Connect. Accelerate. Outperform.™

Mellanox MLNX-OS® User Manual for Lenovo SX90Y3452

Rev 4.20

Software Version 3.4.3002

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 PRODUCT(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.
Hakidma 26
Ofer Industrial Park
Yokneam 2069200
Israel
www.mellanox.com
Tel: +972 (0)74 723 7200
Fax: +972 (0)4 959 3245

Table of Contents

List of Tables

List of Figures

Document Revision History

Rev 4.20 – July 30, 2015

Updated:

- Section 2.4, “Licenses,” on page 23
- the command “ssh server host-key” on page 59
- notes of the command “aaa authorization” on page 266
- the command “show module” on page 347
- the command “snmp-server user” on page 371
- Appendix B, “Security Vulnerabilities and Exposures” on page 427

Rev 4.10 – June 11, 2015

Added:

- Section 2.1, “Configuring the Switch for the First Time,” on page 19 with MLNX-OS® Boot Menu step
- the command “ssh server security strict” on page 64
- the command “ssh server tcp-forwarding enable” on page 65
- the command “show module” on page 347
- Appendix C,“UI Changes in Version 3.4.2008,” on page 443

Updated:

- the command “tcpdump” on page 138
- Section 4.4.2, “Upgrading MLNX-OS Software,” on page 153 with HA group note
- Section 4.4.3, “Upgrading MLNX-OS HA Groups,” on page 157
- the command “show inventory” on page 346
- the command “show asic-version” on page 349
- the command “show guids” on page 382
- the command “show lids” on page 384
- the command “interface ib” on page 386
- the command “speed” on page 390
-
- Section B.9, “Security Vulnerabilities and Exposures,” on page 1330 and added it to the RN

Rev 3.70 – March 19, 2015

Updated:

- the command “speed” on page 390
- the command “show interfaces ib” on page 394
- the command “show interfaces ib status” on page 395

Rev 3.70 – March 19, 2015

No changes

Rev 3.60 – March 05, 2015

Added:

- MLAG configuration Step 10
- the command "system-mac" on page 456
- the command "upgrade-timeout" on page 457
- Section 5.7.4, "BPDU Guard," on page 487

Updated:

- MLAG configuration verification Step 1 with system MAC and upgrade timeout
- the command "show mlag" on page 458
- Table 23, "Supported VLANs by RPVST per Switch System," on page 489

Rev 3.60 – March 05, 2015

No changes

Rev 3.50 – February 24, 2015

Added:

- the command "show version concise" on page 343

Updated:

- the command "show uboot" on page 344

Rev 3.40 – February 11, 2015

Added:

- "List of Tables" and "List of Figures" Sections
- Updated Section 2.4, "Licenses," on page 23
- the command "license delete" on page 30
- the command "license install" on page 31
- the command "telnet" on page 73
- the command "terminal" on page 50
- the command "web cache-enable" on page 77
- the command "ip default-gateway" on page 95
- the command "boot system" on page 166
- the command "configuration write" on page 201
- the command "logging trap" on page 222
- the command "email autosupport enable" on page 229
- the command "email autosupport event" on page 230

- the command "crypto ipsec ike" on page 294

Updated:

- Section 2.3, "Starting the Web User Interface," on page 20
- the command "image options" on page 172
- the command "reload" on page 182
- Section 4.6.2, "Remote Logging," on page 205
- the command "logging debug-files" on page 209
- Section 4.9.1, "User Accounts," on page 250
- the command "username" on page 252
- the command "aaa authentication attempts track" on page 259
- the command "radius-server host" on page 271
- the command "tacacs-server host" on page 275
- the command "snmp-server auto-refresh" on page 361
- the command "snmp-server user" on page 371

Rev 3.30 – November 19, 2014

Updated:

- the command "web https" on page 84
- Section A.6, "HTTPS," on page 423
- Section A.8, "Password Hashing," on page 426

Rev 3.20 – November 09, 2014

Added:

- Section 5.6.2, "MAC Learning Considerations," on page 479
- the command "mac-learning disable" on page 482
- Appendix A,"Enhancing System Security According to NIST SP 800-131A," on page 421

Updated:

- Section 3.2, "Web Interface Overview," on page 39
- the command "show fabric" on page 381

Rev 3.10 – July 20, 2014

Updated:

- Section 4.13.1, "XML API," on page 360

Rev 3.00 – June 05, 2014

No changes

Rev 2.90 – 19 May, 2014

Updated:

- the command "show configuration" on page 203
- the command "show uboot" on page 344
- the command "show voltage" on page 353

Rev 2.80 – May 08, 2014

Added:

- supported versions note in Section 5.9, "IGMP Snooping," on page 529

Rev 2.70 – April 30, 2014

Added:

- Appendix A,"Enhancing System Security According to NIST SP 800-131A," on page 421

Updated:

- the command "show ssh server" on page 72
- the command "web auto-logout" on page 76
- the command "web https" on page 84
- the command "show web" on page 90
- the command "show usernames" on page 254
- the command "ldap base-dn" on page 278
- the command "ldap ssl" on page 288

Rev 2.60 – April 10, 2014

N/A

Rev 2.50 – April 2014

Updated:

- Section 3.1.7, "Command Output Filtering," on page 38
- the command "show protocols" on page 359

Rev 2.40 – February, 2014

Updated:

- Section 4.4.6.2, "Importing Firmware and Changing the Default Firmware," on page 162 – updated Step 1
- the command "show running-config" on page 204
- the command "show log" on page 224
- Section 4.10, "Cryptographic (X.509, IPSec)," on page 293

Added:

- Section 3.1.7, “Command Output Filtering,” on page 38

Rev 2.30 – January, 2014

Updated:

- the command “crypto certificate generation” on page 299
- the command “crypto certificate name” on page 300

Rev 2.20 – January, 2014

N/A

Rev 2.10 – January, 2014

Added:

- Section 4.12.2.1, “Width Reduction Power Saving,” on page 333

Updated:

- Section 2.2, “Starting the Command Line (CLI),” on page 20
- Section 2.3, “Starting the Web User Interface,” on page 20
- Section 4.4.2, “Upgrading MLNX-OS Software,” on page 153 with EULA note

Rev 2.00 – December 2013

Added:

- Section 5.1.2, “Transceiver Information,” on page 403
- Section 5.3.1, “Transceiver Information,” on page 385
- a note to Section 8.4.3, “MTU,” on page 1278

Updated:

- Section 4.4.2, “Upgrading MLNX-OS Software,” on page 153
- Section 4.4.4, “Deleting Unused Images,” on page 157
- the example of the command “show cpld” on page 345
- “Notification Indicator” column in Section 8.3.2, “Standalone Proxy-ARP Configuration,” on page 1271
- the command “lldp tlv-select” on page 556

Moved:

Section 4.6.3, “Switch Power-On Self-Test,” on page 205 from 4.11.1

Section 3.3, “Secure Shell (SSH),” on page 43 from 4.13.2

Removed:

- mention of the MLNX-OS Command Reference Guide
- the command “lldp tlv-select dcbx”

Rev 1.90 – November 2013

Added Appendix A,"MEX6200 System," on page 1329

Rev 1.80 – October 2013

Added:

- Section 5.7.7, "MSTP," on page 488
- Section 5.8, "OpenFlow," on page 520
- Section 5.9.3, "IGMP Snooping Querier," on page 531
- the command "ip igmp snooping querier"
- the command "igmp snooping querier query-interval"
- the command "show ip igmp snooping querier"
- Section 5.10.2, "DCBX," on page 548
- 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 1 - 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 2 - 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).

Table 2 - Glossary

CLI	Command Line Interface. A user interface in which you type commands at the prompt
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
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
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.
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
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
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

Table 2 - Glossary

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® Family 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 SNMPv1, 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 3 - General System Features

