.255.0 1.0.0.2 Vlan11 static`
	`2.0.0.2 Vlan12 static`
	`4.0.0.2 Vlan14 static`
	`3.0.0.2 Vlan13 static`
	`switch (config) #`	

Related Commands	interface vlan ip load sharing show ip route	
Note	The IP prefix and the network mask must be aligned in the LSB mask, (for example 192.168.0.0 /16 or 192.168.10.0 /24, or 192.168.10.10 /32)	

ip load-sharing

ip load-sharing <type>
no ip load-sharing

This command sets the ECMP load sharing mode.
The no form of the command sets the load-sharing to default.

Syntax Description	type	• source-ip-port • destination-ip-port • source-destination-ip-port • traffic-class • all
Default	all	
Configuration Mode	Config	
History	3.2.0230	
Role	admin	

Example	`switch (config) # ip load-sharing all`
	`switch (config) # show ip load-sharing`
	`Load sharing: all`
	`switch (config)`	

Related Commands	ip route	
Note		

show ip route

show ip route [static | summary | -a]

Displays the route table.

Syntax Description	static	Displays routing table
	summary	Displays routing table summary
	-a	Displays static routes currently inactive due to the interface being down
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	First version
	3.3.3500	Added Distance/Metric column
	3.4.0000	Added -a parameter
Role	admin	
Example		

```
switch (config) # show ip route
Destination   Mask            Gateway         Interface   Source   Distance/Metric
default       0.0.0.0         10.224.13.254   mgmt0       DHCP     0/0
10.224.13.0   255.255.255.0   0.0.0.0         mgmt0       direct   0/0
11.11.11.0    255.255.255.0   0.0.0.0         vlan11      direct   0/0
23.23.23.0    255.255.255.0   0.0.0.0         vlan23      direct   0/0
172.21.23.0   255.255.255.0   0.0.0.0         vlan23      ospf     110/2
switch (config) #
```

Related Commands	ip route
Note	ECMP routes are displayed in an aggregated manner.

show ip load-sharing

show ip load-sharing

Displays ECMP hash attribute.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0230
Role	admin

Example	`switch (config) # show ip load-sharing`
	`Load sharing: all`
	`switch (config) #`

Related Commands	ip load-sharing
Note	

6.1.5.5 Network to Media Resolution (ARP)

ip arp

ip arp <ip-address> <MAC-address>
no ip arp <ip-address>

Adds static ARP entry for the defined interface.
The no form of the command deletes the static ARP entry from the interface.

Syntax Description	IP address	IPv4 Address
	Mac-address	Mac address (format XX:XX:XX:XX:XX:XX)
Default	No static ARP entries	
Configuration Mode	Config Interface VLAN	
History	3.2.0230	
Role	admin	

Example	`switch (config interface vlan 11) # ip arp 1.0.0.3  00:11:22:33:44:55`
	`switch (config interface vlan 11) # show ip arp`
	
	`ARP Timeout: 2000`
	
	`Total number of entries: 55`
	`IP Address  MAC Address  Interface`
	`1.0.0.2  00:02:c9:5c:30:40  Vlan11`
	`1.0.0.3  00:11:22:33:44:55  Vlan11`
	`2.0.0.2  00:02:c9:5c:30:40  Vlan12`
	`3.0.0.2  00:02:c9:5c:30:40  Vlan13`
	`4.0.0.2  00:02:c9:5c:30:40  Vlan14`
	`switch (config interface vlan 11) #`	

Related Commands	show ip arp	
Note		

ip arp timeout

ip arp timeout <timeout-value>
no ip arp timeout

Sets the dynamic ARP cache timeout.
The no form of the command sets the timeout to default.

Syntax Description	timeout-value	Time (in seconds) that an entry remains in the ARP cache. Valid values are from 240 to 28800.

Default	1500 seconds
Configuration Mode	Config Interface VLAN
History	3.2.0230
Role	admin

Example	`switch (config) # ip arp timeout 2000`
	`switch (config) # show ip arp`
	
	`ARP Timeout: 2000`
	
	`Total number of entries: 55`
	`IP Address  MAC Address  Interface`
	`1.0.0.2  00:02:c9:5c:30:40  Vlan11`
	`1.0.0.3  00:11:22:33:44:55  Vlan11`
	`2.0.0.2  00:02:c9:5c:30:40  Vlan12`
	`3.0.0.2  00:02:c9:5c:30:40  Vlan13`
	`4.0.0.2  00:02:c9:5c:30:40  Vlan14`
	`switch (config) #`

Related Commands	ip arp show ip arp
Note	This value is used as the ARP timeout whenever a new IP interface is created.

clear ip arp

clear ip arp {[interface <type>] | [<IP-address>]}

Clears dynamic arp entries from the ARP table with possible filters.

Syntax Description	vlan-id	Clears dynamic ARP entries for a interface.
	IP address	Clears dynamic ARP entries for a specific IP address.
Default	N/A	
Configuration Mode	Config	
History	3.2.0230	
Role	admin	
Example	`switch (config) # clear ip arp` `switch (config) #`	
Related Commands	ip arp show ip arp	
Note		

show ip arp

show ip arp [interface <type>| <ip-address> | count]

Displays ARP table.

Syntax Description	interface type	Filters the table according to a specific interface (i.e. interface vlan, mgmt0)
	ip-address	Filters the table to the specific ip-address
	count	Shows ARP statistics
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.3000	
Role	admin	
Example		

```
switch-626a54 [standalone: master] (config) # show ip arp

Total number of entries: 3

  Address             Type           Hardware Address         Interface
  ------------------------------------------------------------------------
---
  10.209.0.1           Dynamic ETH     00:00:5E:00:01:01         mgmt0
  10.209.1.120         Dynamic ETH     00:02:C9:62:E8:C2         mgmt0
  10.209.1.121         Dynamic ETH     00:02:C9:62:E7:42         mgmt0
switch (config) # show ip arp count
ARP Table size: 3 (inband: 0, out of band: 3)
switch (config) #
```

Related Commands	
Note	

6.1.5.6 IP Diagnostic Tools

ping

ping [-LRUbdfnqrvVaA] [-c count] [-i interval] [-w deadline] [-p pattern] [-s packetsize] [-t ttl] [-I interface or address] [-M mtu discovery hint] [-S sndbuf] [-T timestamp option] [-Q tos] [hop1 ...] destination

Sends ICMP echo requests to a specified host.

Syntax Description	Linux Ping options
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # ping 172.30.2.2`
	`PING 172.30.2.2 (172.30.2.2) 56(84) bytes of data.`
	`64 bytes from 172.30.2.2: icmp_seq=1 ttl=64 time=0.703 ms`
	`64 bytes from 172.30.2.2: icmp_seq=2 ttl=64 time=0.187 ms`
	`64 bytes from 172.30.2.2: icmp_seq=3 ttl=64 time=0.166 ms`
	`64 bytes from 172.30.2.2: icmp_seq=4 ttl=64 time=0.161 ms`
	`64 bytes from 172.30.2.2: icmp_seq=5 ttl=64 time=0.153 ms`
	`64 bytes from 172.30.2.2: icmp_seq=6 ttl=64 time=0.144 ms`
	`^C`
	`--- 172.30.2.2 ping statistics ---`
	`6 packets transmitted, 6 received, 0% packet loss, time 5004ms`
	`rtt min/avg/max/mdev = 0.144/0.252/0.703/0.202 ms`
	`switch (config) #`

Related Commands	traceroute
Note	• Ping to IPv6 address is not supported. • When using -I option use the interface name + interface number, for example “ping -I vlan10”

traceroute

traceroute [-46dFITUnrAV] [-f first_ttl] [-g gate,...] [-i device] [-m max_ttl] [-N squeries] [-p port] [-t tos] [-l flow_label] [-w waittime] [-q nqueries] [-s src_addr] [-z sendwait] host [packetlen]

Traces the route packets take to a destination.

Syntax Description

`-4`	Uses IPv4.
`-6`	Uses IPv6
`-d`	Enables socket level debugging.
`-F`	Sets DF (“do not fragment” bit) on.
`-I`	Uses ICMP ECHO for tracerouting.
`-T`	Uses TCP SYN for tracerouting.
`-U`	Uses UDP datagram (default) for tracerouting.
`-n`	Does not resolve IP addresses to their domain names.
`-r`	Bypasses the normal routing and send directly to a host on an attached network.
`-A`	Performs AS path lookups in routing registries and print results directly after the corresponding addresses.
`-V`	Prints version info and exit.
`-f`	Starts from the first_ttl hop (instead from 1).
`-g`	Routes packets throw the specified gateway (maximum 8 for IPv4 and 127 for IPv6).
`-i`	Specifies a network interface to operate with.
`-m`	Sets the max number of hops (max TTL to be reached). Default is 30.
`-N`	Sets the number of probes to be tried simultaneously (default is 16).
`-p`	Uses destination port. It is an initial value for the UDP destination port (incremented by each probe, default is 33434), for the ICMP seq number (incremented as well, default from 1), and the constant destination port for TCP tries (default is 80).
`-t`	Sets the TOS (IPv4 type of service) or TC (IPv6 traffic class) value for outgoing packets.
`-l`	Uses specified flow_label for IPv6 packets.

`-w`	Sets the number of seconds to wait for response to a probe (default is 5.0). Non-integer (float point) values allowed too.
`-q`	Sets the number of probes per each hop. Default is 3.
`-s`	Uses source src_addr for outgoing packets.
`-z`	Sets minimal time interval between probes (default is 0). If the value is more than 10, then it specifies a number in milliseconds, else it is a number of seconds (float point values allowed too).

Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # traceroute 192.168.10.70`
	`traceroute to 192.168.10.70 (192.168.10.70), 30 hops max, 40 byte packets`
	`1 172.30.0.1 (172.30.0.1) 3.632 ms 2.849 ms 3.544 ms`
	`2 10.222.128.46 (10.222.128.46) 3.176 ms 3.289 ms 3.656 ms`
	`3 10.158.128.30 (10.158.128.30) 15.331 ms 15.819 ms 16.388 ms`
	`4 10.158.128.65 (10.158.128.65) 20.468 ms 7.893 ms 12.27 ms`
	`5 10.7.34.115 (10.7.34.115) 16.405 ms 11.985 ms 12.264 ms`
	`6 192.168.10.70 (192.168.10.70) 16.377 ms 16.091 ms 20.475 ms`
	`switch (config) #`

Related Commands	
Note	• Traceroute fot IPv6 is not supported • The following flags are not supported: -6, -l, -A • When using -i option use the interface name + interface number, for example “traceroute -i vlan10”

tcpdump

tcpdump [-aAdeflLnNOpqRStuUvxX] [-c count] [-C file_size]
[-E algo:secret] [-F file] [-i interface] [-M secret]
[-r file] [-s snaplen] [-T type] [-w file]
[-W filecount] [-y datalinktype] [-Z user]
[expression]

Invokes standard binary, passing command line parameters straight through. Runs in foreground, printing packets as they arrive, until the user hits Ctrl+C.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin

Example	`switch (config) # tcpdump`
	`......`
	`09:37:38.678812 IP 192.168.10.7.ssh > 192.168.10.1.54155: P`
	`1494624:1494800(176) ack 625 win 90`
	`<nop,nop,timestamp 5842763 858672398>`
	`09:37:38.678860 IP 192.168.10.7.ssh > 192.168.10.1.54155: P`
	`1494800:1495104(304) ack 625 win 90`
	`<nop,nop,timestamp 5842763 858672398>`
	`...`
	`9141 packets captured`
	`9142 packets received by filter`
	`0 packets dropped by kernel`
	`switch (config) #`

Related Commands	N/A
Note	• When using -i option use the interface name + interface number, for example “tcpdump -i vlan10” • For all flag options of this command refer to the linux ‘man page’ of tcp dump.

6.1.5.7 QoS

qos map dscp-to-pcp preserve-pcp

qos map dscp-to-pcp preserve-pcp
no qos map dscp-to-pcp preserve-pcp

Configures the router to copy PCP bits when transferring data from one subnet to another.
The no form of the command disables this ability.

Syntax Description	N/A
Default	Disabled.
Configuration Mode	Config
History	3.3.4000
Role	admin
Example	`switch (config) # qos map dscp-to-pcp preserve-pcp` `switch (config) #`
Related Commands	
Note	• This commands applies the configuration for all router interfaces • As part of its function, the router performs DSCP to PCP bits mapping (fixed mapping). By activating the command the router preserves the PCP bits from one subnet to another subnet (PCP bits are copied).

6.2 OSPF

Open Shortest Path First (OSPF) is a link-state routing protocol for IP networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).

OSPF-speaking routers send Hello packets to all OSPF-enabled IP interfaces. If two routers sharing a common data link agree on certain parameters specified in their respective Hello packets, they become neighbors.

Adjacencies, which can be thought of as virtual point-to-point links, are formed between some neighbors. OSPF defines several network types and several router types. The establishment of an adjacency is determined by the types of routers exchanging Hellos and the type of network over which the Hello packets are exchanged.

Each router sends link-state advertisements (LSAs) over all adjacencies. The LSAs describe all of the router’s links, or interfaces, the router's neighbors, and the state of the links. These links might be to stub networks (those without another router attached), to other OSPF routers, to networks in other areas, or to external networks (those learned from another routing process). Because of the varying types of link-state information, OSPF defines multiple LSA types.

Each router receiving an LSA from a neighbor records the LSA in its link-state database and sends a copy of the LSA to all of its other neighbors. By flooding LSAs throughout an area, all routers will build identical link-state databases.

When the databases are complete, each router uses the SPF algorithm to calculate a loop-free graph describing the shortest (lowest cost) path to every known destination, with itself as the root.

When all link-state information has been flooded to all routers in an area, and neighbors have verified that their databases are identical, it means the link-state databases have been synchronized and the route tables have been built. Hello packets are exchanged between neighbors as keepalives, and LSAs are retransmitted. If the network topology is stable, no other activity should occur.

For OSPF network design over Mellanox L2 VMS, please refer to Mellanox Virtual Modular Switch Reference Guide.

6.2.1 Router ID

The router ID is a 32-bit number assigned to the router running the OSPF protocol. This number uniquely identifies the router within an Autonomous System.

Router ID can be configured statically, however, if it is not configured, then the default election is as follows:

- If a loopback interface already exists, the router ID takes the loopback IP address;
- Otherwise, the lowest IP address is elected as router ID

6.2.2 ECMP

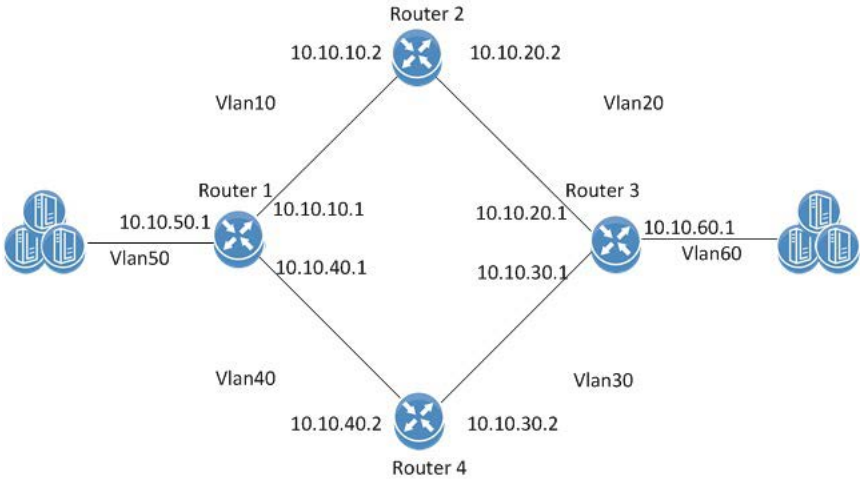
Equal-cost multi-path (ECMP) routing is a routing strategy where next-hop packet forwarding to a single destination can occur over multiple paths. The OSPF link-state routing algorithm can find multiple routes to the same destination, all multiple routes are added to the routing table only if those routes are equal-cost routes.

In case there are several routes with different cost, only the route with the lowest cost is selected. In case there are multiple routes with the same lowest cost, all of them are used (up to maximum of 64 ECMP routes).

ECMP is not configurable but is enabled by default for OSPF.

6.2.3 Configuring OSPF

Figure 24: OSPF Basic Topology



Precondition steps:

The following configuration example refers to Router 2 in Figure 24. The remainder of the routers in the figure are configured similarly.

It is recommended to disable STP before enabling OSPF. Use the command `no spanning-tree`.

Step 1. Make sure an L3 license is installed. For a list of the available licenses see Section 2.4, “Licenses,” on page 20.

Step 2. Enable IP routing functionality. Run:.

```
switch (config)# ip routing
```

Step 3. Enable the desired VLAN. Run:.

```
switch (config)# vlan 10
switch (config)# vlan 20
```

Step 4. Add this VLAN to the desired interface. Run:

```
switch (config)# interface ethernet 1/1
switch (config ethernet 1/1)# switchport access vlan 10
switch (config ethernet 1/1)# exit
switch (config)# interface ethernet 1/2
switch (config ethernet 1/2)# switchport access vlan 20
```

Step 5. Create a VLAN interface. Run:

```
switch (config)# interface vlan 10
```

Step 6. Apply IP address to the VLAN interface. Run:

```
switch (config interface vlan 10)# ip address 10.10.10.2 /16
```

Step 7. Enable the interface. Run:

```
switch (config interface vlan 10)# no shutdown
```

Step 8. Create a second VLAN interface. Run:

```
switch (config)# interface vlan 20
```

Step 9. Apply IP address to the second VLAN interface. Run:

```
switch (config interface vlan 20)# ip address 10.10.20.2 /16
```

Step 10. Enable the second interface. Run:

```
switch (config interface vlan 20)# no shutdown
```

Basic OSPF Configuration:

Step 1. To enable OSPF configuration run:

```
switch (config)# protocol ospf
```

Step 2. To create a router OSPF instance run:

```
switch (config)# router ospf
```

Only one instance of OSPF is supported.

Step 3. Associate the VLAN interfaces to the OSPF area. Area 0 is the backbone area, run:

```
switch (config interface vlan 10)# ip ospf area 0
switch (config interface vlan 10)# exit
switch (config)# interface vlan 20
switch (config interface vlan 20)# ip ospf area 0
```

6.2.4 Verifying OSPF

- ***To verify OSPF configuration and status:***

Step 1. Verify OSPF configuration and status. Run:

```
switch (config) # show ip ospf

Routing Process 1 with ID 10.10.10.10 vrf-default

Stateful High Availability disabled
Graceful-restart is not supported
Supports only single TOS (TOS 0) route
Opaque LSA not supported
OSPF Admin State is enabled
```

```
Redistributing External Routes: Disabled
Administrative distance 110
Reference Bandwidth is 40Gb
Initial SPF schedule delay 1 msecs
SPF Hold time 10 msecs
Maximum paths to destination 64
Router is not originating router LSA with maximum metric
Condition: Always
Number of external LSAs  0, checksum sum  0
Number of opaque AS LSAs 0,checksum sum 0
Number of areas is 1, 1 normal, 0 stub, 0 nssa
Number of active areas is 1, 1 normal, 0 stub, 0 nssa

Area (0.0.0.0) (Active)
Interfaces in this area: 2 Active Interfaces: 2
Passive Interfaces: 0
SPF Calculation has run 5 times
This area is Normal area
Number of LSAs: 1, checksum sum 7700

switch (config) #
```

Step 2. Verify the OSPF neighbors status. Make sure that each neighbor reaches FULL state with its peer to enable it take part in all dynamic routing changes in the network. Run:

```
switch (config) # show ip ospf neighbors

Neighbor 10.10.10.1, interface address 10.10.10.2
In the area 0.0.0.0 via interface Vlan 10
Neighbor priority is 1, State is FULL
BDR is 10.10.10.1
Options 0
Dead timer due in 35

Neighbor 10.10.20.1, interface address 10.10.20.2
In the area 0.0.0.0 via interface Vlan 20
Neighbor priority is 1, State is FULL
BDR is 10.10.20.1
Options 0
Dead timer due in 35

switch (config) #
```

Step 3. Verify the OSPF Interface configuration and status run:

```
switch (config) # show ip ospf interface

Interface Vlan is 10 Enabled, line protocol is Down
IP address 10.10.10.2, Mask 255.255.0.0
Process ID 1 VRF Default, Area 0.0.0.0
OSPF Interface Admin State is enabled
State DOWN, Network Type BROADCAST, Cost 1
Transmit delay 1 sec, Router Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals (sec's): Hello 10, Dead 40, Wait 40, Retransmit 5
No authentication
Number of opaque link LSAs: 0, checksum sum 0

Interface Vlan is 20 Enabled, line protocol is Up
IP address 10.10.20.2, Mask 255.255.0.0
Process ID 1 VRF Default, Area 0.0.0.0
OSPF Interface Admin State is enabled
State DESIGNATED ROUTER, Network Type BROADCAST, Cost 1
Transmit delay 1 sec, Router Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals (sec's): Hello 10, Dead 40, Wait 40, Retransmit 5
No authentication
Number of opaque link LSAs: 0, checksum sum 0

switch (config) #
```

6.2.5 Commands

6.2.5.1 Config

protocol ospf

protocol ospf
no protocol ospf

Enables Open Shortest Path First Protocol (OSPF), and unhides the related OSPF commands.
The no form of the command deletes the OSPF configuration and hides the OSPF related commands.