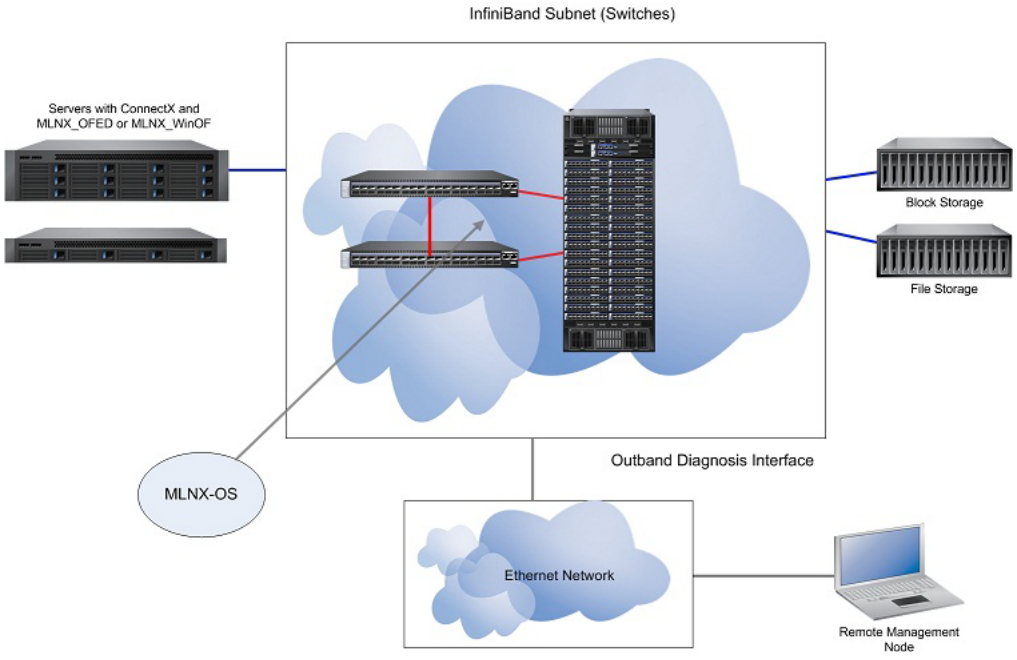
Feature	Description
Software Management	• Dual software image • Software and firmware updates
File management	• FTP • TFTP • SCP
Logging	• Event history log • SysLog support
Management Interface	• DHCP/Zeroconf • IPv6
Chassis Management	• Monitoring environmental controls
Network Management Interfaces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

1.2 Gateway Features

Table 4 - Gateway Features

Feature	Description
Proxy-ARP	• Proxy-ARP interface • Unicast • Multicast • High availability Proxy-ARP

Figure 1: Managing an InfiniBand Software Using MLNX-OS



2 Getting Started

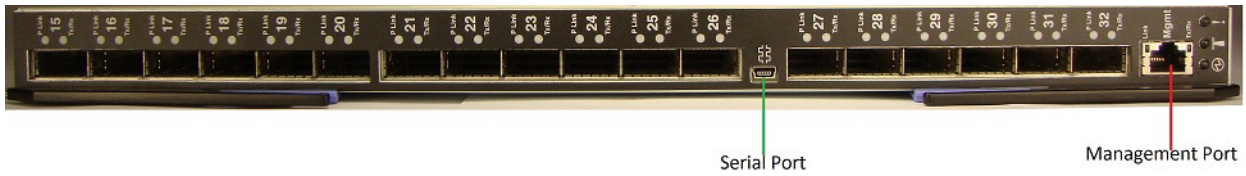
The procedures described in this chapter assume that you have already installed and powered on your switch according to the instructions in the *Hardware Installation Guide*, which was shipped with the product.

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.

This step may be skipped if the DHCP option is used and an IP is already configured for the MGT port.

Table 5 - 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. You are prompted with the boot menu.

```
Mellanox MLNX-OS Boot Menu:

   1: <image #1>
   2: <image #2>
   u: USB menu (if USB device is connected) (password required)
   c: Command prompt (password required)

   Choice:
```

Select “1” to boot with software version installed on partition #1.
Select “2” to boot with software version installed on partition #2.
Selecting “u” is not currently supported.
Select “c” to proceed to advanced booting options – available to Mellanox Support only.

The MLNX-OS Boot Menu features a countdown timer. It is recommended to allow the timer to run out by not selecting any of the options.

Step 4. Login as *admin* and use *admin* as password.

If the machine is still initializing, you might not be able to access the CLI until initialization completes. As an indication that initialization is ongoing, a countdown of the number of remaining modules to be configured is displayed in the following format: “<no. of modules> Modules are being configured”.

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.

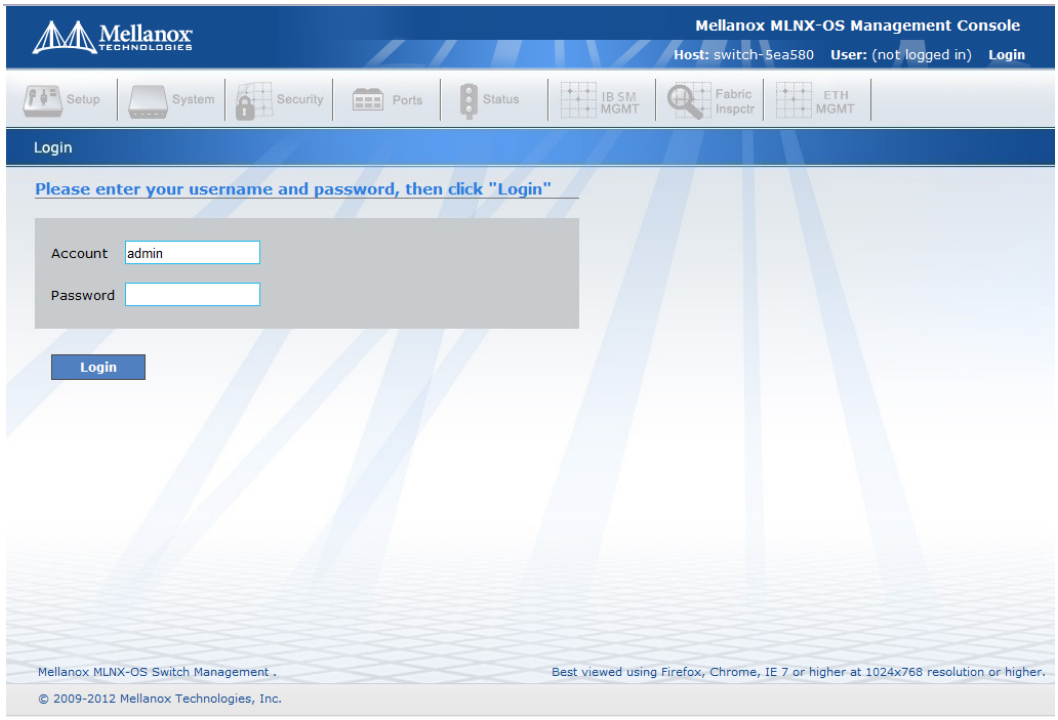
Step 2. Open a web browser – Firefox 12, Chrome 18, IE 8, Safari 5 or higher.

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>.

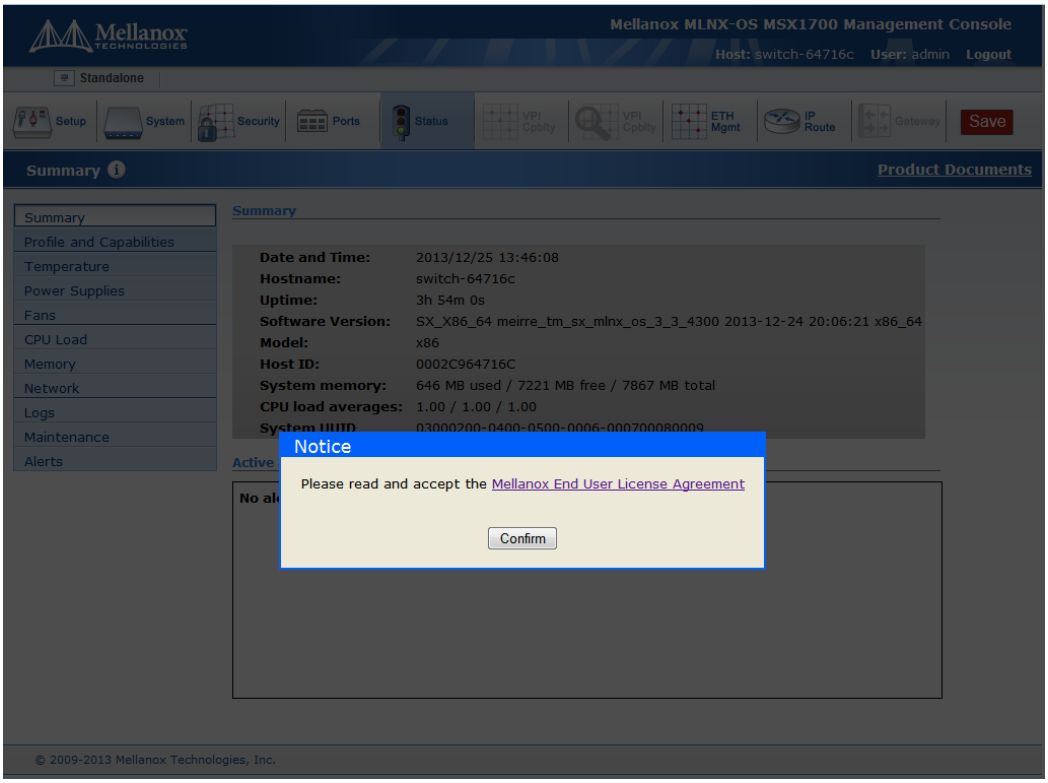
Step 4. Login to the switch (default user name is *admin*, password *admin*).