Syntax Description	N/A
Default	OSPF feature is disabled.
Configuration Mode	Config
History	3.3.3500
Role	admin
Example	`switch (config)# protocol ospf`
Related Commands	ip routing
Note	

router ospf

router ospf
no router ospf

Enters router OSPF configuration mode, and creates default OSPF instance if not exist.
The no form of the command deletes the OSPF instance.

Syntax Description	N/A
Default	No router OSPF is created.
Configuration Mode	Config
History	3.3.3500
Role	admin
Example	`switch (config)# router ospf` `switch (config router ospf)#`
Related Commands	N/A
Note	Only one OSPF instance is supported.

6.2.5.2 Config Router

router-id

router-id <ip-address>
no router-id

Sets Router ID for the OSPF instance.
The no form of the command causes automatic election of router ID by the router.

Syntax Description	ip-address	The Router id in IP address format.
Default	The router ID is a 32-bit number assigned to the router running the OSPF protocol. This number uniquely identifies the router within an Autonomous System. Router ID can be configured statically, however, if it is not configured, then the default election is as follows: • If a loopback interface already exists, the router ID takes the loopback IP address; • Otherwise, the lowest IP address is elected as router ID.	
Configuration Mode	Config OSPF Router	
History	3.3.3500	
Role	admin	
Example	`switch (config router ospf)# router-id 10.10.10.10`	
Related Commands	N/A	
Note		

shutdown

shutdown
no shutdown

Disables the OSPF instance.
The no form of the command enables the OSPF instance.

Syntax Description	N/A
Default	Enable (no shutdown)
Configuration Mode	Config OSPF Router
History	3.3.3500
Role	admin
Example	`switch (config router ospf)# shutdown`
Related Commands	N/A
Note	

distance

distance <value>
no distance

Configures the OSPF route administrative distance.
The no form of the command resets this parameter to default.

Syntax Description	value	OSPF administrative distance. Range is 1-255.
Default	110	
Configuration Mode	Config OSPF Router	
History	3.3.3500	
Role	admin	
Example	`switch (config router ospf)# distance 100`	
Related Commands	N/A	
Note		

redistribute

redistribute {direct | static}
no redistribute {direct | static}

Import routes from other routing protocols as well as any statically configured routers into OSPF.
The no form of the command disables the importing of the routes.

Syntax Description	direct	Redistribute directly connected routes.
	static	Redistribute static configured routes.
Default	Disable (no redistribution)	
Configuration Mode	Config OSPF Router	
History	3.2.1000	
Role	admin	
Example	`switch (config router ospf)# redistribute direct`	
Related Commands	N/A	
Note	Routes from multiple protocols can be imported in parallel.	

timers throttle spf

timers throttle spf <spf-delay> <spf-hold>
no timers throttle spf

Sets the OSPF throttle SPF timers.
The no form of the command resets the timers to default.

Syntax Description	spf-delay	The interval by which SPF calculations delayed after a topology change reception. Range is 0-100 milliseconds.
	spf-hold	The minimum delay between two consecutive delay calculations. Range is 0-1000 milliseconds.
Default	spf-delay: 1 millisecond spf-hold: 10 millisecond	
Configuration Mode	Config OSPF Router	
History	3.3.3500	
Role	admin	
Example	`switch (config router ospf)# timers throttle spf 100 1000`	
Related Commands	N/A	
Note		

area default-cost

area <area-id> default-cost <cost>
no area <area-id> default-cost

Specifies cost for the default summary route sent into an OSPF stub or not-so-stubby area (NSSA).
The no form of the command sets the cost to the default value.

Syntax Description	area-id	OSPF area-id. Range is 0-4294967295.
	cost	The cost for the default summary route. Range is 1-16777215.
Default	The summary route cost is based on the area border router that generated the summary route.	
Configuration Mode	Config OSPF Router	
History	3.3.3500	
Role	admin	
Example	`switch (config router ospf)# area 0 default-cost 100`	
Related Commands	N/A	
Note	Base cost for all calculation is 56GbE.	

area range

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

Consolidates and summarizes routes at an OSPF area boundary.
The no form of the command removes the ip-prefix range from summarization.

Syntax Description	area-id	OSPF area-ID. Range is 0-4294967295.
	ip-address	IP Address.
	not-advertise	Suppresses routes that match the specified IP address.
	prefix	Netowrk prefix (in the format of /24, or 255.255.255.0 for example).
Default	Disabled	
Configuration Mode	Config OSPF Router	
History	3.3.3500	
Role	admin	
Example	`switch (config router ospf)# area 0 range 10.10.10.10 /24`	
Related Commands	N/A	
Note		

area stub

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

Configures an area as an OSPF stub area (an area is created if non-existent).
The no form of the command removes the stub area configuration and changes the area to normal, or deletes the area (if stub is not used).

Syntax Description	area-id	OSPF area-ID. Range is 0-4294967295.
	no-summary	Summary route will not be advertized into the stub area.
Default	Summary route will be advertized.	
Configuration Mode	Config OSPF Router	
History	3.3.3500	
Role	admin	
Example	`switch (config router ospf)# area 0 stub`	
Related Commands	N/A	
Note		

area nssa

area <area-id> nssa [default-information-originate [metric <m-value>] [metric-type <m-type>]] [nosummary] [translate type7 always]
no area <area-id> nssa [default-information-originate] [no-summary] [translate type7 always]

Configures an area as an OSPF not-so-stubby (NSSA) area.
The no form of the command removes the NSSA area configuration and changes the area to default.

Syntax Description	area-id	OSPF area ID. Range is 0-4294967295.
	default-information-originate	A default type7 LSA (Link State Advertisements) is generated into the NSSA area.
	m-type	Metric type for OSPF. Range is 1-2.
	m-value	Metric value for OSPF. Range is 1-65535.
	no-summary	Summary route will not be advertized into the NSSA area.
	translate type7 always	Type7 LSAs is translated to type5 LSAs (Link State Advertisements).
Default	Default m-type:2 Default m-value:10	
Configuration Mode	Config OSPF Router	
History	3.3.3500	
Role	admin	
Example	`switch (config router ospf)# area 0 nssa`	
Related Commands	N/A	
Note	An area can be either stub, NSSA or normal.	

summary-address

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

Creates aggregate addresses for the OSPF protocol.
The no form of the command disables the aggregation of the ip-address.

Syntax Description	ip-address	The summary IP address.
	not-advertise	Suppresses routes that match the specified ip-address.
	prefix	Network prefix (in the format of /24 or 255.255.255.0, for example).
Default	N/A	
Configuration Mode	Config OSPF Router	
History	3.3.3500	
Role	admin	
Example	`switch (config router ospf)# summary-address 10.10.10.10 /24`	
Related Commands	N/A	
Note	Maximum of 1500 summarized IP addresses can be configured.	

6.2.5.3 Interface

ip ospf cost

ip ospf cost <cost>
no ip ospf cost <cost>

Sets OSPF cost of sending packet of this interface.
The no form of the command resets this parameter to default.

Syntax Description	cost	The Interface cost used by the OSPF. Range is 1-65535.
Default	1	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.3500	
Role	admin	
Example	`switch (config interface vlan 10)# ip ospf cost 100`	
Related Commands	N/A	
Note		

ip ospf dead-interval

ip ospf dead-interval <seconds>
no ip ospf dead-interval

Configures the interval during which at least one Hello packet must be received from a neighbor before the router declares that neighbor as down.
The no form of the command resets this parameter to its default.

Syntax Description	seconds	The dead-interval timer, in seconds. Range is 1-65535.
Default	40	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.3500	
Role	admin	
Example	`switch (config interface vlan 10)# ip ospf dean-interval 10`	
Related Commands	N/A	
Note	The value must be the same for all nodes on the network.	

ip ospf hello-interval

ip ospf hello-interval <seconds>
no ip ospf hello-interval

Configures the interval between Hello packets that OSPF sends on the interface. The no form of the command resets this parameter to default.

Syntax Description	seconds	The Hello interval timer, in seconds. Range is 1-65535.
Default	10	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.3500	
Role	admin	
Example	`switch (config interface vlan 10)# ip ospf hello-interval 20`	
Related Commands	N/A	
Note	The value must be the same for all nodes on the network.	

ip ospf priority

ip ospf priority <number>
no ip ospf priority

Configures the priority for this OSPF interface.
The no form of the command resets this parameter to default.

Syntax Description	number	The Interface priority used by the OSPF protocol. Range is 0-255
Default	1	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.3500	
Role	admin	
Example	`switch (config interface vlan 10)# ip ospf priority 100`	
Related Commands	N/A	
Note	• Use the “ip ospf priority” command to set the router priority, which determines the designated router for this network. When two routers are attached to a network, both attempt to become the designated router. • The router with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero cannot become the designated router or backup designated router.	

ip ospf network

ip ospf network <type>
no ip ospf network

Sets the OSPF interface network type.
The no form of the command resets the interface network type to its default.

Syntax Description	type	The network type on this interface. The options are 'broadcast' or 'point-to-point'.
Default	broadcast	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.3500	
Role	admin	
Example	`switch (config interface vlan 10)# ip ospf network point-to-point`	
Related Commands	N/A	
Note	• The network type influences the behavior of the OSPF interface. An OSPF network type is usually broadcast, which uses OSPF multicasting capabilities. Under this network type, a designated router and backup designated router are elected. For point-to-point networks, there are only two neighbors and multicast is not required. • All routers on the same network should have the same network type.	

ip ospf retransmit-interval

ip ospf retransmit-interval <seconds>
no ip ospf retransmit-interval

Configures the time between OSPF link-state advertisement (LSA) retransmissions for adjacencies that belongs to the interface.
The no form of the command resets this parameter to its default.

Syntax Description	seconds	The retransmit interval in seconds. Range is 0-3600.
Default	5	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.3500	
Role	admin	
Example	`switch (config interface vlan 10)# ip ospf retransmit-interval 10`	
Related Commands	N/A	
Note		

ip ospf passive-interface

ip ospf passive-interface
no ip ospf passive-interface

Suppresses flooding of OSPF routing updates on an interface.
The no form of the command reverts the status to active OSPF interface.

Syntax Description	N/A
Default	Active interface (no ip ospf passive-interface)
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port
History	3.3.3500
Role	admin
Example	`switch (config interface vlan 10)# ip ospf passive-interface`
Related Commands	N/A
Note	

ip ospf transmit-delay

ip ospf transmit-delay <seconds>
no ip ospf transmit-delay

Sets the estimated time required to send an OSPF link-state update packet.
The no form of the command resets this parameter to its default.

Syntax Description	seconds	The transmit-delay interval in seconds. Range is 0-3600.
Default	1	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.3500	
Role	admin	
Example	`switch (config interface vlan 10)# ip ospf transmit-delay 2`	
Related Commands	N/A	
Note		

ip ospf shutdown

	ip ospf shutdown **no ip ospf shutdown** Disables the OSPF instance on the interface. The no form of the command enables the OSPF on this interface.
Syntax Description	N/A
Default	Enabled (no shutdown)
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port
History	3.3.3500
Role	admin
Example	`switch (config interface vlan 10)# ip ospf shutdown`
Related Commands	N/A
Note	

ip ospf authentication

ip ospf authentication [message-digest]
no ip ospf authentication

Specifies the authentication type for OSPF.
The no form of the command disables the authentication.

Syntax Description	message-digest	Specifies that message-digest authentication (MD5) is used.
Default	Disabled (no)	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.3500	
Role	admin	
Example	`switch (config interface vlan 10)# ip ospf authentication`	
Related Commands	N/A	
Note	• Without message-digest option, a simple password authentication will be used. • Message-digest authentication can be enabled only if a key is configured.	

ip ospf authentication-key

ip ospf authentication-key [auth-type] <password>
no ip ospf authentication-key

To assign a password for simple password authentication for the OSPF.
The no form of the command deletes the simple password authentication key.

Syntax Description	auth-type	The authentication type: 0 - Unencrypted password 7 - MD5 key
	password	Authentication password, up to 8 alphanumeric string.
Default	Unencrypted password	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.3500	
Role	admin	
Example	`switch (config interface vlan 10)# ip ospf authentication-key 7 mypass-word`	
Related Commands	N/A	
Note	• Without message-digest option, a simple password authentication will be used. • Message-digest authentication can be enabled only if a key is configured.	

ip ospf message-digest-key

ip ospf message-digest-key <key-id> md5 [auth-type] <key>
no ip ospf message-digest-key <key-id>

Sets the message digest key for MD5 authentication.
The no form of the command deletes the key for MD5 authentication.

Syntax Description	auth-type	The authentication type: 0 - Unencrypted password 7 - MD5 key
	key	Authentication password, up to 8 alphanumeric string.
	key-id	Alphanumeric password of up to 16 bytes.
Default	Unencrypted (no)	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.3500	
Role	admin	
Example	`switch (config interface vlan 10)# ip ospf message-digest-key mykeyid md5 7 mykey`	
Related Commands	N/A	
Note	The user cannot delete the last key until authentication is disabled.	

ip ospf area

ip ospf area <area-id>
no ip ospf area

Sets OSPF area of this interface (and creates the area if non-existent).
The no form of the command removes the interface from the area.

Syntax Description	area-id	OSPF area ID. Range is 0-4294967295.
Default	N/A	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port Config Interface Loopback	
History	3.3.3500	
Role	admin	
Example	`switch (config interface vlan 10)# ip ospf area 0`	
Related Commands	N/A	
Note		

6.2.5.4 Show

show ip ospf

show ip ospf

Displays general OSPF configuration and status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.3500
Role	admin

Example	`switch (config)# show ip ospf`
	`Routing Process 201 with ID 192.0.2.1 VRF default`
	`Admin Status is Enabled`
	`Stateful High Availability enabled`
	`Graceful-restart is configured`

Related Commands	N/A
Note	

show ip ospf border-routers

show ip ospf border-routers

Displays routing table entries to an Area Border Routers.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.3500
Role	admin

Example	`switch# show ip ospf border-routers`
	`OSPF Process ID p1, vrf default Internal Routing Table`
	`Codes: i - Intra-area route, I - Inter-area route`
	`i 40.40.40.40 [10], ABR, Area 0.0.0.0, SPF 71 via`
	`192.0.2.1, Ethernet2/1`
	`i 60.60.60.60 [20], ABR, Area 0.0.0.0, SPF 71 via`
	`192.0.2.1, Ethernet2/1`
	`i 40.40.40.40 [10], ABR, Area 0.0.0.1, SPF 71 via`
	`192.0.2.1, Ethernet2/2`
	`i 60.60.60.60 [20], ABR, Area 0.0.0.1, SPF 71 via`
	`192.0.2.1, Ethernet2/2`

Related Commands	N/A
Note	

show ip ospf database

show ip ospf database [summary] [<area-id> [<link-state-id>]] [adv-router <ip-address> | self-originated]

Displays the OSPF database.

Syntax Description	adv-router <ip-address>	Filters per advertize router
	area-id	Filters the command per OSPF area-id. Range is 0-4294967295.
	link-state-id	The link state ID
	self-originated	Self Originate
	summary	Summarizes the output of the OSPF database.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.3500	
Role	admin	

Example	`Router# show ip ospf database`
	`OSPF Router with ID (50.50.50.50) (Process ID p1)`
	`Router Link States (Area 0)`
	`Link ID ADV Router Age Seq# Checksum Link Count`
	`40.40.40.40 40.40.40.40 930 0x80000004 0x2ea1 3`
	`50.50.50.50 50.50.50.50 935 0x80000002 0x8b52 1`
	`60.60.60.60 60.60.60.60 943 0x800003c5 0x9854 2`
	`Network Link States (Area 0)`
	`Link ID ADV Router Age Seq# Checksum`
	`209.165.201.3 60.60.60.60 944 0x80000001 0x7179`
	`192.0.2.1 50.50.50.50 935 0x80000001 0x516a`
	`Summary Network Link States (Area 0)`
	`Link ID ADV Router Age Seq# Checksum`
	`209.165.201.1 40.40.40.40 929 0x80000001 0x2498`
	`209.165.201.1 50.50.50.50 928 0x80000001 0x5b2f`
	`209.165.201.1 60.60.60.60 1265 0x800003c3 0xf49b`
	`192.0.2.0 40.40.40.40 943 0x80000001 0x53f3`
	`192.0.2.0 50.50.50.50 935 0x80000001 0x26f8`
	`192.0.2.0 60.60.60.60 930 0x80000001 0x7b51`	

Related Commands	N/A	
Note		

show ip ospf interface

show ip ospf interface [vlan <vlan-id>] [brief]

Displays the OSPF related interface configuration.

Syntax Description	brief	Gives a brief summary of the output.
	vlan <vlan-id>	Displays OSPF interface configuration and status per VLAN interface.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.3500	
Role	admin	

Example	`switch# show ip ospf interface ethernet 1/5`
	`Ethernet1/5 is up, line protocol is down`
	`IP address 192.0.2.1, Process ID 201 VRF RemoteOfficeVRF, area 0.0.0.10`
	`Enabled by interface configuration`
	`State DOWN, Network type BROADCAST, cost 4`
	`Index 1, Transmit delay 1 sec, Router Priority 1`
	`No designated router on this network`
	`No backup designated router on this network`
	`0 Neighbors, flooding to 0, adjacent with 0`
	`Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5`
	`No authentication`
	`Number of opaque link LSAs: 0, checksum sum 0`
	`switch#`
	
	`This example shows how to display OSPF information in a brief format:`
	`switch# show ip ospf interface brief`
	`OSPF Process ID 201 VRF default`
	`Total number of interface: 1`
	`Interface ID Area Cost State Neighbors Status`
	`VL1 2 0.0.0.0 65535 DOWN 0 down`
	`switch#`	

Related Commands	N/A	
Note		

show ip ospf neighbors

show ip ospf neighbors [vlan <vlan-id>] [<neighbor-id>]

Displays the OSPF related interface neighbor configuration.