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



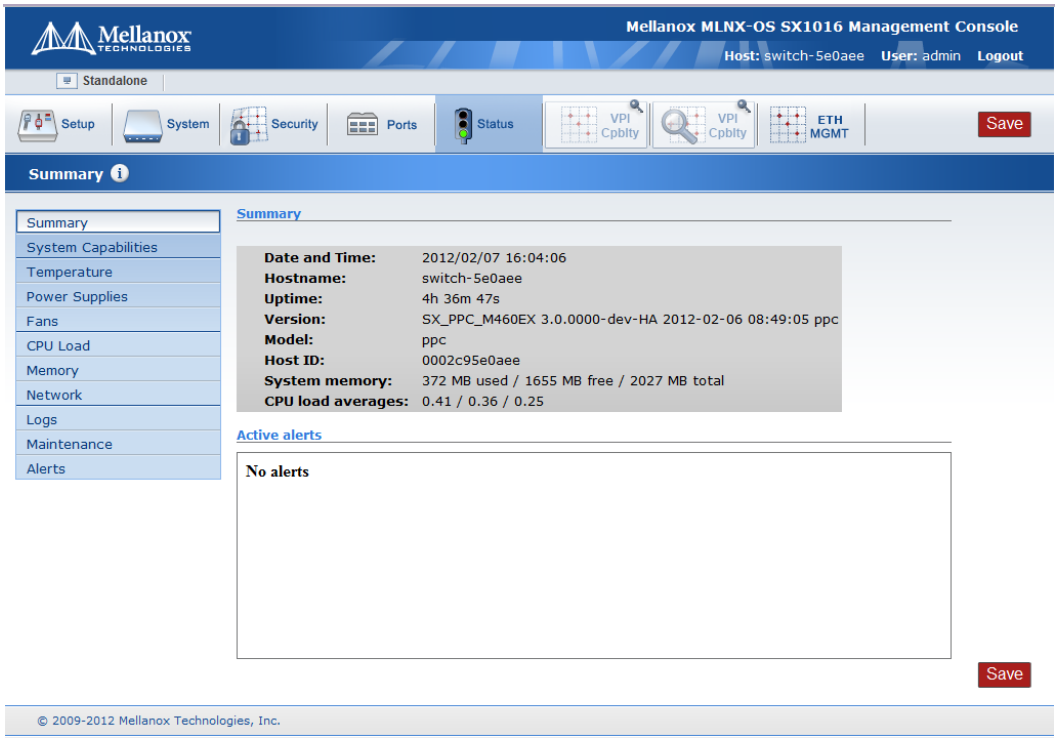
Step 6. The Welcome popup appears. After reading through the content, click OK to continue.
You may click on the links under Documentation to reach the MLNX-OS documentation.
The link under What's New takes you straight to the RN Changes and New Features section.

Figure 5: Welcome Popup

You may also tick the box to not show this popup again. But should you wish to see this window again, click “Product Documents” on the upper right corner of the WebUI.

Step 7. A default status summary is displayed as shown in Figure 6.

Figure 6: Display After Login



2.4 Licenses

Gateway is not supported in MLNX-OS® release 3.4.1110.

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.

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.

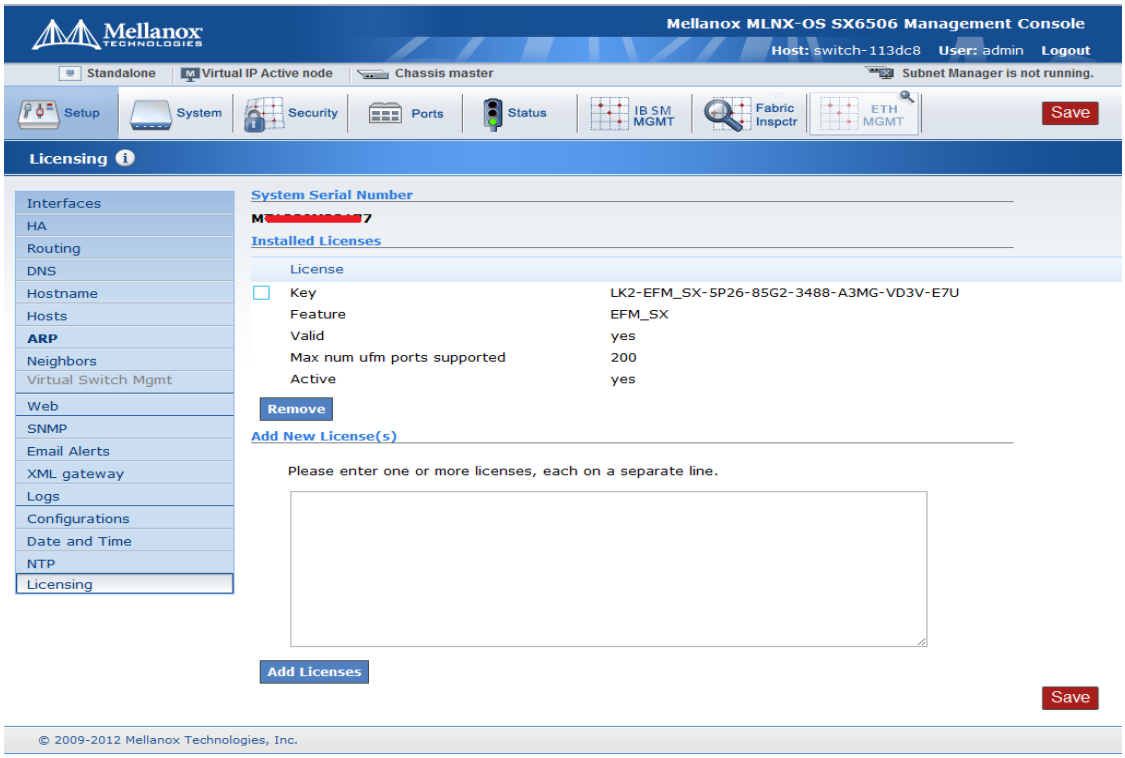
2.4.2 Installing MLNX-OS License (Web)

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

Step 1. Log in as *admin*.

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

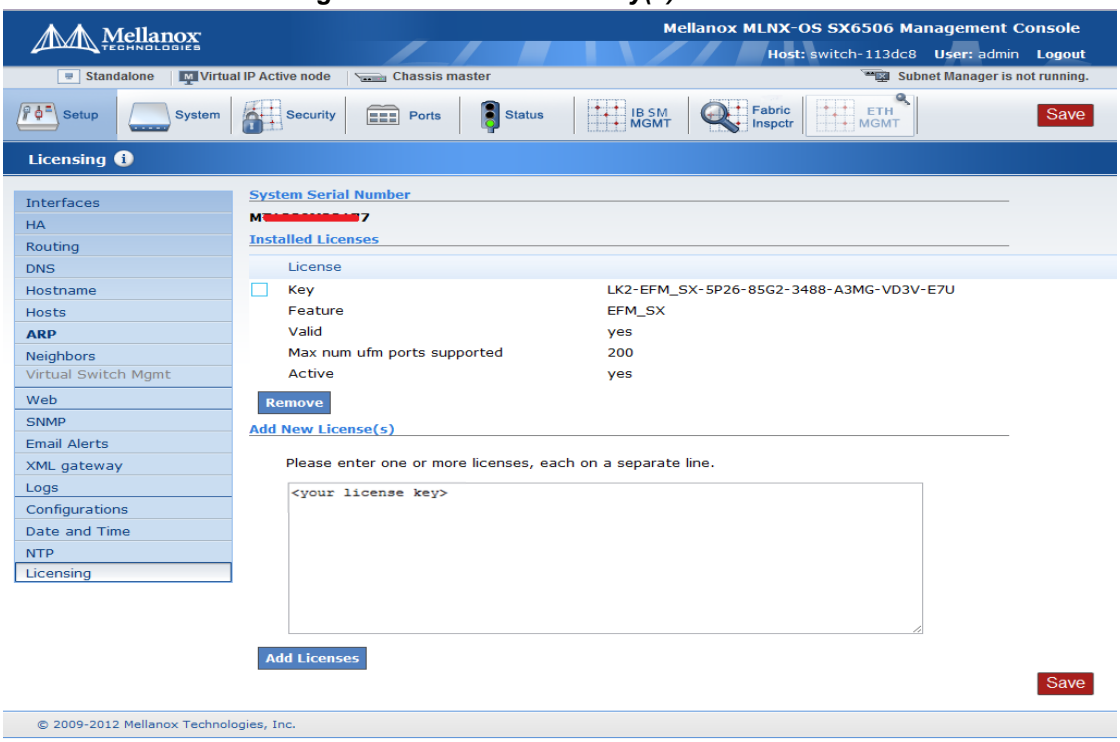
Figure 7: No Licenses Installed



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.