Syntax Description	vlan <vlan-id>	Displays OSPF interface configuration and status per VLAN interface.
	neighbor-id	Filers the output per a specific OSPF neighbor.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.3500	
Role	admin	

Example

```
Router# show ip ospf neighbors 10.199.199.137
Neighbor 10.199.199.137, interface address 192.0.2.37
In the area 0.0.0.0 via interface Ethernet2/1
Neighbor priority is 1, State is FULL
Options 2
Dead timer due in 0:00:32
Link State retransmission due in 0:00:04
Neighbor 10.199.199.137, interface address 209.165.201.189
In the area 0.0.0.0 via interface Ethernet4/3
Neighbor priority is 5, State is FULL
Options 2
Dead timer due in 0:00:32
Link State retransmission due in 0:00:03

This example shows how to display the neighbors that match the neighbor
ID on an interface:
Router# show ip ospf neighbors ethernet 2/1 10.199.199.137
Neighbor 10.199.199.137, interface address 192.0.2.37
In the area 0.0.0.0 via interface Ethernet2/1
Neighbor priority is 1, State is FULL
Options 2
Dead timer due in 0:00:37
Link State retransmission due in 0:00:04
This example shows how to display detailed information about OSPF neigh-
bors:
Router# show ip ospf neighbors detail
Neighbor 192.168.5.2, interface address 10.225.200.28
In the area 0 via interface GigabitEthernet1/0/0
Neighbor priority is 1, State is FULL, 6 state changes
DR is 10.225.200.28 BDR is 10.225.200.30
Options is 0x42
LLS Options is 0x1 (LR), last OOB-Resync 00:03:08 ago
Dead timer due in 00:00:36
Neighbor is up for 00:09:46
Index 1/1, retransmission queue length 0, number of retransmission 1
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 1, maximum is 1
Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands	N/A
Note	

show ip ospf request-list

show ip ospf request-list <neighbor-id> vlan <vlan-id>

Displays the OSPF list of all link-state advertisements (LSAs) requested by a router.

Syntax Description	neighbor-id	Filers the output per a specific OSPF neighbor.
	vlan-id	Filers the output per a specific VLAN ID.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.3500	
Role	admin	

Example	`Router# show ip ospf request-list 40.40.40 ethernet 2/1`
	`OSPF Process ID p1`
	`Neighbor 40.40.40.40, interface Ethernet2/1, address 192.0.2.1`
	`1 LSAs on request-list`
	`Type LS ID ADV RTR Seq NO Age Checksum`
	`1 192.0.2.12 192.0.2.12 0x8000020D 8 0x6572`	

Related Commands	N/A	
Note		

show ip ospf retransmission-list

show ip ospf retransmission-list <neighbor-id> vlan <vlan-id>

Displays the OSPF list of all link-state advertisements (LSAs) waiting to be resent to neighbors.

Syntax Description	neighbor-id	Filers the output per a specific OSPF neighbor.
	vlan-id	Filers the output per a specific VLAN ID.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.3500	
Role	admin	

Example	`Router# show ip ospf retransmission-list 192.0.2.11 ethernet 2/1`
	`OSPF Router with ID (192.0.2.12) (Process ID 1)`
	`Neighbor 192.0.2.11, interface Ethernet2/1 address 209.165.201.11`
	`Link state retransmission due in 3764 msec, Queue length 2`
	`Type LS ID ADV RTR Seq NO Age Checksum`
	`1 192.0.2.12 192.0.2.12 0x80000210 0 0xB196`	

Related Commands	N/A	
Note		

show ip ospf summary-address

show ip ospf summary-address

Displays a list of all summary address redistribution information configured on the OSPF.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.3500
Role	admin

Example	`switch (config)# show ip ospf summary-address`
	`Display of Summary addresses for External Routes and area ranges for the summary LSAs`
	`OSPF Process default`
	`OSPF External Summary Address and area-range Configuration Information`
	`-----------------------------------------------------`
	`Network Mask Area Advertise LSA type Metric Tag`
	`-----------------------------------------------------------------`
	`1.1.1.1 255.255.255.0 NA Advertise Type5 10 0`
	`2.2.2.0 255.255.255.0 10.10.10.10 Not Advertise Type3 10 0`

Related Commands	N/A
Note	

6.3 BGP

Border Gateway Protocol (BGP) is an exterior gateway protocol which is designed to transfer routing information between routers. It maintains and propagates a table of routes which designates network reachability among autonomous systems (ASs).

BGP neighbors, or peers, are routers configured manually to converse using the BGP protocol on top of a TCP session on port 179. A BGP speaker periodically sends keep-alive messages to maintain the connection. Network reachability includes such information as forwarding destinations (IPv4 or IPv6) together with a list of ASs that this information traverses and other attributes, so it becomes possible to construct a graph of AS connectivity without routing loops. BGP makes possible to apply policy rules to enforce connectivity graph.

BGP routers communicate through TCP connection on port 179. Connection between BGP neighbors is configured manually or can be established dynamically by configuring dynamic listen groups. When BGP runs between two peers in the same AS, it is referred to as Internal BGP (iBGP, or Interior Border Gateway Protocol). When it runs between separate ASs, it is called External BGP (eBGP, or Exterior Border Gateway Protocol). Both sides can initiate a connection, after the initial connectivity is created, BGP state machine drives both sides to enter into ESTABLISHED state where they can exchange UPDATE messages with reachability information.

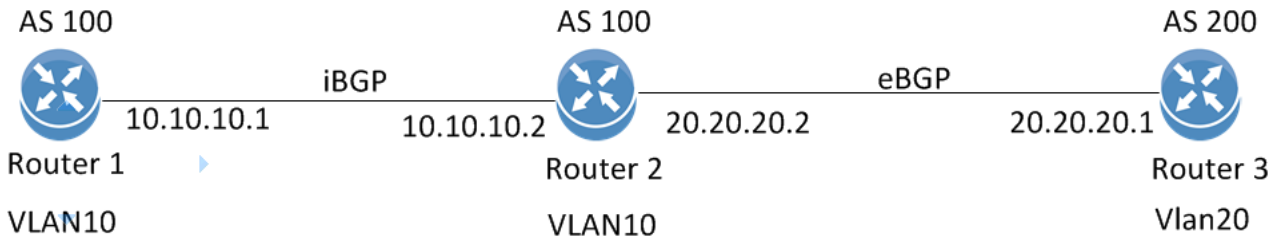
6.3.1 State Machine

In order to make decisions in its operations with peers, a BGP peer uses a simple finite state machine (FSM) that consists of six states: Idle; Connect; Active; OpenSent; OpenConfirm; and Established. For each peer-to-peer session, a BGP implementation maintains a state variable that tracks which of these six states the session is in. The BGP protocol defines the messages that each peer should exchange in order to change the session from one state to another.

The first state is the “Idle” state. In “Idle” state, BGP initializes all resources, refuses all inbound BGP connection attempts and initiates a TCP connection to the peer. The second state is “Connect”. In the “Connect” state, the router awaits the TCP connection to complete and transitions to the “OpenSent” state if successful. If unsuccessful, it initializes the ConnectRetry timer and transitions to the “Active” state upon expiration. In the “Active” state, the router resets the ConnectRetry timer to zero and returns to the “Connect” state. In the “OpenSent” state, the router sends an Open message and waits for one in return in order to transition to the “OpenConfirm” state. KeepAlive messages are exchanged and, upon successful receipt, the router is placed into the “Established” state. In the “Established” state, the router can send/receive: KeepAlive; Update; and Notification messages to/from its peer.

6.3.2 Configuring BGP

Figure 25: Basic BGP Configuration



Follow these steps for basic BGP configuration on two switches (Router 1 and Router 2):

Preconditions:

Step 1. Make sure the license installed supports L3.

Step 2. Enable IP routing functionality. Run:

```
switch (config)# ip routing
```

Step 3. Enable the desired VLAN. Run:

```
switch (config)# vlan 10
```

The same VLAN must be configured on both switches.

Step 4. Add this VLAN to the desired interface. Run:

```
switch (config)# interface ethernet 1/1
switch (config ethernet 1/1)# switchport access vlan 10
```

Step 5. Create a VLAN interface. Run:

```
switch (config)# interface vlan 10
```

Step 6. Apply IP address to the VLAN interface on Router 1. Run:

```
switch (config interface vlan 10)# ip address 10.10.10.1 /24
```

Step 7. Apply IP address to the VLAN interface on Router 2. Run:

```
switch (config interface vlan 10)# ip address 10.10.10.2 /24
```

Step 8. Enable the interface. Run:

```
switch (config interface vlan 10)# no shutdown
```

Configure BGP:

Step 1. Enable BGP. Run:

```
switch (config)# protocol bgp
```

Step 2. Configure an AS number that identifies the BGP router. Run:

```
switch (config)# router bgp 100
```

To run iBGP, the AS number of all remote neighbors should be similar to the local AS number of the configured router.

Step 3. Configure BGP Router 1 neighbor. Run:.

```
switch (config router bgp 100)# neighbor 10.10.10.2 remote-as 100
```

Step 4. Configure BGP Router 2 neighbor. Run:.

```
switch (config router bgp 100)# neighbor 10.10.10.1 remote-as 100
```

6.3.3 Verifying BGP

Step 1. Check the general status of BGP. Run:

```
switch (config)# show ip bgp summary
BGP router identifier 10.10.10.1, local AS number 100
BGP table version is 100, main routing table version 100
0 network entries using 0 bytes of memory
0 path entries using 0 bytes of memory
0 BGP AS-PATH entries using 0 bytes of memory
0 BGP community entries using 0 bytes of memory
0 BGP extended community entries using 0 bytes of memory
Neighbor        V         AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down     State/PfxRcd
10.10.10.2      0       100     100      76       3    0    0 00:0:10:19 ESTABLISHED
switch (config)#
BGP summary information for VRF default, address family IPv4
```

- Verify that the state of each BGP neighbor reached to ESTABLISHED state.
- In case the neighbor is disabled (shutdown). The state of the neighbor will be IDLE.
- BGP incoming and outgoing messages should be incremented.
- The AS number of each neighbor is the correct one.

Step 2. Check the status of the neighbors. Run:

```
switch (config)# show ip bgp neighbors
BGP neighbor is 10.10.10.2, remote AS 100, external link
   BGP version 0, remote router ID 0.0.0.0
   BGP State = ESTABLISHED
   Last read 0:00:00:00, last write 0:00:00:00, hold time is 180, keepalive
interval is 60 seconds
   Configured hold time is 180, keepalive interval is 60 seconds
   Minimum holdtime from neighbor is 0 seconds
switch (config)#
```

You should be able to see running BGP counters and ESTABLISHED state per active neighbor.

6.3.4 Commands

6.3.4.1 Config

protocol bgp

protocol bgp
no protocol bgp

Enables BGP feature, and unhides BGP related commands.
The no form of the command deletes all BGP configuration and hides BGP related commands.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.5006
Role	admin
Example	`switch (config)# protocol bgp` `switch (config)#`
Related Commands	ip routing
Note	

clear ip bgp

clear ip bgp [{<ip-address> | all} [soft] [in | out]]

Clears BGP learned routes from the BGP table and resets the connection to the neighbor.

Syntax Description	ip-address	A BGP peer IP address. Only the specified neighbor is reset.
	all	All BGP peers. All BGP neighbors are reset.
	soft	Clears BGP learned routes from the BGP table without resetting the connection to the neighbor.
	in	Inbound routes are reset.
	out	Outbound routes are reset.
Default	N/A	
Configuration Mode	Config	
History	3.3.5006	First release
	3.3.5200	Updated description
Role	admin	
Example	`switch (config)# clear ip bgp all` `switch (config)#`	
Related Commands	N/A	
Note	This command removes BGP IPv4 learned routes from the routing table, reads all routes from designated peers, and sends routes to those peers as required.	

router bgp

router bgp <as-number>
no router bgp <as-number>

Creates and enters a BGP instance with the specified AS number.
The no form of the command deletes all router BGP instance configuration.

Syntax Description	as-number	Autonomous system number: A unique number to be used to identify the AS. The AS is a number which identifies the BGP router to other routers and tags the routing information passed along. Range: 1-65535.
Default	N/A	
Configuration Mode	Config	
History	3.3.5006	First version
	3.3.5200	Updated syntax description
Role	admin	
Example	`switch (config)# router bgp 100` `switch (config router bgp 100)#`	
Related Commands	ip routing	
Note		

6.3.4.2 Config Router

shutdown

shutdown
no shutdown

Gracefully disables BGP protocol without removing existing configuration.
The no form of the command enables BGP.

Syntax Description	N/A
Default	Enabled
Configuration Mode	Config Router BGP
History	3.3.5006
Role	admin
Example	`switch (config router bgp 100)# no shutdown`
Related Commands	
Note	

aggregate-address

aggregate-address <prefix> [summary-only] [as-set] [attribute-map]
no aggregate-address <prefix> [summary-only] [as-set] [attribute-map]

Creates an aggregate route in the BGP database.
The no form of the command disables ECMP across AS paths.

Syntax Description	prefix	Destination to aggregate
	summary-only	Contributor routes are not advertised.
	as-set	Includes AS_PATH information from contributor routes as AS_SET attributes
	attribute-map	Assigns attribute values in set commands of the map's permit clauses. Deny clauses and match commands in permit clauses are ignored.
Default	Disabled	
Configuration Mode	Config Router BGP	
History	3.4.0000	
Role	admin	
Example	`switch-e07c04 [standalone: master] (config router bgp 4) # aggregate-address 3.5.3.7 /32`	
Related Commands		
Note	• Aggregate routes combine the characteristics of multiple routes into a single route that the switch advertises • Aggregation can reduce the amount of information that a BGP speaker is required to store and transmit when advertising routes to other BGP speakers • Aggregate routes are advertised only after they are redistributed	

bestpath as-path multipath-relax

bestpath as-path multipath-relax
no bestpath as-path multipath-relax

Enables ECMP across AS paths.
The no form of the command disables ECMP across AS paths.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config Router BGP
History	3.3.5006
	3.3.5200 Updated description and notes
Role	admin
Example	`switch (config router bgp 100)# bestpath as-path multipath-relax`
Related Commands	maximum-paths
Note	• With this option disabled, only routes with exactly the same AS path as the best route to a destination are considered for ECMP. • With this option enabled, all routes with similar length AS path as the best route are considered for ECMP.

bgp fast-external-fallover

bgp fast-external-fallover
no bgp fast-external-fallover

Terminates eBGP sessions of any directly adjacent peer without waiting for the hold-down timer to expire if the link used to reach the peer goes down.
The no form of the command waits for hold-down timer to expire before terminating eBGP sessions.

Syntax Description	N/A
Default	no bgp fast-external-fallover
Configuration Mode	Config Router BGP
History	3.4.0000
Role	admin
Example	`switch (config router bgp 100)# bgp fast-external-fallover`
Related Commands	maximum-paths
Note	Although this feature improves BGP conversion time, it may cause instability in your BGP table due to a flapping interface.

bgp listen limit

bgp listen limit <maximum>
no bgp listen limit

Limits the number of dynamic BGP peers allowed on the switch.
The no form of the command resets to the default value.

Syntax Description	maximum	The maximum number of dynamic BGP peers to be allowed on the switch. Range: 1-128.
Default	100	
Configuration Mode	Config Router BGP	
History	3.4.0000	
Role	admin	
Example	`switch (config router bgp 100)# bgp listen limit 101`	
Related Commands		
Note		

bgp listen range

bgp listen range <ip-prefix> <length> peer-group <peer-group-name> remote-as <as-number>
no bgp listen range <ip-prefix> <length>

Identifies a range of IP addresses from which the switch will accept incoming dynamic BGP peering requests.
After applying the no form of the command, the switch will no longer accept dynamic peering requests on the range.

Syntax Description	ip-prefix	IP address
	length	Mask length (e.g. /24 or 255.255.255.254)
	peer-group-name	Peer group name
	remote-as <as-number>	Remote peer's number.
Default	100	
Configuration Mode	Config Router BGP	
History	3.4.0000	
Role	admin	
Example	`switch (config router bgp 100)# bgp listen range 10.10.10.10 /24 peer-group my-group remote-as 13`	
Related Commands		
Note	• To create a static peer group, use the command `neighbor peer-group` • Neighbors in a dynamic peer group are configured as a group and cannot be configured individually.	

bgp redistribute-internal

bgp redistribute-internal
no bgp redistribute-internal

Enables iBGP redistribution into an interior gateway protocol (IGP).
The no form of the command disables iBGP redistribution into an interior gateway protocol (IGP).

Syntax Description	ip-prefix	IP address
	length	Mask length (e.g. /24 or 255.255.255.254)
	peer-group-name	Peer group name
	remote-as <as-number>	Remote peer's number.
Default	Disabled	
Configuration Mode	Config Router BGP	
History	3.4.0000	
Role	admin	
Example	`switch (config router bgp 100)# bgp redistribute-internal`	
Related Commands		
Note		

cluster-id

cluster-id <ip-address>
no cluster-id <ip-address>

Configures the cluster ID in a cluster with multiple route reflectors.
The no form of the command resets the cluster ID for route reflector.

Syntax Description	ip-address	The route reflector cluster ID • 0.0.0.1 to 255.255.255.255 Valid cluster ID number • 0.0.0.0 removes the cluster-ID from the switch (similar to "no cluster-id")
Default	Cluster ID is the same as Router ID	
Configuration Mode	Config Router BGP	
History	3.2.1000	First version
	3.4.0000	Updated syntax description
Role	admin	
Example	`switch (config router bgp 100)# cluster-id 10.10.10.10`	
Related Commands	N/A	
Note		

client-to-client reflection

client-to-client reflection
no client-to-client reflection

The switch will be configured as a route reflector.
The no form of the command stops the switch from being a route reflector

Syntax Description	N/A
Default	client-to-client reflection is enabled
Configuration Mode	Config Router BGP
History	3.2.1000
Role	admin
Example	`switch (config router bgp 100)# client-to-client reflection`
Related Commands	N/A
Note	

distance

distance <external> <internal> <local>
no distance

Sets the administrative distance of the routes learned through BGP.
The no form of the command resets the administrative distance its default.

Syntax Description	external	Administrative distance for external BGP routes. Range: 1-255.
	internal	Administrative distance for internal BGP routes. Range: 1-255.
	local	Administrative distance for local BGP routes. Range: 1-255.
Default	external: 200 internal: 200 local: 200	
Configuration Mode	Config Router BGP	
History	3.3.5006	
Role	admin	
Example	`switch (config router bgp 100)# distance 10 20 30`	
Related Commands	N/A	
Note	• Routers use administrative distances to decide on a route when two protocols provide routing information to the same destination. • Lower distance values correspond to higher reliability. • Routes are external when learned from an external autonomous system. • Routes are internal when learned from a peer in the local autonomous system. • Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks being redistributed from another process. • BGP routing tables do not include routes with a distance of 255.	

graceful-restart stalepath-time

graceful-restart stalepath-time <interval>
no graceful-restart stalepath-time

Configures the maximum time that stale routes from a restarting BGP neighbor are retained after a BGP session is reestablished with that peer.
The no form of the command resets to the default value.

Syntax Description	interval	Time in seconds. Range: 1-3600.
Default	300 seconds	
Configuration Mode	Config Router BGP	
History	3.4.0000	
Role	admin	
Example	`switch (config router bgp 100)# graceful-restart stalepath-time 350`	
Related Commands	N/A	
Note		

graceful-restart helper

graceful-restart helper
no graceful-restart helper

Enables BGP graceful restart helper mode on the switch for all BGP neighbors. The no form of the command disables BGP graceful restart helper mode on the switch for all BGP neighbors.

Syntax Description	N/A
Default	Graceful restart is enabled
Configuration Mode	Config Router BGP
History	3.4.0000
Role	admin
Example	`switch (config router bgp 100)# graceful-restart helper`
Related Commands	N/A
Note	• When graceful restart helper mode is enabled, the switch retains routes from neighbors capable of graceful restart while those neighbors are restarting BGP • Individual neighbor configuration takes precedence over the global configuration

maximum-paths

maximum-paths [ibgp] <maximum-path>

Configures the maximum number of parallel eBGP/iBGP routes that the switch installs in the routing table.

Syntax Description	ibgp	Sets the configuration on the internal BGP.
	maximum-path	The number of routes to install to the routing table.
Default	1	
Configuration Mode	Config Router BGP	
History	3.3.5006	
	3.3.5200	Updated description and notes
Role	admin	
Example	`switch (config router bgp 100)# maximum-paths ibgp 10` `switch (config router bgp 100)#`	
Related Commands	N/A	
Note	• This command provides an ECMP parameter that controls the number of equal-cost paths that the switch installs in the routing table for each destination. • The action is effective after BGP restart. • If the parameter “ibgp” is not used, the setting is applied on routes learned from peers from other ASs; if “ibgp” is used, the setting is applied to routes learned from peers of the same AS.	

neighbor advertisement-interval

neighbor {<ip-address> | <peer-group-name>} advertisement-interval <delay>
no neighbor {<ip-address> | <peer-group-name>} advertisement-interval

Sets the minimum route advertisement interval (MRAI) between the sending of BGP routing updates.
The no form of the command disables this function.

Syntax Description	ip-address	A BGP peer IP address
	peer-group-name	Peer group name
	delay	Time (in seconds) is specified by an integer. Range: 0-600.
Default	30 seconds	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 advertisement-interval 90`	
Related Commands		
Note		

neighbor allowas-in

neighbor {<ip-address> | <peer-group-name>} allowas-in [number]
no neighbor {<ip-address> | <peer-group-name>} allowas-in

Configures the switch to permit the advertisement of prefixes containing duplicate autonomous switch numbers (ASNs).
The no form of the command disables this function.

Syntax Description	ip-address	A BGP peer IP address
	peer-group-name	Peer group name
	number	Number of switch's (ASN) allowed in path. Range: 1-10.
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 allowas-in 2`	
Related Commands	ip routing router bgp <as-number>	
Note	Neighbors from the same AS as the router are considered as iBGP peers, and neighbors from other ASs are considered eBGP peers.	

neighbor description

neighbor {<ip-address> | <peer-group-name>} description <string>
no neighbor {<ip-address> | <peer-group-name>} description

Associates descriptive text with the specified peer or peer group.
The no form of the command removes the description from the peer.

Syntax Description	ip-address	IP address of the neighbor.
	peer-group-name	Peer group name
	string	Free string, up to 80 characters in length.
Default	No description	
Configuration Mode	Config Router BGP	
History	3.3.5006	First version
	3.3.5200	Updated example
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 description The next door neighbor`	
Related Commands	N/A	
Note	The peer description only appears in the show commands.	

neighbor ebgp-multihop

neighbor {<ip-address> | <peer-group-name>} ebgp-multihop [<ttl>]
no neighbor {<ip-address> | <peer-group-name>} ebgp-multihop

Enables BGP to connect to external peers that are not directly connected to the switch. The no form of the command applies the system disables connecting to external peers.

Syntax Description	ip-address	IP address of the BGP-speaking neighbor
	peer-group-name	Peer group name
	ttl	Time-to-live. Range: 1-255 hops.
Default	ttl: 1	
Configuration Mode	Config Router BGP	
History	3.3.5006	First version
	3.3.5200	Updated default
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 ebgp-multihop 5`	
Related Commands	ip routing neighbor <ip-address> remote-as <as-number>	
Note	The command does not establish the multi-hop if the only route to the peer is the default route (0.0.0.0).	

neighbor export-localpref

neighbor {<ip-address> | <peer-group-name>} export-localpref <value>
no neighbor {<ip-address> | <peer-group-name>} export-localpref

Configures the local preference value sent to the specified peer or peer group. The no form of the command resets the local preference to its default value.

Syntax Description	ip-address	IP address of the BGP-speaking neighbor
	peer-group-name	Peer group name
	value	Preference value. Range: 0-2147483647.
Default	100	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 export-localpref 100`	
Related Commands		
Note		

neighbor graceful-restart helper

neighbor {<ip-address> | <peer-group-name>} graceful-restart helper
no neighbor {<ip-address> | <peer-group-name>} graceful-restart helper

Enables BGP graceful restart helper mode for the specified BGP neighbor or peer group.
The no form of the command

Syntax Description	ip-address	IP address of the BGP-speaking neighbor
	peer-group-name	Peer group name
Default	Graceful restart is enabled	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor graceful-restart helper`	
Related Commands		
Note	• When graceful restart helper mode is enabled, the switch retains routes from neighbors capable of graceful restart while those neighbors are restarting BGP • Individual neighbor configuration takes precedence over the global configuration	

neighbor import-localpref

neighbor {<ip-address> | <peer-group-name>} import-localpref <value>
no neighbor {<ip-address> | <peer-group-name>} import-localpref

Configures the local preference value assigned to routes received from the specified peer or peer group.
The no form of the command resets the local preference to its default value.

Syntax Description	ip-address	IP address of the BGP-speaking neighbor
	peer-group-name	Peer group name
	value	Preference value. Range: 0-2147483647.
Default	100	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 import-localpref 100`	
Related Commands		
Note		

neighbor local-as

neighbor {<ip-address> | <peer-group-name>} local-as <as-id> [no-prepend | replace-as]
no neighbor {<ip-address> | <peer-group-name>} local-as
Enables the modification of the AS path attribute for routes received from an eBGP neighbor.
The no form of the command disables AS path modification for the specified peer or peer group.

Syntax Description	ip-address	IP address of the BGP-speaking neighbor
	peer-group-name	Peer group name
	no-prepend	local-as number is not prepended to the routes received from external neighbors
	replace-as	Prepends only the local autonomous system number (as configured with the IP address argument) to the AS path attribute.
Default	12000	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch-e07c04 [standalone: master] (config router bgp 4) # neighbor 100.100.100.100 local-as 123`	
Related Commands	ip routing neighbor <ip-address> remote-as <as-number>	
Note	• This function allows the switch to appear as a member of a different autonomous system (AS) to external peers. • To disable peering with the neighbor run the command `clear ip bgp`	

neighbor maximum-prefix

neighbor {<ip-address> | <peer-group-name>} maximum-prefix <maximum> [warning-only]
no neighbor {<ip-address> | <peer-group-name>} maximum-prefix
Configures the number of BGP routes the switch accepts from a specified neighbor and defines an action when the limit is exceeded.
The no form of the command removes the limitation

Syntax Description	ip-address	IP address of the BGP-speaking neighbor
	peer-group-name	Peer group name
	maximum	Number of BGP routes the switch accepts from a specified neighbor. Range: 1-2147483647.
	warning-only	Only generates a warning rather than disconnecting the neighbor
Default	12000	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 maximum-prefix 12000 warning-only`	
Related Commands	ip routing neighbor <ip-address> remote-as <as-number>	
Note		

neighbor next-hop-peer

neighbor {<ip-address> | <peer-group-name>} next-hop-peer
no neighbor {<ip-address> | <peer-group-name>} next-hop-peer

Configures the switch to list the peer address as the next hop in routes that it receives from the specified peer BGP-speaking neighbor or members of the specified peer group.
The no form of the command disables this function.

Syntax Description	ip-address	IP address of the neighbor.
	peer-group-name	Peer group name
Default	no next-hop-peer	
Configuration Mode	Config Router BGP	
History	3.3.5006	
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 next-hop-peer`	
Related Commands		
Note	This command overrides the next hop for all routes received from this neighbor or peer group	

neighbor next-hop-self

neighbor {<ip-address> | <peer-group-name>} next-hop-self
no neighbor {<ip-address> | <peer-group-name>} next-hop-self

Configures the IP address of the router as the next hop address in routes advertises to the specific neighbor.
The no form of the command resets this parameter to its default.

Syntax Description	ip-address	IP address of the neighbor.
	peer-group-name	Peer group name
Default	no next-hop-self	
Configuration Mode	Config Router BGP	
History	3.3.5006	
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 next-hop-self`	
Related Commands	neighbor <ip-address> remote-as <as-number>	
Note	• This function is used in networks where BGP neighbors do not directly access all other neighbors on the same subnet. • In the default state, the next hop is generated based on the IP address and the present next hop in the route information.	

neighbor password

neighbor {<ip-address> | <peer-group-name>} password [<encryption>] <string>
no neighbor {<ip-address> | <peer-group-name>} password

Enables authentication on a TCP connection with a BGP peer.
The no form of the command resets the value to its default.

Syntax Description	ip-address	IP address of the neighbor
	peer-group-name	Peer group name
	encryption	Possible values: • no parameter – clear text • 0 – clear text • 7 – obfuscated
	string	Up to 8 bytes in length
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 password 7 admin123`	
Related Commands		
Note	• Peers must use the same password to ensure communication. • neighbor <ip-address> password 7 <password>' can only accept data that was created using 'show config'. • 'show config' will never show the clear-test password, it will always be obfuscated (and thus displayed using the 'password 7' syntax).	

neighbor peer-group

1. neighbor {<ip-address>} peer-group <peer-group-name>
2. neighbor {<peer-group-name>} peer-group
3. no neighbor {<ip-address>} peer-group <peer-group-name>
4. no neighbor {<peer-group-name>} peer-group <peer-group-name>

1. Assigns BGP neighbors to an existing peer group.
2. Creates a peer-group
3. Unassigns BGP neighbors to an existing peer group.
4. Removes a specified neighbor from the peer group

Syntax Description	ip-address	IP address of the neighbor
	peer-group-name	Peer group name
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor groupA peer-group` `switch (config router bgp 100)# neighbor 1.2.3.4 peer-group groupA`	
Related Commands		
Note	• Once a peer group is created, the group name can be used as a parameter in neighbor configuration commands, and the configuration will be applied to all members of the group. • Settings applied to an individual neighbor in the peer group override group settings. • A neighbor can only belong to one peer group, so issuing this command for a neighbor that is already a member of another group removes it from that group. • When a neighbor is removed from a peer group, the neighbor retains the configuration inherited from the peer group.	

neighbor remote-as

neighbor {<ip-address>} remote-as <as-number>
no neighbor {<ip-address>} remote-as <as-number>

Configures a neighbor.
The no form of the command removes the neighbor, dropping the connection and all routes if already connected.

Syntax Description	ip-address	A BGP peer IP address
	peer-group-name	Peer group name
	as-number	The BGP peer as-number. Range: 1-65535.
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.3.5006	First version
	3.3.5200	Updated description and note
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 remote-as 200` `switch (config router bgp 100)#`	
Related Commands	ip routing router bgp <as-number>	
Note	Neighbors from the same AS as the router are considered as iBGP peers, and neighbors from other ASs are considered eBGP peers.	

neighbor remove-private-as

neighbor {<ip-address> | <peer-group-name>} remove-private-as
no neighbor {<ip-address> | <peer-group-name>} remove-private-as

Removes private autonomous system numbers from outbound routing updates for external BGP (eBGP) neighbors.
The no form of the command preserves private AS numbers for the specified peer.

Syntax Description	ip-address	A BGP peer IP address
	peer-group-name	Peer group name
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 remove-private-as` `switch (config router bgp 100)#`	
Related Commands	ip routing router bgp <as-number>	
Note	• This can only be used with external BGP (eBGP) peers. • If the update has only private AS numbers in the AS path, BGP removes these numbers. • If the AS path includes both private and public AS numbers, BGP does not remove the private AS numbers. This situation is considered a configuration error. • If the AS path contains the AS number of the eBGP neighbor, BGP does not remove the private AS number. • If the AS path contains confederations, BGP removes the private AS numbers only if they come after the confederation portion of the AS path.	

neighbor route-map

neighbor {<ip-address> | <peer-group-name>} route-map <route-map-name> in
no neighbor {<ip-address> | <peer-group-name>} route-map <route-map-name> in

Configures a route map to inbound BGP routes.
The no form of the command undoes the configuration.

Syntax Description	ip-address	IP address of the neighbor
	peer-group-name	Peer group name
	route-map-name	String. The name of the route-map
	in	Applies route map to inbound routes
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.3.5006	First version
	3.3.5200	Updated notes and default
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 route-map MyRouteMap in`	
Related Commands	neighbor <ip-address> remote-as <as-number> route-map <map-name> [deny | permit] [sequence-number] clear ip bgp {<ip-address> | all}	
Note	• Only one inbound route-map can be applied to a given neighbor. • If a new route-map is applied to a neighbor, it replaces the previous route map. • Changing a route-map only takes effect on routes received or sent after the change.	

neighbor route-reflector-client

neighbor {<ip-address> | <peer-group-name>} route-reflector-client
no neighbor {<ip-address> | <peer-group-name>} route-reflector-client

Sets the neighbor as a client but does not set up the reflection itself.
The no form of the command disables route reflection for the specific peer.

Syntax Description	ip-address	IP address of the neighbor.
	peer-group-name	Peer group name
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.3.5006	First version
	3.3.5200	Updated notes and default
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 route-reflector-client`	
Related Commands		
Note		

neighbor send-community

neighbor {<ip-address> | <peer-group-name>} send-community
no neighbor {<ip-address> | <peer-group-name>} send-community

Configures the switch to send community attributes to the specified BGP neighbor. The no form of the command disables sending community attributes for the specified peer.

Syntax Description	ip-address	IP address of the neighbor.
	peer-group-name	Peer group name
Default	Enabled	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 send-community`	
Related Commands	N/A	
Note		

neighbor shutdown

neighbor {<ip-address> | <peer-group-name>} shutdown
no neighbor {<ip-address> | <peer-group-name>} shutdown

Disables BGP neighbor gracefully.
The no form of the command enables BGP neighbor.

Syntax Description	ip-address	IP address of the neighbor.
	peer-group-name	Peer group name
Default	Enabled	
Configuration Mode	Config Router BGP	
History	3.3.5006	First version
	3.3.5200	Updated note
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 shutdown`	
Related Commands	N/A	
Note	Disabling a neighbor terminates all its active sessions and removes associated routing information.	

neighbor soft-reconfiguration inbound

neighbor {<ip-address> | <peer-group-name>} soft-reconfiguration inbound
no neighbor {<ip-address> | <peer-group-name>} soft-reconfiguration inbound

Disables BGP neighbor gracefully.
The no form of the command restores the system default behavior (retaining all routes from the specified neighbor or group).

Syntax Description	ip-address	IP address of the neighbor.
	peer-group-name	Peer group name
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 soft-reconfiguration inbound`	
Related Commands	N/A	
Note	• This command also allows the switch to display all advertised routes when the command `show ip bgp neighbor advertised-routes` is issued. • The no form of the command configures the switch to discard information about routes received from the specified neighbor or group that fail the import policy.	

neighbor timers

neighbor {<ip-address> | <peer-group-name>} timers <keep-alive> <hold-time>
no neighbor {<ip-address> | <peer-group-name>} timers

Configures the keepalive and hold times for a specified peer.
The no form of the command resets the parameters to their default values.

Syntax Description	ip-address	IP address of the neighbor.
	peer-group-name	Peer group name
	keep-alive	The period between the transmission of consecutive keep-alive messages. Range: 1-3600 seconds. “0” means that keepalive is not sent and the connection does not expire.
	hold-time	The period the switch waits for a keepalive or update message before it disables peering. Range: 3-7200 seconds. “0” means that keepalive is not sent and the connection does not expire.
Default	keep-alive: 60 seconds hold-time: 180 seconds	
Configuration Mode	Config Router BGP	
History	3.3.5006	First version
	3.3.5200	Updated description
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 timers 65 195`	
Related Commands	neighbor <ip-address> remote-as <as-number>	
Note	Hold time must be at least 3 seconds and should be three times longer than the keep-alive setting.	

neighbor transport connection-mode passive

neighbor {<ip-address> | <peer-group-name>} transport connection-mode passive
no neighbor {<ip-address> | <peer-group-name>} transport connection-mode passive

Sets the TCP connection for the specified BGP neighbor or peer group to passive mode.
The no form of the command sets the specified BGP neighbor or peer group to active connection mode.

Syntax Description	ip-address	IP address of the neighbor.
	peer-group-name	Peer group name
Default	TCP sessions initiated	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 transport connection-mode passive`	
Related Commands		
Note	• When the peer's transport connection mode is set to passive, it accepts TCP connections for BGP, but does not initiate them. • BGP peers in active mode can both accept and initiate TCP connections for BGP.	

neighbor update-source

neighbor <ip-address> update-source {ethernet <slot/port> | loopback <number> | port-channel <number> | vlan <vlan-id>}
no neighbor <ip-address> update-source

Configures the source-address for routing updates and to establish TCP connections with peers.
The no form of the command disables configured source-address for routing updates and for TCP connection establishment with a peer.

Syntax Description	ip-address	IP address of the neighbor.
	ethernet <slot/port>	Ethernet interface.
	loopback <number>	Loopback interface number.
	vlan <vlan-id>	VLAN interface. Range: 1-4094.
	port-channel <number>	LAG interface. Range is 1-4094.
Default	BGP uses best local address	
Configuration Mode	Config Router BGP	
History	3.3.5006	First version
	3.3.5200	Updated example
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.2 update-source vlan 10`	
Related Commands	N/A	
Note		

neighbor weight

neighbor {<ip-address> | <peer-group-name>} weight <value>
no neighbor {<ip-address> | <peer-group-name>} weight

Assigns a weight attribute to paths from the specified neighbor.
The no form of the command resets to default values.

Syntax Description	ip-address	IP address of the neighbor
	peer-group-name	Peer group name
	value	Weight value. Range: 1-65535.
Default	Value is 32768 for router-originated paths and 0 for routes received through BGP	
Configuration Mode	Config Router BGP	
History	3.4.0000	First version
Role	admin	
Example	`switch (config router bgp 100)# neighbor 10.10.10.10 weight 100`	
Related Commands	N/A	
Note	• Weight values set through route map commands have precedence over neighbor weight command values. • Other attributes are used only when all paths to the prefix have the same weight. • A path's BGP weight is also configurable through route maps. • When multiple paths to a destination prefix exist, the best-path selection algorithm prefers the path with the highest weight. • Weight is the first parameter that the BGP best-path selection algorithm considers.	

network

network <ip-prefix> <length> [<route-map-name>]
no network <ip-prefix> <length> [<route-map-name>]

Configures a route for advertisement to BGP peers.
The no form of the command removes the route from the BGP routes table, preventing its advertisement. The route is only advertised if the router has a gateway to the destination.

Syntax Description	ip-prefix	A string that specific route map is assigned to the network.
	length	/24 or 255.255.255.0 format.
	route-map-name	The name of a route-map which is used to set the route's attributes when it is advertised.
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.3.5006	First version
	3.3.5200	Updated description, syntax description and notes
Role	admin	
Example	`switch (config router bgp 100)# network 10.10.10.0 /24 routemap`	
Related Commands		
Note	• The parameters "ip-prefix" and "length" specify the route destination. • The configuration zeros the host portion of the specified network address. For example, 192.0.2.4/24 is stored as 192.0.2.0/24.	

redistribute

redistribute {connected | static | ospf | ospf-internal | ospf-external} [<route-map>]
no redistribute {connected | static | ospf}

Enables redistribution of specified routes to the BGP domain.
The no form of the command disables route redistribution from the specified source.

Syntax Description	connected	Redistributes the direct routes
	static	Redistributes the user-defined (static) route
	ospf	Redistributes all routes learned by ospf protocol
	ospf-internal	Redistributes all osfp-learned routes which are marked as internal
	ospf-external	Redistributes all osfp-learned routes which are marked as external
Default	No redistribution	
Configuration Mode	Config Router BGP	
History	3.2.1000	
Role	admin	
Example	`switch (config router bgp 100)# redistribute ospf`	
Related Commands	N/A	
Note	Multiple redistribution options can be applied.	

router-id

router-id <ip-address>
no router-id

Configures a fixed router ID for BGP.
The no form of the command removes the fixed router ID and restores the system default.

Syntax Description	ip-address IP Address identified the router ID
Default	The Router ID is dynamically elected (no router-id). • If a loopback interface is configured, the router ID is set to the IP address of the loopback interface. • If multiple loopback interfaces are configured, the router ID is set to the IP address of the loopback interface with the highest IP address. • If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.
Configuration Mode	Config Router BGP
History	3.3.5006
Role	admin
Example	`switch (config router bgp 100)# router-id 10.10.10.10`
Related Commands	
Note	The IP address configured identifies the BGP speaker. The command triggers an automatic notification and session reset for the BGP neighbors.

timers bgp

timers bgp <keep-alive> <hold>
no timers bgp

Configures the BGP keepalive and hold times.
The no form of the command resets the parameters to their default settings.

Syntax Description	keep-alive	Frequency (in seconds) with which keepalive messages are sent to its peer. Range: 1-3600 seconds; 0 – no keep-alive messages are sent.
	hold	Interval (in seconds) after not receiving a keepalive message that a peer is declared dead. 3-7200 seconds; 0 – peer is held indefinitely regardless of keep-alive messages.
Default	Keepalive time: 60 secs Hold time: 180 secs	
Configuration Mode	Config Router BGP	
History	3.3.5006	First version
	3.3.5200	Updated syntax description, related commands and notes
Role	admin	
Example	`switch (config router bgp 100)# timers bgp 61 181` `switch (config router bgp 100)#`	
Related Commands	ip routing neighbor timers router bgp <as-number> show ip bgp	
Note	• Timer settings apply to every peer connection. • The command “neighbor timers” configures the times on a specified peer connection. • Hold time should be three times longer than the keepalive setting.	

6.3.4.3 Show

show ip bgp

show ip bgp [<ip-address> <mask> [detail | longer-prefixes [detail]]]

Displays information about the BGP routes table (RIB).

Syntax Description	ip-address	IP address (e.g. 172.3.12.4).
	mask	Netmask (e.g. /24 or 255.255.255.0).
	detail	Displays detailed information about a subset of the bgp learned routes.
	longer-prefixes	Displays the routes to the specified destination and any routes to a more specific destination. Example: If “10.20.30.0 /24 longer-prefixes” is run, all routes starting with 10.20.30 regardless of the prefix length (10.20.30.X /24, 10.20.30.X /25, etc.) are displayed – providing there are any such routes received/ sent from/to that neighbor.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.5200	
Role	admin	
Example		
Related Commands	N/A	
Note		

```
switch (config) # show ip bgp
BGP table version is 100, local router ID is 16.0.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
      100.100.100.0/24 2.2.2.2 0 2 50 100 e
      100.100.100.0/24 2.2.2.12 0 12 50 100 e
Network            Next Hop        Metric LocPrf Weight Path
20.20.20.0/24      2.2.2.2         0      2      20     e
40.40.40.0/24      4.4.4.4         0      4      40     i
100.100.90.32/28   2.2.2.2         0      2      100    i
100.100.100.0/24   4.4.4.4         0      4      50     i

switch (config) #
```

show ip bgp community

show ip bgp community <comm$_1$> <comm$_2$> … <comm$_n$> [exact] [detail]

Displays information about the BGP routes (RIB) filtered according to communities.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.4.0000
Role	admin
Example	

```
switch (config) # show ip bgp community 100:1
BGP table version is 8, local router ID is 3.5.7.4
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
              r RIB-failure, S Stale, m multipath, b backup-path, x best-
external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop            Metric     LocPrf     Weight
Path
*>  3.4.3.11/32       0.0.0.0                  0          0      32768 i
*>  3.5.7.88/32       0.0.0.0                  0          0      32768 i
*>  3.5.7.99/32       0.0.0.0                  0          0      32768 i

switch (config) # show ip bgp community 100:1 exact
BGP table version is 8, local router ID is 3.5.7.4
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
              r RIB-failure, S Stale, m multipath, b backup-path, x best-
external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop            Metric     LocPrf     Weight
Path
*>  3.4.3.11/32       0.0.0.0                  0          0      32768 i
*>  3.5.7.99/32       0.0.0.0                  0          0      32768 i
```

Related Commands	N/A
Note	

show ip bgp neighbors

show ip bgp neighbors

Displays summaries information about all BGP neighbors.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.5200
Role	admin

Example	`switch (config) # show ip bgp neighbors <ip> received`
	`switch-e07c04 [standalone: master] (config) # show ip bgp neighbors 3.5.7.5 received`
	`BGP table version is 66, local router ID is 3.5.7.4`
	`Status codes: s suppressed, d damped, h history, * valid, > best, i - internal`
	`r RIB-failure, S Stale, m multipath, b backup-path, x best-external`
	`Origin codes: i - IGP, e - EGP, ? - incomplete`
	
	`Network Next Hop Metric LocPrf Weight Path`
	`*> 100.0.20.0/24 3.5.7.5 10 100 0 5 i`
	`*> 3.5.7.128/32 3.5.7.5 7 100 0 5 i`
	`*> 100.0.30.0/24 3.5.7.5 0 100 0 5 i`
	`*> 10.20.30.0/24 3.5.7.5 0 100 0 5 12 i`
	`switch-e07c04 [standalone: master] (config) #`

Related Commands	N/A
Note	

show ip bgp neighbors <ip>

show ip bgp neighbors <ip-address>

Displays BGP summary information.

Syntax Description	ip-address	Neighbor IP address.
	advertised	Displays routes advertised to the specified neighbor.
	received	Displays routes received and accepted from specified neighbor.
	both	Displays routes received from specified neighbor.
	longer-prefixes	Displays the routes to the specified destination and any routes to a more specific destination. Example: If “10.20.30.0 /24 longer-prefixes” is run, all routes starting with 10.20.30 regardless of the prefix length (10.20.30.X /24, 10.20.30.X /25, etc.) are displayed – providing there are any such routes received/sent from/to that neighbor.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.5200	
Role	admin	

Example