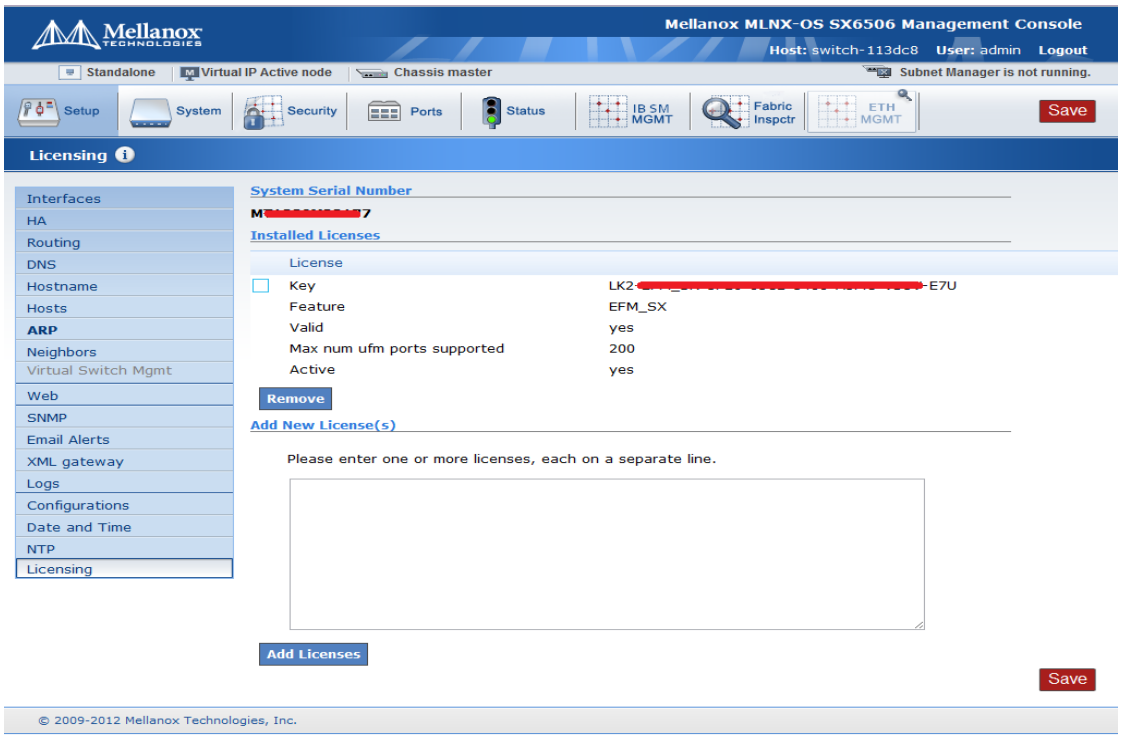
If you wish to add another license key in the future, you can simply enter it in the text box and click “Add Licenses” to install it.

Figure 8: Enter License Key(s) in Text Box



All installed licenses should now be displayed.

Figure 9: 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
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 23.

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

2.4.4 Commands

file eula upload

file eula upload <filename> <URL>

Uploads the Mellanox End User License Agreement to a specified remote location.

Syntax Description	filename	The Mellanox End User License Agreement
	URL	URL or scp://username[:password]@hostname/path/filename
Default	N/A	
Configuration Mode	Config	
History	3.4.1100	
Role	monitor/admin	
Example	`switch (config) # file help-docs upload Mellanox_End_User_License_Agreement.pdf <scp://username[:password]@hostname/path/filename>` `switch (config) #`	
Related Commands	license	
Note		

file help-docs upload

file help-docs upload <filename> <URL or scp://username[:password]@host-name/path/filename>

Uploads the MLNX-OS UM or RN to a specified remote location.