```
switch-e07c04 [standalone: master] (config) # show ip bgp neighbors
3.5.7.5 received
BGP table version is 66, local router ID is 3.5.7.4
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
              r RIB-failure, S Stale, m multipath, b backup-path, x best-
external
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf     Weight
Path
*>  100.0.20.0/24     3.5.7.5                10        100         0 5 i
*>  3.5.7.128/32      3.5.7.5                 7        100         0 5 i
*>  100.0.30.0/24     3.5.7.5                 0        100         0 5 i
*>  10.20.30.0/24      3.5.7.5                  0        100          0
5 12 i
switch-e07c04 [standalone: master] (config) #
```

Related Commands	N/A
Note	

show ip bgp neighbors <ip> received

show ip bgp neighbors <ip-address> received [<ip-address> [<mask>] [longer-prefixes]

Displays BGP summary information.

Syntax Description	ip-address	Neighbor IP address.
	received	Displays routes received and accepted from specified neighbor.
	longer-prefixes	Displays the routes to the specified destination and any routes to a more specific destination. Example: If “10.20.30.0 /24 longer-prefixes” is run, all routes starting with 10.20.30 regardless of the prefix length (10.20.30.X /24, 10.20.30.X /25, etc.) are displayed – providing there are any such routes received/sent from/to that neighbor.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.5200	
Role	admin	
Example		
Related Commands	N/A	
Note		

show ip bgp paths

show ip bgp paths

Displays summary of all AS paths.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.5200
Role	admin

Example	`switch (config) # show ip bgp paths`
	`Refcount  Metric  Path`
	`1  0  4 50 100`
	`1  0  2 50 100`
	`1  0  4 40`
	`1  0  12 50 100`
	`1  0  2`
	`1  0  2 20`
	`switch (config) #`

Related Commands	N/A
Note	

show ip bgp peer-group

show ip bgp peer-group [<peer-group-name>]

Displays information about peer groups.

Syntax Description	peer-group-name	Displays information about a specific peer-group.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.4.0000	
Role	admin	

Example

```
switch (config) # show ip bgp peer-group
BGP Peer-group [grpA]:
Hold time: 1, Keep-alive: 60
Allow as-in: 0
Weight: 32768
Max prefix: 12000
Export local preferences: 100, Import local preferences: 100
Soft reconfiguration: set
Neighbor        V       AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down
State/PfxRcd
3.5.7.5          0         5      0      0      0    0    0 0:00:00:42
CONNECT
100.100.100.100   0       100      0      0      0    0    0 Never
IDLE

BGP Peer-group [grpB]:
Hold time: 1, Keep-alive: 60
Allow as-in: 0
Weight: 32768
Max prefix: 12000
Export local preferences: 100, Import local preferences: 100
Soft reconfiguration: set
Neighbor        V       AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down
State/PfxRcd
3.4.3.7          0         7      0      0      0    0    0 0:00:00:17
ACTIVE

BGP Peer-group [tomer_group]:
Hold time: 1, Keep-alive: 60
Allow as-in: 0
Weight: 32768
Max prefix: 12000
Export local preferences: 100, Import local preferences: 100
Soft reconfiguration: set

Peer-groups count: 3
switch-e07c04 [standalone: master] (config) #
```

Related Commands	N/A
Note	

show ip bgp summary

show ip bgp summary

Displays BGP summary information.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.5200
Role	admin

Example	`switch (config) # show ip bgp summary`
	`BGP router identifier 3.5.7.4, local AS number 4`
	`BGP table version is 70, main routing table version 70`
	`8 network entries using 2176 bytes of memory`
	`4 path entries using 1088 bytes of memory`
	`4 BGP path attribute entries using 256 bytes of memory`
	`0 multipath network entries and 0 multipath paths`
	`4 BGP community entries using 64 bytes of memory`
	`0 received paths for inbound soft reconfiguration`
	`BGP using 26308 total bytes of memory`
	`Dampening disabled. 0 history paths, 0 dampened paths`
	`BGP activity 37/8 prefixes, 37/4 paths`
	`Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd`
	`3.4.3.7 4 7 3 9 70 0 0 0:00:00:48 ESTABLISHED`
	`3.5.7.5 0 5 0 0 0 0 0 0:00:01:54 CONNECT`
	`100.100.100.100 0 100 0 0 0 0 0 Never IDLE`
	
	`switch-e07c04 [standalone: master] (config) #`

Related Commands	N/A
Note	

6.3.5 IP AS-Path Access-List

6.3.5.1 Commands

ip as-path access-list

ip as-path access-list <list-name> {permit | deny} <reg-exp> [any | egp | igp | incomplete]
no ip as-path access-list <list-name>

Creates an access list to filter BGP route updates.
The no ip as-path access-list command deletes the named access list.

Syntax Description	list-name	The name for the access list
	permit	Permits access for a matching condition
	deny	Denies access for a matching condition
	reg-exp	Regular expression that is used to specify a pattern to match against an input string.
	any	Any route type
	egp	External BGP routes
	igp	Internal BGP routes
	incomplete	Routes marked as “Incomplete”
Default	N/A	
Configuration Mode	Config	
History	3.4.0000	
Role	admin	
Example	`switch (config)# ip as-path access-list mylist permit` `switch (config)#`	
Related Commands	N/A	
Note	If access list_name does not exist, this command creates it. If it already exists, this command appends statements to the list.	

show ip as-path access-list

show ip as-path access-list [list-name]

Presents defined as-path access lists

Syntax Description	list-name	Displays a specific prefix-list.
Default	N/A	
Configuration Mode	Config	
History	3.4.0000	
Role	admin	
Example	`switch (config)# show ip as-path access-list mylist`	
Related Commands	N/A	
Note		

6.3.6 IP Community-List

6.3.6.1 Commands

ip community-list standard

ip community-list standard <list-name> {deny | permit} <list-of-communities>
no ip community-list standard <list-name>

Adds a standard entry to a community-list.
The no form of the command deletes the specified community list.

Syntax Description	list-name	The name for the community list
	permit	Permits access for a matching condition.
	deny	Denies access for a matching condition.
	list-of-communities	List of standard communities: • <aa:nn> • <number> • internet • local-AS • no-advertise • no-export
Default	N/A	
Configuration Mode	Config	
History	3.4.0000	
Role	admin	
Example	`switch (config)# ip community-list standard mycommunity permit 1:2 3:4`	
Related Commands	N/A	
Note	A BGP community access list filters route maps that are configured as BGP communities. The command uses regular expressions to name the communities specified by the list.	

ip community-list expanded

ip community-list expanded <list-name> {deny | permit} <reg-exp>
no ip community-list expanded <list-name>

Adds a regular expression entry to a community-list
The no form of the command deletes the specified community list.

Syntax Description	list-name	Configures a named standard community list.
	permit	Permits access for a matching condition.
	deny	Denies access for a matching condition.
	reg-exp	Regular expression that is used to specify a pattern to match against an input string.
Default	N/A	
Configuration Mode	Config	
History	3.4.0000	
Role	admin	
Example	`switch (config)# ip community-list expanded mycommunity permit 1:[0-9]+`	
Related Commands	N/A	
Note	A BGP community access list filters route maps that are configured as BGP communities. The command uses regular expressions to name the communities specified by the list.	

show ip community-list

show ip community-list [community-list-name]

Displays the defined community lists

Syntax Description	community-list-name	An optional parameter to display only the specified list
Default	N/A	
Configuration Mode	Config	
History	3.4.0000	
Role	admin	
Example	`switch (config)# show ip community-list mycommunity`	
Related Commands	N/A	
Note	A BGP community access list filters route maps that are configured as BGP communities. The command uses regular expressions to name the communities specified by the list.	

6.4 Policy Rules

6.4.1 Route Map

Route maps define conditions for redistributing routes between routing protocols. A route map clause is identified by a name, filter type (permit or deny) and a sequence number. Clauses with the same name are components of a single route map; the sequence number determines the order in which the clauses are compared to a route.

6.4.1.1 Commands

route-map

route-map <map-name> [deny | permit] [sequence-number]
no route-map <map-tag> {deny | permit} [<sequence-number>]

Creates a route map that can be used for importing, exporting routes and applying local policies.

Syntax Description	name	Name of the route-map.
	deny | permit	Configures the rule to be used.
	sequence-number	Sequence number for a route-map specific record.
Default	N/A	
Configuration Mode	Config	
History	3.3.5006	
	3.3.5200	Updated notes
Role	admin	
Example	`switch (config) # route-map mymap permit 1200` `switch (config route-map mymap permit 1200)#`	
Related Commands	N/A	
Note	• All changes in a the route map configuration mode become pending until the end of the route-map session. • If not configured, deny | permit is configured as permit. • If not configured, sequence-number default value is 10.	

continue <sequence-number>

continue <sequence-number>
no continue

Enables additional route map evaluation of routes whose parameters meet the clause's matching criteria.
The no form of the command removes this configuration from the route map clause.

Syntax Description	prefix-list-name	
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5006	First version
	3.3.5200	Updated example
Role	admin	

Example

```
switch (config route-map mymap permit 10)# match as-number 40
switch (config route-map mymap permit 10)# set weight 7
switch (config route-map mymap permit 10)# continue 1200
switch (config route-map mymap permit 10)# exit
switch (config)# show route-map test
route-map test, permit, sequence 10
  Match clauses:
    as-number 40
  Set clauses:
    weight 7
    continue 1200
switch (config route-map mymap permit 10)# route-map test permit 10 no
continue
switch (config route-map mymap permit 10)# show route-map test
route-map test, permit, sequence 10
  Match clauses:
    as-number 40
  Set clauses:
    weight 7
switch (config route-map mymap permit 10)#
```

Related Commands route-map <map-name> [deny | permit] [sequence-number]

Note

- A clause typically contains a match (route-map) and a set (route-map) statement. The evaluation of routes whose settings are the same as match statement parameters normally end and the clause's set statement are applied to the route. Routes that match a clause containing a continue statement are evaluated against the clause specified by the continue statement.
- When a route matches multiple route-map clauses, the filter action (deny or permit) is determined by the last clause that the route matches. The set statements in all clauses matching the route are applied to the route after the route map evaluation is complete. Multiple set statements are applied in the same order by which the route was evaluated against the clauses containing them.
- Continue cannot be set to go back to a previous clause; <sequence-number> of the continue must always be higher than the current clause's sequence number.

abort

abort

Discards pending changes and returns to global configuration mode.

Syntax Description	N/A	
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5006	First version
	3.3.5200	Updated example
Role	admin	

Example	`switch (config)# route-map mymap permit 10 match as-number 40`
	`switch (config)# route-map mymap permit 10 set weight 7`
	`switch (config)# show route-map test`
	`route-map test, permit, sequence 10`
	`  Match clauses:`
	`    as-number 40`
	`  Set clauses:`
	`    weight 7`
	`switch (config)# route-map mymap permit 1200`
	`switch (config route-map mymap permit 1200)# set weight 11`
	`switch (config route-map mymap permit 1200)# abort`
	`switch (config)# show route-map mymap`
	`route-map mymap, permit, sequence 10`
	`  Match clauses:`
	`    as-number 40`
	`  Set clauses:`
	`    weight 7`
	`switch (config)#`	

Related Commands	N/A	
Note		

exit

exit

Saves pending route map clause changes to running-config and returns to global configuration mode.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config Route Map
History	3.3.5006
Role	admin

Example	`switch (config)# route-map mymap permit 10 match as-number 40`
	`switch (config)# route-map mymap permit 10 set weight 7`
	`switch (config)# show route-map test`
	`route-map test, permit, sequence 10`
	`  Match clauses:`
	`    as-number 40`
	`  Set clauses:`
	`    weight 7`
	`switch (config)# route-map mymap permit 1200`
	`switch (config route-map mymap permit 1200)# set weight 11`
	`switch (config route-map mymap permit 1200)# exit`
	`switch (config)# show route-map test`
	`route-map mymap, permit, sequence 10`
	`  Match clauses:`
	`    as-number 40`
	`  Set clauses:`
	`    weight 7`
	`route-map mymap, permit, sequence 1200`
	`  Set clauses:`
	`    weight 11`
	`switch (config)#`

Related Commands	N/A
Note	

match as-number

match as-number <number>
no match as-number

Filters according to one of the AS numbers in the AS path of the route.
The no form of the command removes this configuration from the route map clause.

Syntax Description	number	Autonomous system number to check.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5006	
Role	admin	
Example	`switch (config route-map mymap permit 10)# match as-number 40` `switch (config route-map mymap permit 10)#`	
Related Commands	N/A	
Note	• When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement. • When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number. • If all clauses fail to permit or deny the route, the route is denied.	

match as-path

match as-path <as-path-list name>
no match as-path

Creates a route map clause entry that matches the route‘s AS path using an as-path access-list.
The no form of the command removes the match statement from the configuration mode route map clause.

Syntax Description	number	Autonomous system number to check.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5006	
Role	admin	
Example	`switch (config route-map mymap permit 10)# match as-path my-list`	
Related Commands	N/A	
Note	• When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement. • When a route’s properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number. • If all clauses fail to permit or deny the route, the route is denied.	

match community

match community <list-of-communities> [exact-match]
no match community <list-of-communities>

Creates a route map clause entry that matches a route if it contains at least the specified communities.
The no form of the command removes the match clause.

Syntax Description	list of communities	List of standard communities: • <aa:nn> • <number> • internet • local-AS • no-advertise • no-export
	exact-match	Creates a route map clause entry that matches the route‘s communities exactly.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5006	
Role	admin	
Example	`switch (config route-map mymap permit 10)# match community 1:100 3:52`	
Related Commands	N/A	
Note	• When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement. • When a route’s properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number. • If all clauses fail to permit or deny the route, the route is denied.	

match community-list

match community <communities-list-name> exact-match
no match community <communities-list-name> exact-match

Creates a route map clause entry that specifies one route filtering condition
The no form of the command removes the match clause.

Syntax Description	communities-list-name A name of an IP community list
Default	N/A
Configuration Mode	Config Route Map
History	3.3.5006
Role	admin
Example	`switch (config route-map mymap permit 10)# match community-list COM_LIST exact-match`
Related Commands	N/A
Note	• When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement. • When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number. • If all clauses fail to permit or deny the route, the route is denied.

match interface

match interface <interface-type> <number>
no match interface

Matches the route's interface
The no form of the command removes the match clause.

Syntax Description	prefix-list-name	Prefix-list name.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5006	
Role	admin	
Example	`switch (config route-map mymap permit 10)# match interface ethernet 1/1`	
Related Commands	N/A	
Note	• When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement. • When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number. • If all clauses fail to permit or deny the route, the route is denied.	

match ip address

match ip address <prefix-list-name>
no match ip address

Filters according to IPv4 prefix list.
The no form of the command removes this configuration from the route map clause.

Syntax Description	prefix-list-name	Prefix-list name.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5006	
Role	admin	
Example	`switch (config route-map mymap permit 10)# match ip address listSmallRoutes`	
Related Commands	N/A	
Note	• When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement. • When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number. • If all clauses fail to permit or deny the route, the route is denied. • The prefix-list-name should point to an existing IP prefix-list. If it is not found, no route is considered as a match for this clause.	

match ip next-hop

match ip next-hop <value>
no match ip next-hop

Configures a route's entry next-hop match.
The no form of the command removes a route-map's entry next-hop match.

Syntax Description	value	Next hop IP address: A.B.C.D (e.g. 10.0.13.86).
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
Role	admin	
Example	`switch (config route-map mymap permit 10)# match ip next-hop 10.10.10.10`	
Related Commands	N/A	
Note	• When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement. • When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number. • If all clauses fail to permit or deny the route, the route is denied.	

match local-preference

match local-preference <value>
no match local-preference

Configures a route's entry local-preference match.
The no form of the command removes a route-map's entry local-preference match.

Syntax Description	value	Range: 1-2147483647.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	First version
	3.4.0000	Updated value range
Role	admin	
Example	`switch (config route-map mymap permit 10)# match local-preference 10`	
Related Commands	N/A	
Note	• When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement. • When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number. • If all clauses fail to permit or deny the route, the route is denied.	

match metric

match metric <value>
no match metric

Configures a route's entry metric match.
The no form of the command removes a route-map's entry metric match.

Syntax Description	value	Range: 1-2147483647.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	First version
	3.4.0000	Updated value range
Role	admin	
Example	`switch (config route-map mymap permit 10)# match metric 10`	
Related Commands	N/A	
Note	• When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement. • When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number. • If all clauses fail to permit or deny the route, the route is denied.	

set as-path prepend

set as-path prepend <value$_1$> <value$_2$> ... <value$_n$>
no set as-path prepend

Modifies as-path on affected routes
The no form of the command removes the set statement from the route map.

Syntax Description	value	BGP AS number that is prepended to as-path. Range: 1-4294967295.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.4.0000	
Role	admin	
Example	`switch (config route-map mymap permit 10)# set as-path prepend 5 10`	
Related Commands	N/A	
Note		

set as-path tag

set as-path tag <value>
no set as-path tag

Configures a route's entry AS-path tag parameter.
The no form of the command removes a route-map's entry AS path tag setting.

Syntax Description	value	Range: 1-2147483648.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
Role	admin	
Example	`switch (config route-map mymap permit 10)# set as-path tag 1`	
Related Commands	N/A	
Note		

set community

set community {<list of communities> | none}
no set community {<list of communities> | none}

Sets the community attribute of a distributed route
The no form of the command removes the set statement from the clause.

Syntax Description	list of communities	List of standard communities: • <aa:nn> • <number> • internet • local-AS • no-advertise • no-export
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
Role	admin	
Example	`switch (config route-map mymap permit 10)# set community 1:2 3:4`	
Related Commands	N/A	
Note		

set community additive

set community {<list of communities> | none}
no set community {<list of communities> | none}

Adds the matching communities
The no form of the command removes the set statement from the clause.

Syntax Description	list of communities	List of standard communities: • <aa:nn> • <number> • internet • local-AS • no-advertise • no-export
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
Role	admin	
Example	`switch (config route-map mymap permit 10)# set community none`	
Related Commands	N/A	
Note		

set community none

	set community none **no set community none** Sets the community attribute of a distributed route to be empty The no form of the command removes the set statement from the clause.
Default	N/A
Configuration Mode	Config Route Map
History	3.3.5200
Role	admin
Example	`switch (config route-map mymap permit 10)# set community none`
Related Commands	N/A
Note	

set community delete

set community <list of communities> delete
no set community <list of communities> delete

Deletes matching communities.
The no form of the command removes the set statement from the clause.

Syntax Description	list of communities	List of standard communities: • <aa:nn> • <number> • internet • local-AS • no-advertise • no-export
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
Role	admin	
Example	`switch-e07c04 [standalone: master] (config) # route-map test_route_map` `switch-e07c04 [standalone: master] (config route-map test_route_map permit 10) # set community 400:1 delete`	
Related Commands	N/A	
Note		

set community-list

set community-list <community-list-name>
no set community <list of communities>

Configures a named standard community list.
The no form of the command removes the set statement from the clause.

Syntax Description	<community-list-name> Name of community list
Default	N/A
Configuration Mode	Config Route Map
History	3.3.5200
Role	admin
Example	`switch (config route-map mymap permit 10)# set community internet 1:3 additive`
Related Commands	N/A
Note	

set community-list additive

set community-list <community-list-name> additive
no set community <list of communities> additive

Adds to existing communities using the communities found in the community list. The no form of the command removes the set statement from the clause.

Syntax Description	<community-list-name> Name of community list
Default	N/A
Configuration Mode	Config Route Map
History	3.3.5200
Role	admin
Example	`switch (config route-map mymap permit 10)# set community-list mycommunity additive`
Related Commands	N/A
Note	

set community-list delete

set community-list <community-list-name> delete
no set community-list

Deletes the matching community list permit entries from the route community list
The no form of the command removes the set statement from the clause.

Syntax Description	community-list-name	Name of community list
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
Role	admin	
Example	`switch (config route-map mymap permit 10)# set community-list mycommunity delete`	
Related Commands	N/A	
Note		

set ip next-hop

set ip next-hop <value>
no set ip next-hop

Configures a route's entry next-hop parameter.
The no form of the command removes a route-map's entry next-hop setting.

Syntax Description	value	Route next-hop IP: A.B.C.D (e.g. 10.0.13.86).
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
Role	admin	
Example	`switch (config route-map mymap permit 10)# set ip next-hop 10.10.10.10`	
Related Commands	N/A	
Note		

set local-preference

set local-preference <value>
no set local-preference

Configures a route's entry local-preference parameter.
The no form of the command removes a route-map's entry local-pref setting.

Syntax Description	value	Route local-pref: 1-2147483648.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
Role	admin	
Example	`switch (config route-map mymap permit 10)# set local-preference 10`	
Related Commands	N/A	
Note		

set metric

set metric <value>
no set metric

Configures a route's entry metric parameter.
The no form of the command removes a route-map's entry metric setting.

Syntax Description	value	Route metric: 1-2147483647.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
Role	admin	
Example	`switch (config route-map mymap permit 10)# set metric 10`	
Related Commands	N/A	
Note		

set origin

set origin {egp | igp | incomplete}
no set origin

Configures a route's entry origin parameter.
The no form of the command removes a route-map's entry origin setting.

Syntax Description	egp	Set a route's entry origin parameter to external.
	igp	Set a route's entry origin parameter to internal.
	incomplete	Set a route's entry origin parameter to incomplete.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
Role	admin	
Example	`switch (config route-map mymap permit 10)# set origin egp`	
Related Commands	N/A	
Note		

set tag

set tag <value>
no set tag

Configures a route's entry tag parameter.
The no form of the command removes a route-map's entry tag setting.

Syntax Description	value	Range: 1-2147483647.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
	3.4.0000	Updated parameter range
Role	admin	
Example	`switch (config route-map mymap permit 10)# set tag 10`	
Related Commands	N/A	
Note		

set weight

set weight <number>
no set weight

Configures modifications to redistributed routes.
The no form of the command removes this configuration from the route map clause.

Syntax Description	number	Value of the weight to set. Range: 1-65535.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5006	First version
	3.4.0000	Updated parameter range
Role	admin	
Example	`switch (config route-map mymap permit 10)# set weight 7`	
Related Commands	route-map <map-name> [deny | permit] [sequence-number]	
Note		

show route-map

show route-map [<name>]

Displays route map configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.5006
Role	admin

Example	`switch (config)# show route-map mymap`
	`route-map mymap, permit, sequence 1200`
	`  Set clauses:`
	`    continue 1800`
	`switch (config)#`

Related Commands	N/A
Note	

6.4.2 IP Prefix-List

Prefix-list is a list of entries, each of which can match one or more IP prefixes. A prefix-list is usually used to match a specific IP prefix, mostly in relation to IP route destinations.

The prefix is considered to match the list if one of the entries match the prefix; the entry itself can be marked as a “permit” entry or a “deny” entry, which can be used by the matching code to decide if the route is to be accepted or not.

The prefix is matched to the prefix-list entries in the order of the sequence number of the entries in the list.

6.4.2.1 Commands

ip prefix-list

ip prefix-list <list-name> [seq <number>] {permit | deny} <ip> [eq <length> | <prefix> [eq <length> | le <length> | ge <length> [le <length>]]]
no ip prefix-list <list-name> [seq <number>]

Creates or updates a prefix-list.
The no form of the command deletes a prefix-list or a prefix-list entry

Syntax Description	list-name	String
	seq <number>	Sequence number assigned to entry. Range: 0-65535.
	permit	Permits access for a matching condition.
	deny	Denies access for a matching condition.
	ip	IP address
	eq | ge | le <mask>	• eq: Equal to a specified prefix length • ge: Greater than or equal to a specified prefix length • le: Less than or equal to a specified prefix length
Default	Sequence value = 10	
Configuration Mode	Config	
History	3.3.5200	
Role	admin	
Example	`switch (config)# ip prefix-list a-list permit 10.20.0.0 /16 eq 24` `switch (config)#`	
Related Commands	N/A	
Note		

show ip prefix-list

show ip prefix-list [<name>]

Displays prefix-lists.

Syntax Description	name	Displays a specific prefix-list.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.5200	
Role	admin	

Example	`switch (config)# show ip prefix-list`
	`prefix-list: a-list`
	`  count: 1, range entries: 1, sequences: 10 - 10`
	`  seq 10 permit 10.20.0.0 /16 ge 24 (hit count: 0, refcount: 0)`
	`prefix-list: b-list`
	`  count: 2, range entries: 2, sequences: 10 - 20`
	`  seq 10 deny 10.10.0.0 /16 le 24 (hit count: 0, refcount: 0)`
	`  seq 20 deny 10.20.0.0 /16 le 24 (hit count: 0, refcount: 0)`
	`switch (config)#`	

Related Commands	N/A	
Note		

6.5 Multicast (IGMP and PIM)

Protocol independent multicast (PIM) is a collection of protocols that deal with efficient delivery of IP multicast (MC) data. Those protocols are published in the series of RFCs and define different ways and aspects of multicast data distribution. PIM protocol family includes PIM dense mode (PIM-DM), PIM sparse mode (PIM-SM), Bidirectional PIM (PIM-BIDIR) and Bootstrap router (BSR) protocol.

PIM builds and maintains multicast routing tables based on the unicast routing information provided by unicast routing tables that can be maintained statically or dynamically by IP routing protocols like OSPF and BGP.

6.5.1 Basic PIM-SM

PIM relies on the underlying topology gathering protocols that collect unicast routing information and build multicast routing information base (MRIB). The primary role of MRIB is to determine the next hop for PIM messages. MC data flows along with the reverse path of the PIM control.

MC tree construction contains three phases:

1. Construction of a shared distribution tree. This tree is built around a special designated router (DR) called the rendezvous point (RP).
2. Establishing a native forwarding path from MC sources to the RP
3. Building an optimized MC distribution tree from each MC source to all MC targets bypassing the RP

The first stage of the multicast tree establishment starts when the MC receiver expresses desire to start receiving MC data. It can happen as a result of using one of the L2 protocols like MLD or IGMP, or by static configuration. When such request is received by the last hop router (a designated router) this router starts to build a distribution path from the RP. It starts to send periodic “Join” messages to the nearest PIM neighbor router towards the RP. The next router continues to do the same. Eventually the process converges when Join messages reach RP or a router that has already created that distribution tree. Usually that tree is called a shared tree because it is created for any source for specific MC group G and is noted as (*,G).

At that stage, MC senders can start sending MC data. The DR next to the MC source extracts the packets from the data flow and tunnels them to the RP. The RP decapsulates the packets and distributes them to all MC receivers along with the share tree.

On the second stage the RP switches from tunneling of multicast packets from MC sources to forwarding native traffic. When the RP identifies that a new MC source started to send packets, it initiates an establishment of a native forwarding path from the DR of that source to itself. For this purpose it starts to send Join messages towards MC source to nearest neighbor to that source according the MRIB. This is a source specific Join and is noted as (S,G). When data path is established up to the DR, the DR switches from tunneling MC packets to their native forwarding, so the RP does not need to decapsulate MC packets anymore, but still continue to distribute the packets along with shared tree.

On the third phase multicast receivers will try to switch from shared tree to source specific tree by creating a direct distribution path from a multicast source. When last hop router of the multicast receiver identifies multicast traffic coming from any multicast source it will start to send Join messages towards the source with purpose to create a direct source specific path to that source. Once such path will be established and Designated router that is attached to the source L2

network will start to distribute the multicast traffic directly bypassing shared tree, the last hop router will detach its receivers from shared tree for that data and will switch to the shortest path tree distribution.

6.5.2 Bidirectional PIM

Bidirectional PIM (PIM-BIDIR) is a variant of PIM-SM that builds bidirectional distribution trees that connect multicast senders and receivers. It differs from PIM-SM by eliminating a need to tunnel multicast packets to RP and to keep a state for each (S,G) pair. It also eliminates a need in data driven protocol events. PIM-BIDIR achieves it by defining a new role, Designated Forwarder (DF), and by defining new forwarding rules and keeping all other PIM-SM mechanisms intact.

DF is a PIM enabled router that is the closest router to RP among all PIM routers residing on specific L2 network. It is dynamically elected by all PIM routers on that network. DF is required on each L2 multicast capable network for each RP. DF serves all multicast groups that share the same RP and has following duties:

- It is an only router that is responsible to receive and forward upstream multicast packets on that L2 segment
- It is a router that should collect all Join requests from the routers on that L2 segment
- It is an only router that will distribute downstream multicast packets on that segment.

Once Designated forwarders are elected and forwarding rules are established, PIM routers can start to issue (*,G) Join messages and build shared distribution trees. When shared tree is created, multicast sources can start to exchange data with receivers and it doesn't require any additional maintenance of the multicast states.

Compared to PIM-SM, in bidirectional PIM:

- Each router will keep only (*,G) state and not (*,G) and (S,G) like in PIM-SM
- Multicast traffic from the beginning is forwarded naturally - no need to tunnel data to RP
- Resulting multicast tree is not shortest path optimal and converges around selected Rendezvous point, but is shared among all participants in that multicast group

In BIDIR-PIM, the packet forwarding rules have been improved over PIM-SM, allowing traffic to be passed up the shared tree toward the RP. To avoid multicast packet looping, bidir-PIM introduces a new mechanism called designated forwarder (DF) election, which establishes a loop-free SPT rooted at the RP.

6.5.3 Bootstrap Router

For correct operation each PIM router requires a capability to map a multicast group that it needs to serve to a Rendezvous point for that group. This mapping can be done manually or the mapping can be distributed dynamically in the network. BSR protocol serves for this purpose.

This protocol introduces new role in the multicast network – Bootstrap router. That router is responsible to flood multicast group to RP mapping through the multicast routing domain. Bootstrap router is elected dynamically among bootstrap router candidates (C-BSR) and once elected will collect from Rendezvous point candidate (C-RP) mapping information and distribute it in the domain.

Bootstrap activity contains 4 steps. First each C-BSR configured in the network originates floods into the network bootstrap messages that express the router desire to become BSR and also its

BSR priority. Any C-BSR that receives that information and has lower priority will suspend itself, so eventually only one router will send BSR messages and become BSR.

When BSR is elected all RP candidates start to advertise to BSR a list of groups that this RP can serve. On the next step, after BSR learns the group mapping proposals, it forms a final group to RP mapping in the domain and starts to distribute it among PIM routers in the multicast routing domain. When PIM router receives BSR message with the group to RP mapping, it installs that mapping in the router local cache and uses that information to create multicast distribution trees.

6.5.4 Configuring Multicast

Precondition steps:

Step 1. Enable IP routing functionality. Run:

```
switch (config)# ip routing
```

Step 2. Enable the desired VLAN. Run:

```
switch (config)# vlan 10
```

Step 3. Add this VLAN to the desired interface. Run:

```
switch (config)# interface ethernet 1/1
switch (config ethernet 1/1)#switchport access vlan 10
```

Step 4. Create a VLAN interface. Run:

```
switch (config)# interface vlan 10
```

Step 5. Apply IP address to the VLAN interface. Run:

```
switch (config interface vlan 10)# ip address 10.10.10.10 /24
```

Step 6. Enable the interface. Run:

```
switch (config interface vlan 10)# no shutdown
```

6.5.4.1 Configuring IGMP

IGMP is enabled when IP multicast is enabled and static multicast or PIM is enabled on the interface.

6.5.4.2 Verifying IGMP

Step 1. Display a brief IGMP interface status. Run:

```
switch (config)# show ip igmp interface brief
IGMP Interfaces for VRF "default", Count: 1
Interface        IP Address       IGMP Querier   Membership    Version
VLAN10           10.10.10.1       10.10.10.1      5             v2
```

Step 2. Display detailed IGMP interface status. Run:

```
switch (config)#show ip igmp interface vlan 10
IGMP Interfaces for VRF "default"

VLAN10
 Interface status: protocol-up/admin-up/link-up
 IP address: 10.10.10.1, IP Subnet: 10.10.10.0/24
 Active Querier:  10.10.10.1
 Membership count: 5
 Route-queue depth: 0
 IGMP Version:  2
 IGMP query interval:  125 secs, configured value:   125 secs
 IGMP max response time:  10  secs, configured value:   10  secs
 IGMP startup query interval:  125  secs, configured value:   125  secs
 IGMP startup query count:       2
 IGMP group timeout:  260  secs, configured value:   260  secs
 IGMP querier timeout:  260  secs configured value:   260  secs
 IGMP last member mrt:  25  secs configured value:   25
 IGMP robustness variable:       2
 IGMP interface immediate leave: Disabled
 IGMP interface statistics:
 General (sent/received):
 v1/v2-reports:  0/10
 v2-queries:     271/0,v2-leaves:  0/0
 v3-queries:     0/0,
 v3-reports:     0/0
switch (config)#
```

Step 3. Display the list of IGMP groups and their status. Run:

```
switch (config)#show ip igmp groups
IGMP Connected Group Membership for VRF "default", - 2 total entries
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address Type     Interface Uptime            Expires          Last
Reporter
 226.0.1.0    D       vlan10    [0d 00:00:07.46]  [0d 00:04:05.08] 10.10.10.2
  226.0.1.1    D       vlan10    [0d 00:00:07.47]  [0d 00:04:05.08] 10.10.10.2
switch (config)#
```

6.5.4.3 Configuring PIM

Prerequisites:

Step 1. If not enabled, enable IP routing. Run:

```
switch (config)# ip routing
```

Step 2. Globally enable multicast routing. Run:

```
switch (config)# ip multicast-routing
```

➢ ***To configure PIM:***

Step 1. Enable PIM. Run:

```
switch (config)# protocol pim
```

Step 2. Globally enable Bidirectional PIM (BIDIR mode). Run:

```
switch (config)# no ip pim bidir shutdown
```

6.5.5 Commands

6.5.5.1 PIM

protocol pim

protocol pim
no protocol pim

Enables protocol independent multicast (PIM).
The no form of the command hides all PIM commands and deletes all PIM configurations.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.5006
Role	admin
Example	`switch (config) # protocol pim`
Related Commands	N/A
Note	

ip pim bidir shutdown

ip pim bidir shutdown
no ip pim bidir shutdown

Disables PIM bidir.
The no form of the command enables PIM bidir.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.5006
Role	admin
Example	`switch (config) # no ip pim bidir shutdown`
Related Commands	N/A
Note	

ip pim rp-address

ip pim rp-address <rp-address> [group-list <ip-address> <prefix>] [override] bidir
no ip pim rp-address <rp-address> [group-list <ip-address> <prefix>]

Configures a static IP address of a rendezvous point for a multicast group range or adds new multicast range to existing RP.
The no form of the command removes the rendezvous point for a multicast group range or removes all configuration of the RP.

Syntax Description	rp-address	The static IP address of rendezvous point.
	ip-address	IP address of the group-range (coupled with the prefix parameter).
	prefix	Network prefix (in the format of /24, or 255.255.255.0 for example) of group range.
	override	Specifies that this configuration overrides dynamic configuration learned by BSR.
	bidir	Specifies that the group range uses a bidirectional PIM.
Default	N/A	
Configuration Mode	Config	
History	3.3.5006	
Role	admin	
Example	`switch (config) # ip pim rp-address 10.10.10.10 bidir`	
Related Commands	N/A	
Note		

ip pim bsr-candidate

ip pim bsr-candidate {vlan <vlan-id> | loopback <number> | ethernet <port>} [hash-len <hash-length>] [priority <priority>] [interval <interval>]
no ip pim bsr-candidate {vlan <vlan-id> | loopback <number> | ethernet <port>} [hash-len <hash-length>] [priority <priority>] [interval <interval>]

Configures the switch as a candidate BSR router (C-BSR).
The no form of the command removes BSR-candidate configuration or restores default parameters values.

Syntax Description	vlan <vlan-id>	The VLAN ID. Range is 1-4094.
	loopback <number>	Loopback interface number.
	ethernet <port>	Ethernet interface.
	hash-len	Specifies the hash mask length used in BSR messages. Range: 0-32.
	priority	BSR priority rating. Larger numbers denote higher priority. Range: 0-255.
	interval	Period between the transmission of BSMs (seconds). Range:10-536870906.
Default	The interface is not BSR candidate by default. priority: 64 interval: 60 hash-len: 30	
Configuration Mode	Config Config Interface Ethernet configured as a router port Config Interface Loopback Config Interface Port Channel configured as a router port Config Interface VLAN	
History	3.3.5006	
Role	admin	
Example	`switch (config) # ip pim bsr-candidate vlan 10 priority 100`	

Related Commands	ip pim sparse-mode
Note	• IP PIM sparse-mode must be enabled on the interface. • A BSR is a PIM router within the PIM domain through which dynamic RP selection is implemented. The BSR selects RPs from a list of candidate RPs and exchanges bootstrap messages (BSM) with all routers in the domain. The BSR is elected from one of the C-BSRs through an exchange of BSMs. A subset of PIM routers within the domain are configured as candidate Bootstrap routers (C-BSRs). Through the exchange of Bootstrap messages (BSMs), the C-BSRs elect the BSR, which then uses BSMs to inform all domain routers of its status. • Command parameters specify the switch's BSR address, the interval between BSM transmissions, hash length used for RP calculations and the priority assigned to the switch when electing a BSR. • Entering an ip pim bsr-candidate command replaces any previously configured bsr-candidate command. If the new command does not specify a priority or interval, the previously configured values persist in running-config.

ip pim bsr-holdtime

ip pim bsr-holdtime <period>
no ip pim bsr-holdtime

Configures the timeout period an elected BSR remains valid after receiving a BSM. The no form of the command resets the parameters to their default.

Syntax Description	period	In seconds. Range: 12-1073741823 (1.073 billion).
Default	period = 2*(BSR candidate interval) + 10	
Configuration Mode	Config	
History	3.3.5006	
Role	admin	
Example	`switch (config) # ip pim bsr-holdtime 30`	
Related Commands		
Note		

ip pim rp-candidate

ip pim rp-candidate {vlan <vlan-id> | loopback <number> | ethernet <slot/port>} group-list <ip-address> <prefix> [bidir] [priority <priority>] [interval <interval>]
no ip pim rp-candidate {vlan <vlan-id> | loopback <number> | ethernet <slot/port>} group-list <ip-address> <prefix> [bidir] [priority <priority>] [interval <interval>]

Configures the switch as a candidate rendezvous point (C-RP).
The no form of the command removes the ip pim rp-candidate from running-config command for the specified multicast group.

Syntax Description	ethernet <slot/port>	Ethernet interface.
	port-channel <number>	LAG interface.
	vlan <vlan-id>	VLAN ID. Range: 1-4094.
	loopback <number>	Loopback interface number.
	ip-address	The group IP address.
	prefix	Network prefix (for example /24, or 255.255.255.0).
	priority	RP priority rating. Range: 0-255, where smaller numbers mean higher priority.
	interval	RP-advertisements message transmission interval. Range: 0-16383.
Default	The RP priority is 192. The BSR message interval is 60 seconds.	
Configuration Mode	Config Config Interface Ethernet configured as a router port Config Interface Loopback Config Interface Port Channel configured as a router port Config Interface VLAN	
History	3.3.5006	
Role	admin	
Example	`switch (config) # ip pim rp-candidate vlan 19 group-list 225.6.5.0 /25 priority 20 interval 30 bidir`	

Related Commands	N/A
Note	• The BSR selects a multicast group's dynamic RP set from the list of C-RPs in the PIM domain. The command specifies the interface (used to derive the RP address), C-RP advertisement interval, and priority rating. The BSR selects the RP set by comparing C-RP priority ratings. The C-RP advertisement interval specifies the period between successive C-RP advertisement message transmissions to the BSR. • Running-config supports multiple multicast groups through multiple ip pim rp-candidate statements: • All commands must specify the same interface. Issuing a command with an interface that differs from existing commands removes all existing commands from running-config. • Running-config stores the interval and priority setting in a separate statement that applies to all rp-candidate statements. When a command specifies an interval that differs from the previously configured value, the new value replaces the old value and applies to all configured rp-candidate statements. The default interval value is 60 seconds. • When the no commands do not specify a multicast group, all rp-candidate statements are removed from running-config. The no ip pim rp-candidate interval commands restore the interval setting to the default value of 60 seconds. • When setting a priority, all previous rp-candidates within all interfaces and groups are configured to this priority.

ip pim sparse-mode

	ip pim sparse-mode **no ip pim sparse-mode** Sets PIM sparse mode on this interface. The no form of the command disables the sparse-mode on the interface and deletes all interfaces configuration.
Syntax Description	N/A
Default	Disabled
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port
History	3.3.5006
Role	admin
Example	`switch (config interface vlan 10) # ip pim sparse-mode`
Related Commands	N/A
Note	

ip pim dr-priority

ip pim dr-priority <priority>
no ip pim dr-priority

Configures the designated router (DR) priority of PIM Hello messages.
The no form of the command resets this parameter to its default.

Syntax Description	priority	The designated router priority of the PIM Hello messages. Range is 1-4294967295.
Default	1	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.5006	
Role	admin	
Example	`switch (config interface vlan 10) # ip pim dr-priority 5`	
Related Commands	ip pim sparse-mode	
Note	The command “ip pim sparse-mode” must be run prior to using this command.	

ip pim hello-interval

ip pim hello-interval <interval>
no ip pim hello-interval

Configures PIM Hello interval in milliseconds.
The no form of the command resets this parameter to its default.

Syntax Description	interval	PIM Hello interval in milliseconds. Range:1000-65535000.
Default	30,000 milliseconds	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.5006	
Role	admin	
Example	`switch (config interface vlan 10) # ip pim hello-interval 70000`	
Related Commands	ip pim sparse-mode	
Note	The command “ip pim sparse-mode” must be run prior to using this command.	

ip pim join-prune-interval

ip pim join-prune-interval <period>
no ip pim join-prune-interval

Configures the period between Join/Prune messages that the configuration mode interface originates and sends to the upstream RPF neighbor.
The no form of the command resets this parameter to its default.

Syntax Description	period	Range: 1-1000000 seconds.
Default	60 seconds	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.5200	
Role	admin	
Example	`switch (config interface vlan 10) # ip pim join-prune-interval 60`	
Related Commands		
Note		

ip pim border

ip pim border
no ip pim border

Configures an interface on an IPv4 PIM border.
The no form of the command removes the interface from being a PIM border.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port
History	3.3.5006
Role	admin
Example	`switch (config interface vlan 10) # ip pim border`
Related Commands	
Note	PIM border blocks PIM control traffic, but sends and receives all multicast traffic.

ip pim bsr-border

	ip pim bsr-border **no ip pim bsr-border** Prevents the switch from sending bootstrap router messages (BSMs) over the configuration mode interface. The no form of the command resets the parameter to its default value.
Syntax Description	N/A
Default	no pim bsr-border
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port
History	3.3.5200
Role	admin
Example	`switch (config interface vlan 10) # ip pim bsr-border`
Related Commands	
Note	

debug ethernet ip pim

debug ethernet ip pim {all | control-plane | data-path | fail-all | init-shut | management | memory | packet-dump | resources}
no debug ethernet ip pim {all | control-plane | data-path | fail-all | init-shut | management | memory | packet-dump | resources}

Configures the trace level for PIM.
The no form of the command removes the trace level for PIM.

Syntax Description	all	Enable track traces.
	control-plane	Control plane traces.
	data-path	IP packet dump trace.
	fail-all	All failures including Packet Validation Trace.
	init-shut	Init and shutdown messages.
	management	Management messages.
	memory	Memory related messages.
	packet-dump	Packet dump messages.
	resources	OS Resource trace.
Default	N/A	
Configuration Mode	Config	
History	3.3.5200	
Role	admin	
Example	`switch (config)# debug ethernet ip pim all`	
Related Commands		
Note		

show ip pim protocol

show ip pim protocol

Displays PIM protocol information (counters).

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.5200
Role	admin

Example	`switch (config) # show ip pim protocol`
	`PIM Control Counters`
	`                    Received     Sent         Invalid`
	`Assert              0            0            0`
	`Bootstrap Router     0            0            0`
	`CRP Advertisement    0            0            0`
	`Graft               0            0            0`
	`Grapt Ack            0            0            0`
	`Hello               0            0            0`
	`J/P                 0            0            0`
	`Register            0            0            0`
	`Register Stop        0            0            0`
	`State Refresh       0            0            0`
	`switch (config) #`

Related Commands	
Note	

show ip pim bsr

show ip pim bsr

Displays PIM BSR information.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.5006
Role	admin

Example	`arc-switch14 [standalone: master] (config) # show ip pim bsr`
	`PIMv2 Bootstrap information`
	`  BSR address: 4.4.4.14`
	`  Uptime:      00:00:30, BSR Priority: 0, Hash mask length: 30`
	`  Expires:     00:00:57`
	`This system is a candidate BSR`
	`  Candidate BSR address: 4.4.4.14, priority: 0, hash mask length: 30`
	`             interval: 60, holdtime: 130`

Related Commands	
Note	

show ip pim neighbor

show ip pim neighbor [vlan <vlan-id> | <other interfaces> | <ip-addr>]

Displays information about IPv4 PIM neighbors.

Syntax Description	vlan <vlan-id>	Filters the output per specific VLAN ID.
	neighbor-addr	Filters the output per specific neighbor IP address.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.5006	
Role	admin	

Example	`switch (config) # show ip pim neighbor`
	`PIM Neighbor Status for VRF "default"`
	`Neighbor Interface Uptime Expires Ver DR Prio Mode`
	`5.5.5.1 VLAN5 10:36:45 00:01:43 1`
	`9.9.9.1 VLAN9 10:36:42 00:01:43 1`
	`switch (config) #`	

Related Commands		
Note		

show ip pim rp

show ip pim rp <rp-address>

Displays information about the rendezvous points (RPs) for PIM.

Syntax Description	rp-address	A rendezvous points address.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.5006	
Role	admin	

Example	`switch(config)# show ip pim rp`
	`PIM RP Status Information for VRF "default"`
	`BSR: 10.10.10.10, expires: 00:01:16,`
	`priority: 255, hash-length: 0`
	`RP: 11.11.11.11, expires: 00:01:36`
	`priority: 0, RP-source: 10.10.10.10, group ranges:`
	`225.10.0.0/24`
	`RP: 8.8.8.2, expires: 00:01:36`
	`priority: 0, RP-source: 10.10.10.10, group ranges:`
	`225.12.0.0/24`
	`switch(config)#`	

Related Commands		
Note		

show ip pim rp-hash

show ip pim rp-hash <group>

Displays the hashed value of the group (RP address according the group address).

Syntax Description	group	Filters the output per a specific IP Multicast group address.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.5006	
Role	admin	

Example	`switch (config) # show ip pim rp-hash 225.7.6.2`
	`RP 20.20.20.49, v2`
	`Info Source: 20.20.20.49, via bootstrap, priority 60, holdtime 57`
	`Expires: 00:00:53`
	`PIMv2 Hash Value (mask 255.255.255.252)`
	`switch (config)#`	

Related Commands		
Note		

show ip pim rp-candidate

show ip pim rp-candidate

Displays information about RP candidate status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.5006
Role	admin

Example	`switch (config)# show ip pim rp-candidate`
	
	`Next Candidate-RP-Advertisement in 00:11:22/00:60:00`
	`RP: 10.10.10.10`
	`group prefixes priority`
	`224.0.0.0/4  190`
	`225.0.0.0/4  191`
	`switch (config)#`

Related Commands	
Note	

show ip pim interface

show ip pim interface {[vlan <vlan id> | ethernet <port>] [df] | brief}

Displays information about the enabled interfaces for PIM.

Syntax Description	vlan <vlan-id>	Filters the output for specific interface.
	ethernet <port>	Ethernet interface.
	df	Displays information about elected designated forwarders.
	brief	Displays a summary of information for all interfaces.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.5006	
Role	admin	
Example		

```
# arc-switch55 [standalone: master] (config) # show ip pim interface
vlan 2919
Interface Vlan2919 address is 70.28.23.80
PIM: enabled
PIM version: 2, mode: sparse
PIM DR: 70.28.23.80 (this system)
PIM DR Priority: 1
PIM configured DR priority:
PIM neighbor count: 1
PIM neighbor holdtime: 105 secs
PIM Hello Interval: 30 seconds, next hello sent in: 00:00:28
PIM Hello Generation ID: 61345
PIM Join-Prune Interval: 60 seconds
PIM domain border: no
PIM Interface Statistics:
        General (sent/received):
                Hellos: 36/37, JPs: 0/0, Asserts: 0/0
                Grafts: 0/0, Graft-Acks: 0/0
                DF-Offers: 0/0, DF-Winners: 0/0, DF-Backoffs: 0/0, DF-
Passes: 0/0
        Errors:
               Checksum errors: 0, Invalid packet types/DF subtypes: 0/0
                Authentication failed: 0
                Packets from non-neighbors: 1
                JPs received on RPF-interface: 0
                (*,G) Joins received with no/wrong RP: 0/0
                (*,G)/(S,G) JPs received for SSM/Bidir groups: 0/0
```

Related Commands	
Note	

show ip pim upstream joins

show ip pim upstream joins

Displays information about any PIM joins/prunes which are currently being sent to upstream PIM routers

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.5006
Role	admin

Example	`switch (config) # show ip pim upstream joins`
	`Neighbor address: 159.135.45.26`
	`via interface: 159.135.45.34`
	`next message in 43 seconds`
	`Group: 224.0.10.0`
	`Joins:`
	`22.74.49.25`
	`Prunes:`
	`No prunes included`
	`switch (config) #`

Related Commands	
Note	Should contain the following information: neighbor address, interface address, group range, Joins, Prunes.

6.5.5.2 Multicast

ip multicast-routing

ip multicast-routing
no ip multicast-routing

Allows the switch to forward multicast packets.
The no form of the command disables multicast routing.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.5006
Role	admin
Example	`switch (config)# ip multicast-routing`
Related Commands	N/A
Note	

ip mroute

ip mroute {<ip-addr> <ip-mask> <next-hop>} [pref]
no ip mroute {<ip-addr> <ip-mask>}

Configure multicast reverse path forwarding (RPF) static routes.
The no form of the command deletes the static multicast route.

Syntax Description	ip-addr	Unicast IP address.
	ip-mask	Network mask in a dotted format (e.g. 255.255.255.0) or /24 format.
	next-hop	Next hop IP address.
	preference	Route preference. Range: 1-255.
Default	Preference is 1	
Configuration Mode	Config	
History	3.3.5006	
Role	admin	
Example	`arc-switch14 [standalone: master] (config) # ip mroute 16.16.0.0 /16 3.3.3.1`	
Related Commands	N/A	
Note		

ip multicast ttl-threshold

ip multicast ttl-threshold <ttl-value>
no ip multicast ttl-threshold

Configures the time-to-live (TTL) threshold of packets being forwarded out of an interface.
The no form of the command removes RPF static routes.

Syntax Description	ttl-value Range: 0-225.
Default	0 – all packets are forwarded
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port
History	3.3.5006
Role	admin
Example	`switch (config interface vlan 10)# ip multicast ttl-threshold 10`
Related Commands	N/A
Note	

show ip mroute

show ip mroute [summary | <group> [<prefix> [<source>]]]

Displays information about IPv4 multicast routes.

Syntax Description	source	Source IP address.
	group	IP address of multicast group.
	prefix	Network prefix of multicast group (in the format of /24, or 255.255.255.0 for example).
	summary	Displays a summary of the multicast routes.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.2.1000	
Role	admin	

Example	`arc-switch14 [standalone: master] (config) # show ip mroute`
	`IP Multicast Routing Table`
	`Flags: B - Bidir Group, L - Local, P - Pruned, R - RP-bit set, T - SPT-bit set`
	`J - Join SPT`
	`Timers: Uptime/Expires`
	`Interface state: Interface, State/Mode`
	
	`(*, 225.0.0.0/24), 00D 00:14:49, RP 18.18.18.14, flags: BR`
	`Bidir-Upstream: Lo7`
	`Outgoing interface list:`	

Related Commands	N/A	
Note		

6.5.5.3 IGMP

ip igmp immediate-leave

ip igmp immediate-leave
no ip igmp immediate-leave

Enables the device to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group.
The no form of the command disables immediate-leave.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port
History	3.3.5006
Role	admin
Example	`switch (config interface vlan 10)# ip igmp immediate-leave`
Related Commands	N/A
Note	

ip igmp last-member-query-count

ip igmp last-member-query-count <count>
no ip igmp last-member-query-count

Configures the number of query messages the switch sends in response to a group-specific or group-source-specific leave message.
The no form of the command resets this parameter to its default.

Syntax Description	Count Range:1-7.
Default	2
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port
History	3.3.5006
Role	admin
Example	`switch (config interface vlan 10)# ip igmp last-member-query-count 7`
Related Commands	N/A
Note	This parameter reflects expected packet loss on a congested network.

ip igmp last-member-query-response-time

ip igmp last-member-query-response-time <interval>
no ip igmp last-member-query-response-time

Configures the IGMP last member query response time in seconds.
The no form of the command resets this parameter to its default.

Syntax Description	interval	IGMP last member query response time. Range:1-25 seconds.
Default	1	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.5006	
Role	admin	
Example	`switch (config interface vlan 10)# ip igmp last-member-query-response-time 10`	
Related Commands	N/A	
Note		

ip igmp startup-query-count

ip igmp startup-query-count <count>
no ip startup-query-count

Configures the number of query messages an interface sends during startup. The no form of the command resets this parameter to its default.

Syntax Description	count	Range: 1-65535.
Default	2	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.5006	
Role	admin	
Example	`switch (config interface vlan 10)# ip igmp startup-query-count 10`	
Related Commands	N/A	
Note		

ip igmp startup-query-interval

ip igmp startup-query-interval <interval>
no ip startup-query-interval

Configures the IGMP startup query interval in seconds.
The no form of the command resets this parameter to its default.

Syntax Description	interval	Range: 1-1800 seconds.
Default	30	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.5006	
Role	admin	
Example	`switch (config interface vlan 10)# ip igmp startup-query-interval 10`	
Related Commands	N/A	
Note		

ip igmp query-interval

ip igmp query-interval <interval>
no ip igmp query-interval

Configures the IGMP query interval in seconds.
The no form of the command resets this parameter to its default.

Syntax Description	interval	The IGMP query interval. Range: 1-1800 seconds.
Default	125	
Configuration Mode	Config Interface VLAN	
History	3.3.5006	
Role	admin	
Example	`switch (config interface vlan 10)# ip igmp query-interval 60`	
Related Commands	N/A	
Note		

ip igmp query-max-response-time

ip igmp query-max-response-time <time>
no ip igmp query-max-response-time

Configures the IGMP max response time in seconds.
The no form of the command resets this parameter to its default.

Syntax Description	time	The IGMP max response time. Range: 1-25 seconds.
Default	10	
Configuration Mode	Config Interface VLAN	
History	3.3.5006	
Role	admin	
Example	`switch (config interface vlan 10)# ip igmp query-max-response-time 20`	
Related Commands	N/A	
Note		

ip igmp robustness-variable

ip igmp robustness-variable <count>
no ip igmp robustness-variable

Configures the IGMP robustness variable.
The no form of the command resets this parameter to its default.

Syntax Description	count	IGMP robustness variable. Range: 1-7.
Default	2	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.5006	
Role	admin	
Example	`switch (config interface vlan 10)# ip igmp robustness-variable 4`	
Related Commands	N/A	
Note	• The robustness variable can be increased to increase the number of times that packets are resent. • This parameter reflects expected packet loss on a congested network.	

ip igmp static-oif

ip igmp static-oif <group>
no ip igmp static-oif

Statically binds an IP interface to a multicast group.
The no form of the command deletes the static multicast address from the interface.

Syntax Description	group	Multicast IP address.
Default	no ip igmp static-oif	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.5006	
Role	admin	
Example	`switch (config interface vlan 10)# ip igmp static-oif 10.10.10.5`	
Related Commands	N/A	
Note	PIM must be enabled in order to configure the route in the hardware.	

clear ip igmp groups

clear ip igmp groups {all | <group-address> <mask>}

Clears IGMP group information.

Syntax Description	all	Clears all IGMP groups.
	group-address	Clears a specific group.
Default	no ip igmp static-oif	
Configuration Mode	Config	
History	3.3.5200	
Role	admin	
Example	`switch (config)# clear ip igmp groups all` `switch (config)#`	
Related Commands	N/A	
Note		

debug ethernet ip igmp-l3

debug ethernet ip igmp-l3 {all | control-plane | data-path | fail-all | init-shut | management | memory | packet-dump | resources}
no debug ethernet ip igmp-l3 {all | control-plane | data-path | fail-all | init-shut | management | memory | packet-dump | resources}

Configures the trace level for IGMP.
The no form of the command removes the trace level for IGMP.

Syntax Description	all	Enable track traces.
	control-plane	Control plane traces.
	data-path	IP packet dump trace.
	fail-all	All failures including Packet Validation Trace.
	init-shut	Init and shutdown messages.
	management	Management messages.
	memory	Memory related messages.
	packet-dump	Packet dump messages.
	resources	OS Resource trace.
Default	N/A	
Configuration Mode	Config	
History	3.3.5200	
Role	admin	
Example	`switch (config)# debug ethernet ip igmp-l3 all`	
Related Commands		
Note		

show ip igmp groups

show ip igmp groups [<group>] [vlan <vlan-id>]

Displays information about IGMP-attached group membership.

Syntax Description	group	Filters the output to a specific IP multicast group address.
	vlan <vlan-id>	Filters the output to a specific VLAN ID.
Default	N/A	
Configuration Mode	Any Command Mode	
History		
Role	admin	

Example	`switch (config)# show ip igmp groups`
	`IGMP Connected Group Membership for VRF "default"`
	`Type: S - Static, D - Dynamic, L - Local, T - SSM Translated`
	
	`Group Address Type Interface Uptime Expires Last Reporter`
	`225.7.6.0 S vlan19 [0d 00:12:12.14] [0d 00:00:00.00] 0.0.0.0`
	`225.7.10.1 D vlan19 [0d 00:00:01.18] [0d 00:04:08.81] 19.19.19.1`
	`225.7.7.7 S vlan19 [0d 00:12:12.15] [0d 00:00:00.00] 0.0.0.0`
	`225.7.7.7 S vlan21 [0d 00:12:12.15] [0d 00:00:00.00] 0.0.0.0`	

Related Commands	N/A	
Note		

show ip igmp interface

show ip igmp interface [vlan <vlan-id> | brief]

Displays IGMP brief configuration and status.

Syntax Description	brief	Displays brief output information.
	vlan <vlan-id>	Filters the output to a specific VLAN ID.
Default	N/A	
Configuration Mode	Any Command Mode	
History		
Role	admin	

Example

```
switch(config)#show ip igmp interface
IGMP Interfaces for VRF "default"

VLAN5
Interface status: protocol-down/admin-up/link-down
IP address: 5.5.5.49, IP Subnet: 5.5.5.0/24
Active Querier: 5.5.5.48
Membership count: 0
Route-queue depth: 0
IGMP Version: 2
IGMP query interval: 125 secs, configured value: 125 secs
IGMP max response time: 100 secs, configured value: 100 secs
IGMP startup query interval: 125 secs, configured value: 125 secs
IGMP startup query count: 2
IGMP group timeout: 350 secs, configured value: 350 secs
IGMP querier timeout: 350 secs configured value: 350 secs
IGMP last member mrt: 10 secs configured value: 10
IGMP robustness variable: 2
IGMP interface immediate leave: Disabled
IGMP interface statistics:
General (sent/received):
v1/v2-reports: 0/0
v2-queries: 3/1,v2-leaves: 0/0
v3-queries: 0/0,
v3-reports: 0/0

VLAN19
Interface status: protocol-up/admin-up/link-up
IP address: 19.19.19.49, IP Subnet: 19.19.19.0/24
Active Querier: 19.19.19.49
Membership count: 3
Route-queue depth: 0
IGMP Version: 2
IGMP query interval: 125 secs, configured value: 125 secs
IGMP max response time: 10 secs, configured value: 10 secs
IGMP startup query interval: 125 secs, configured value: 125 secs
IGMP startup query count: 2
IGMP group timeout: 260 secs, configured value: 260 secs
IGMP querier timeout: 260 secs configured value: 260 secs
IGMP last member mrt: 1 secs configured value: 1
IGMP robustness variable: 2
IGMP interface immediate leave: Disabled
IGMP interface statistics:
General (sent/received):
v1/v2-reports: 0/5
v2-queries: 14/0,v2-leaves: 0/1
v3-queries: 0/0,
v3-reports: 0/0
```

Related Commands N/A

Note

6.6 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides for automatic assignment of available IP routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork.

The protocol achieves this by creating virtual routers, which are an abstract representation of multiple routers (that is, a master and backup routers, acting as a group). The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the master router.

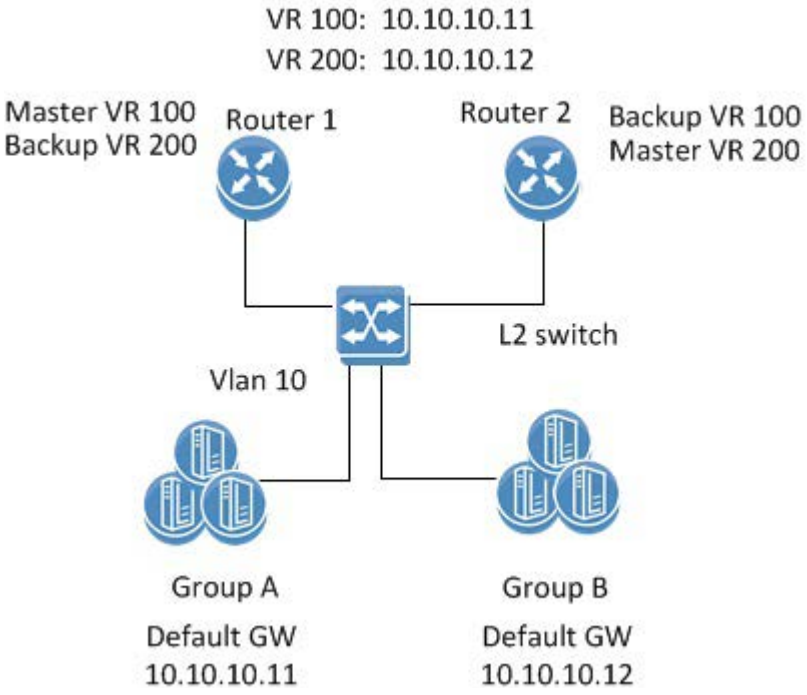
VRRP provides information on the state of a router, not the routes processed and exchanged by that router. Each VRRP instance is limited, in scope, to a single subnet. It does not advertise IP routes beyond that subnet or affect the routing table in any way.

Routers have a priority of between 1-255 and the router with the highest priority becomes the master. The configurable priority value ranges from 1-254, the router which owns the interface IP address as one of its associated IP addresses has the priority value 255. When a planned withdrawal of a master router is to take place, its priority can be lowered, which means a backup router will preempt the master router status rather than having to wait for the hold time to expire.

6.6.1 Load Balancing

To create load balancing between routers participating in the same VR, it is recommended to create 2 (or more) VRs. Each router will be a master in one of the VRs, and a backup to the other VR(s). A group of hosts should be configured with Router 1's virtual address as the default gateway, while the second group should be configured with Router 2's virtual address.

Figure 26: Common VRRP Configuration with Load Balancing



6.6.2 Configuring VRRP

➢ ***To configure VRRP:***

Precondition steps:

Step 1. Enable IP routing functionality. Run:

```
switch (config)# ip routing
```

Step 2. Enable the desired VLAN. Run:

```
switch (config)# vlan 20
```

The VLAN cannot be the same one configured for the MLAG IPL, if MLAG is used.

Step 3. Add this VLAN to the desired interface. Run:

```
switch (config)# interface ethernet 1/1
switch (config ethernet 1/1)# switchport access vlan 20
```

Step 4. Create a VLAN interface. Run:

```
switch (config)# interface vlan 20
```

Step 5. Apply IP address to the VLAN interface.

On one of the switches, run:

```
switch (config interface vlan 20)# ip address 20.20.20.20 /24
```

On the other switch, run:

```
switch (config interface vlan 20)# ip address 20.20.20.30 /24
```

Step 6. Enable the interface. Run:

```
switch (config interface vlan 20)# no shutdown
```

Configure VRRP:

This is the same configuration on both switches

Step 1. Enable VRRP protocol globally. Run:

```
switch (config)# protocol vrrp
```

Step 2. Create a virtual router group for an IP interface. Up to 255 VRRP IDs are supported. Run:

```
switch (config interface vlan 20)# vrrp 100
```

Step 3. Set the VIP address. Run:

```
switch (config interface vlan 20 vrrp 100)# address 20.20.20.40
```

Step 4. Influence the election of the master in the VR cluster make sure that the priority of the desired master is the highest. Note that the higher IP address is selected in case the priority of the routers in the VR are the same. Select the priority. Run:

```
switch (config interface vlan 20 vrrp 100)# priority 200
```

Step 5. The advertizement interval should be the same for all the routers within the VR. Modify the interval. Run:

```
switch (config interface vlan 20 vrrp 100)# advertisement-interval 2
```

Step 6. The authentication text should be the same for all the routers within the VR. Configure the authentication text. Run:

```
switch (config interface vlan 20 vrrp 100)# authentication text my-password
```

Step 7. Use the `preempt` command to enable a high-priority backup virtual router to preempt the low-priority master virtual router. Run:

```
switch (config interface vlan 20 vrrp 100)# preempt
```

Step 8. Disable VRRP. Run:

```
switch (config interface vlan 20 vrrp 100)# shutdown
```

The configuration will not be deleted, only the VRRP state machine will be stopped.

6.6.3 Verifying VRRP

Step 1. Display VRRP brief status. Run:

```
switch(config)# show vrrp
Interface   VR  Pri  Time   Pre   State VR   IP addr
-----------------------------------------------------
Vlan20      1   200  2s     Y     Init       20.20.20.20
…
switch(config)#
```

Step 2. Display VRRP detailed status. Run:

```
switch (config)# show vrrp detail

VRRP Admin State : Enabled

Vlan20 - Group 1 (IPV4)

Instance Admin State : Enabled
State : Backup
Virtual IP Address : 20.20.20.40
Priority : 200
Advertisement interval (sec) : 2
Preemption : Enabled
Virtual MAC address : AA:BB:CC:DD:EE:FF
switch (config)#
```

Step 3. Display VRRP statistic counters. Run:

```
switch (config)# show vrrp statistics
Ethernet1/5 - Group 1 (IPV4)
Invalid packets:               0
Too short:                     0
Transitions to Master          6
Total received:                155
Bad TTL:                       0
Failed authentication:         0
Unknown authentication:        0
Conflicting authentication:    0
Conflicting Advertise time:    0
Conflicting Addresses:         0
Received with zero priority:   3
Sent with zero priority:       3
switch (config)#
```

6.6.4 Commands

protocol vrrp

protocol vrrp
no protocol vrrp

Enables VRRP globally and unhides VRRP related commands.
The no form of the command deletes all the VRRP configuration and hides VRRP related commands.

Syntax Description	N/A
Default	no feature vrrp
Configuration Mode	Config
History	3.3.4500
Role	admin
Example	`switch (config)# protocol vrrp`
Related Commands	
Note	

vrrp

vrrp <number>
no vrrp <number>

Creates a virtual router group on this interface and enters a new configuration mode. The no form of the command deletes the VRRP instance and the related configuration.

Syntax Description	number	A VRRP instance number. Range is 1-255.
Default	N/A	
Configuration Mode	Config Interface VLAN	
History	3.3.4500	
Role	admin	
Example	`switch (config interface vlan 10)#` `switch (config interface vlan 10 vrrp 10)#`	
Related Commands		
Note	Maximum of 10 VRRP instances are supported.	

address

address <ip-address> [secondary]
no address [<ip-address> [secondary]]

Sets virtual router IP address (primary and secondary).
The no form of the command deletes the IP address from the VRRP interface.

Syntax Description	ip-address	The virtual IP address.
	secondary	A secondary IP address for the virtual router.
Default	N/A	
Configuration Mode	Config VRRP Interface	
History	3.3.4500	
Role	admin	

Example	`switch (config vrrp 100)# address 10.10.10.10`
	`switch (config vrrp 100)# address 10.10.10.11 secondary`
	`switch (config vrrp 100)# address 10.10.10.12 secondary`	

Related Commands		
Note	• This command is the enabler of the protocol. Therefore, set all the protocol parameters initially and only then set the ip-address. • There are up to 10 IP addresses associated with the VRRP instance. One primary and up to 10 secondary ip-addresses. • If the configured IP address is the same as the interface IP address, this switch automatically owns the IP address (priority 255).	

shutdown

	shutdown **no shutdown** Disables the virtual router. The no form of the command enables the virtual router (stops the VRRP state machine).
Syntax Description	N/A
Default	Enabled (no shutdown)
Configuration Mode	Config VRRP Interface
History	3.3.4500
Role	admin
Example	`switch (config vrrp 100)# shutdown`
Related Commands	
Note	

priority

priority <level>
no priority

Sets the priority of the virtual router.
The no form of the command resets the priority to its default.

Syntax Description	level	The virtual router priority level. Range is 1-254.
Default	100	
Configuration Mode	Config VRRP Interface	
History	3.3.4500	
Role	admin	
Example	`switch (config vrrp 100)# priority 200`	
Related Commands		
Note	• The higher IP address will be selected as master, in case the priority of the routers in the VR are the same. • To influence the election of the master in the VR cluster make sure that the priority of the desired master is the higher.	

preempt

	preempt **no preempt** Sets virtual router preemption mode. The no form of the command disables the virtual router preemption.
Syntax Description	N/A
Default	Enabled (preempt)
Configuration Mode	Config VRRP Interface
History	3.3.4500
Role	admin
Example	`switch (config vrrp 100)# preempt`
Related Commands	
Note	To set this router as backup for the current virtual router master, preempt must be enabled.

authentication text

authentication text <password>
no authentication text

Sets virtual router authentication password and enables authentication.
The no form of the command disables the authentication mechanism.

Syntax Description	password	The virtual router authentication password. The password string must be up to 8 alphanumeric characters.
Default	Disabled	
Configuration Mode	Config VRRP Interface	
History	3.3.4500	
Role	admin	
Example	`switch (config vrrp 100)# authentication text mypassword`	
Related Commands		
Note		

advertisement-interval

advertisement-interval <seconds>
no advertisement-interval

Sets the virtual router advertisement-interval.
The no form of the command resets the parameter to its default.

Syntax Description	seconds	The virtual router advertisement-interval in seconds. Range: 1-255.
Default	1	
Configuration Mode	Config VRRP Interface	
History	3.3.4500	
Role	admin	
Example	`switch (config vrrp 100)# advertisement-interval 10`	
Related Commands		
Note		

show vrrp

show vrrp [interface <type> <number>] [vr <id>]

Displays VRRP brief configuration and status.

Syntax Description	interface <type> <number>	Filters the output to a specific interface type and number.
	vr <id>	Filters the output to a specific virtual router. Range: 1-10.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4500	
Role	admin	

Example	`switch(config)# show vrrp`
	`Interface  VR Pri Time  Pre  State VR  IP addr`
	`---------------------------------------------------`
	`Eth1/5     1  200  2s   Y    Init      192.0.1.10`
	…
	`switch(config)#`	

Related Commands		
Note		

show vrrp detail

show vrrp detail [interface <type> <number>] [vr <id>]

Displays detailed VRRP configuration and status.

Syntax Description	interface <type> <number>	Filters the output to a specific interface type and number.
	vr <id>	Filters the output to a specific virtual router. Range: 1-255.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4500	
Role	admin	

Example	`switch (config)# show vrrp detail`
	
	`VRRP Admin State : Enabled`
	
	`Vlan20 - Group 1 (IPV4)`
	
	`Instance Admin State : Enabled`
	`State : Backup`
	`Virtual IP Address : 20.20.20.40`
	`Priority : 200`
	`Advertisement interval (sec) : 2`
	`Preemption : Enabled`
	`Virtual MAC address : AA:BB:CC:DD:EE:FF`
	`switch (config)#`	

Related Commands		
Note		

show vrrp statistics

show vrrp statistics [interface <type <number>] [vr <id>]

Displays VRRP counters.

Syntax Description	interface <type> <number>	Filters the output to a specific interface type and number.
	vr <id>	Filters the output to a specific virtual router. Range: 1-255.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4500	
Role	admin	

Example	`switch (config)# show vrrp statistics`
	`Ethernet1/5 - Group 1 (IPV4)`
	`Invalid packets: 0`
	`Too short: 0`
	`Transitions to Master 6`
	`Total received: 155`
	`Bad TTL: 0`
	`Failed authentication: 0`
	`Unknown authentication: 0`
	`Conflicting authentication: 0`
	`Conflicting Advertise time: 0`
	`Conflicting Addresses: 0`
	`Received with zero priority: 3`
	`Sent with zero priority: 3`
	`switch (config)#`	

Related Commands		
Note		

6.7 MAGP

Multi-active gateway protocol (MAGP) is aimed to solve the default gateway problem when a host is connected to a set of switch routers (SRs) via MLAG.

The network functionality in that case requires that each SR is an active default gateway router to the host, thus reducing hops between the SRs and directly forwarding IP traffic to the L3 cloud regardless which SR traffic comes through.

Designated traffic, such as ping to the MAGP interface is not supported. One of the two switches will be able to ping, so a ping from one switch can be done.

6.7.1 MAGP Configuration

Prerequisite steps:

Step 1. Enable IP routing functionality. Run:

```
switch (config)# ip routing
```

Step 2. Enable the desired VLAN. Run:

```
switch (config)# vlan 20
switch (config vlan 20)#
```

The VLAN cannot be the same one configured for the MLAG IPL, if MLAG is used.

Step 3. Add this VLAN to the desired interface. Run:

```
switch (config)# interface ethernet 1/1
switch (config interface ethernet 1/1)# switchport access vlan 20
```

Step 4. Create a VLAN interface. Run:

```
switch (config)# interface vlan 20
switch (config interface vlan 20)#
```

Step 5. Set an IP address to the VLAN interface. Run:

```
switch (config interface vlan 20)# ip address 20.20.20.20 /24
```

Step 6. Enable the interface. Run:

```
switch (config interface vlan 20)# no shutdown
```

Configuring MAGP:

Step 1. Enable MAGP protocol globally. Run:

```
switch (config)# protocol magp
```

Step 2. Create a virtual router group for an IP interface. Up to 255 MAGP IDs are supported. Run:

```
switch (config interface vlan 20)# magp 100
```

Step 3. Set a virtual router primary IP address. Run:

```
switch (config interface vlan 20 magp 100)# ip virtual-router address 11.11.11.254
```

Step 4. Set a virtual router primary MAC address. Run:

```
switch (config interface vlan 20 magp 100)# ip virtual-router mac-address
AA:BB:CC:DD:EE:FF
```

The IP address must be the IP address of the interface. This IP address is the default gateway for this MAGP instance. This becomes the default gateway configured on the hosts connected to the relevant MLAG.

- ***To verify the MAGP configuration, run:***

```
switch (config)# show magp 1
MAGP 1
  Interface vlan:1
  MAGP state:Master
  MAGP virtual IP: 11.11.11.254
  MAGP virtual MAC: AA:BB:CC:DD:EE:FF
switch (config)#
```

This output is to be expected in both MAGP switches.

6.7.2 Commands

protocol magp

protocol magp
no protocol magp

Enables MAGP globally and unhides MAGP commands.
The no form of the command deletes all the MAGP configuration and hides MAGP commands.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.4500
Role	admin
Example	`switch (config)# protocol magp` `switch (config)#`
Related Commands	
Note	IP routing must be enabled to enable MAGP.

magp

magp <instance>
no magp <instance>

Creates an MAGP instance on this interface and enters a new configuration mode. The no form of the command deletes the MAGP instance.

Syntax Description	instance	MAGP instance number. Range: 1-255.
Default	Disabled	
Configuration Mode	Config Interface VLAN	
History	3.3.4500	
Role	admin	
Example	`switch (config interface vlan 10)# magp 1` `switch (config interface vlan 10 magp 1)#`	
Related Commands		
Note	• Only one MAGP instance can be created on an interface • Different interfaces cannot share an MAGP instance • MAGP and VRRP are mutually exclusive	

shutdown

	shutdown **no shutdown** Enables MAGP instance. The no form of the command disables the MAGP instance.
Syntax Description	N/A
Default	Disabled
Configuration Mode	Config Interface VLAN MAGP
History	3.3.4500
Role	admin
Example	`switch (config interface vlan 10 magp 1)# protocol magp` `switch (config interface vlan 10 magp 1)#`
Related Commands	
Note	

ip virtual-router address

ip virtual-router address <ip-address>
no ip virtual-router address

Sets MAGP virtual IP address.
The no form of the command resets this parameter to its default.

Syntax Description	ip-address	The virtual router IP address.
Default	N/A	
Configuration Mode	Config Interface VLAN MAGP	
History	3.3.4500	
Role	admin	
Example	`switch (config interface vlan 10 magp 1)# ip virtual-router address 10.10.10.10` `switch (config interface vlan 10 magp 1)#`	
Related Commands		
Note	The MAGP virtual IP address must be different from the interface IP address	

ip virtual-router mac-address

ip virtual-router mac-address <mac-address>
no ip virtual-router mac-address

Sets MAGP virtual MAC address.
The no form of the command resets the MAC address to its default.

Syntax Description	mac-address	MAC address. Format: AA:BB:CC:DD:EE:FF.
Default	00:00:5E:00:01-<magp instance>	
Configuration Mode	Config Interface VLAN MAGP	
History	3.3.4500	
Role	admin	
Example	`switch (config interface vlan 10 magp 1)# ip virtual-router mac-address AA:BB:CC:DD:EE:FF` `switch (config interface vlan 10 magp 1)#`	
Related Commands		
Note		

show magp

show magp [<instance> | interface vlan <id>]

Displays the configuration of a specific MAGP instance.

Syntax Description	instance	MAGP instance number. Range: 1-255.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4500	
Role	admin	

Example	`switch (config)# show magp 3`
	`Magp instance id: 3`
	`Interface : vlan 10`
	`Magp state: Active`
	`Magp virtual ip :192.168.1.1`
	`Magp virtual MAC : 00:11:22:22:44:55`
	`switch (config)#`	

Related Commands		
Note		

6.8 DHCP Relay

Since Dynamic Host Configuration Protocol must work correctly even before DHCP clients have been configured, the DHCP server and DHCP client need to be connected to the same network.

In larger networks, this is not always practical because each network link contains one or more DHCP relay agents. These DHCP relay agents receive messages from DHCP clients and forward them to DHCP servers thus extending the reach of the DHCP beyond the local network.

6.8.1 Commands

ip dhcp relay address

ip dhcp relay address <ip-address>
no ip dhcp relay address <ip-address>

Configures IP address of the DHCP server to forward DHCP requests.
The no form of the command deletes the DHCP server IP address.

Syntax Description	ip-address	Valid IP unicast address of DHCP server.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config)# ip dhcp relay address 10.10.10.10` `switch (config)#`	
Related Commands	N/A	
Note	• Up to 16 IP addresses may be configured • To enable DHCP relay, at least one IP address should be configured, or always-on parameter should be turned on using the command “ip dhcp relay always-on”	

ip dhcp relay information option

ip dhcp relay information option
no ip dhcp relay information option

Enables the DHCP relay agent to insert option 82 info on the packets.
The no form of the command removes option 82 from the packets.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.4150
Role	admin
Example	`switch (config)# ip dhcp relay information option` `switch (config)#`
Related Commands	N/A
Note	

ip dhcp relay always-on

ip dhcp relay always-on
no ip dhcp relay always-on

Broadcasts DHCP requests to all interfaces with the DHCP relay agent.
The no form of the command disables the “always-on” mode.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.4150
Role	admin
Example	`switch (config)# ip dhcp relay always-on` `switch (config)#`
Related Commands	N/A
Note	• In order to enable DHCP relay, at least one IP address should be configured, or always-on parameter should be turned on using the command “ip dhcp relay always-on” • When DHCP servers are configured. requests are forwarded only to configured servers

clear ip dhcp relay counters

clear ip dhcp relay counters

Clears all DHCP relay counters (all interfaces).

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.4150
Role	admin
Example	`switch (config)# clear ip dhcp relay counters` `switch (config)#`
Related Commands	N/A
Note	• In order to enable DHCP relay, at least one IP address should be configured, or always-on parameter should be turned on using the command “ip dhcp relay always-on” • When DHCP servers are configured. requests are forwarded only to configured servers

6.8.1.1 Interface

ip dhcp relay information option circuit-id

ip dhcp relay information option circuit-id <label>
no ip dhcp relay information option circuit-id

Specifies the content of tags that the switch attaches to DHCP requests before they are forwarded.
The no form of the command removes the label assigned.

Syntax Description	label	Specifies the label attached to packets. The string may be up to 15 characters.
Default	The label is taken from the IP interface name (e.g. “vlan1”)	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port	
History	3.3.4150	
Role	admin	
Example	`switch (config interface vlan 10)# ip dhcp relay information options circuit-id my-label` `switch (config interface vlan 10)#`	
Related Commands	N/A	
Note		

clear ip dhcp relay counters

ip dhcp relay counters
no ip dhcp relay counters

Clears all DHCP relay counters on the interface.

Syntax Description	N/A
Default	The label is taken from the IP interface name (e.g. “vlan1”)
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port Config Interface Port Channel configured as a router port
History	3.3.4150
Role	admin
Example	`switch (config interface vlan 10)# clear ip dhcp relay counters` `switch (config interface vlan 10)#`
Related Commands	N/A
Note	

6.8.1.2 Show

show ip dhcp relay

show ip dhcp relay

Displays DHCP relay configuration and status.

Syntax Description	N/A
Default	The label is taken from the IP interface name (e.g. “vlan1”)
Configuration Mode	Any Command Mode
History	3.3.4150
Role	admin

Example	`switch (config)# show ip dhcp relay`
	`DHCP servers: 172.22.22.11, 172.33.33.33, … (or N/A)`
	`DHCP clients requests are processed on all interfaces`
	`DHCP server responses are processed on all interfaces`
	`DHCP relay agent information option is {enabled, disabled}`
	`DHCP relay agent always-on is {enabled, disabled}`
	`Interface Label`
	`--------- --------`
	`Vlan10    my-label`
	`switch (config)#`

Related Commands	N/A
Note	

show ip dhcp relay counters

show ip dhcp relay counters

Displays the DHCP relay counters.

Syntax Description	N/A
Default	The label is taken from the IP interface name (e.g. “vlan1”)
Configuration Mode	Any Command Mode
History	3.3.4150
Role	admin

Example	`switch (config)#show ip dhcp relay counters`
	
	`Interface Received Forwarded Dropped`
	`--------- -------- --------- --------`
	`All Req 376 376 0`
	`All Resp 277 277 0`
	`Interface Received Forwarded Dropped Last cleared`
	`--------- -------- --------- ------- -------------`
	`vlan1000 1000 1000 0 <Date>`
	`vlan1020 2000 2000 0 <Date>`
	`// <Date> == <DD-MM-YY, Hour-Minutes-Seconds> - something like: “20-07-13, 22:34:36”`
	`switch (config)#`

Related Commands	N/A
Note	