Syntax Description	filename	The file to upload to a remote host
	URL	URL or scp://username[:password]@hostname/path/filename
Default	N/A	
Configuration Mode	Config	
History	3.4.1100	
Role	admin	
Example	`switch (config) # file help-docs upload MLNX-OS_LEN_IB_User_Manual.pdf <scp://username[:password]@hostname/path/filename>` `switch (config) #`	
Related Commands		
Note		

license delete

license delete <license-key>

Removes license keys by ID.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.4.1100
Role	admin
Example	`switch (config) # license delete <license-key>` `switch (config) #`
Related Commands	
Note	

license install

licenses install <license-key>

Installs a new license key.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.4.1100
Role	admin
Example	`switch (config) # licenses install <license-key>` `switch (config) #`
Related Commands	
Note	

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	3.4.1100
Role	admin

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

Related Commands	
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 6 - CLI Modes and Config Context

Configuration Mode	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.
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 7 - 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 8 - 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 8 - 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) # show asic-version | include SX
MGMT               SX                  9.3.3150

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

switch (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:

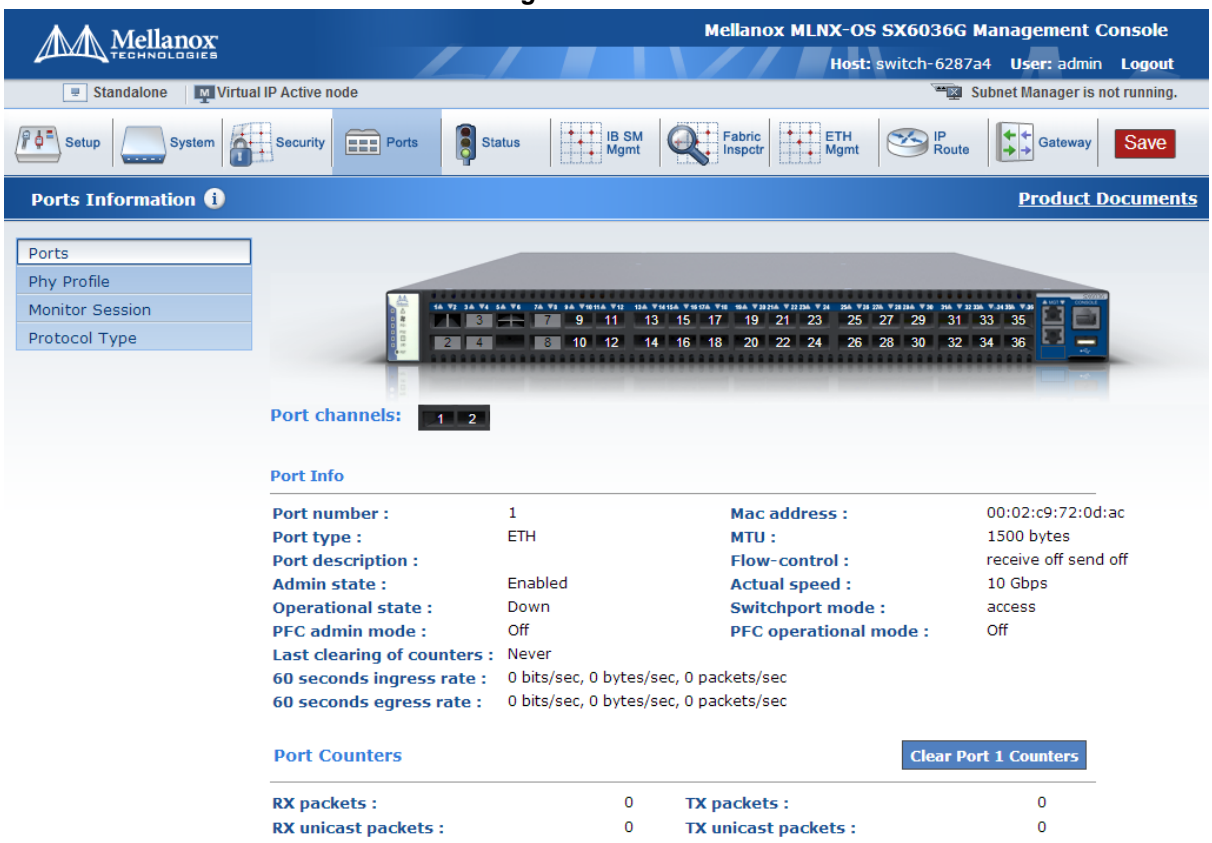
- Internet Explorer 8.0 or higher
- Chrome 18 or higher
- Mozilla Firefox 12 or higher
- Safari 5 or higher

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 10: WebUI



3.2.1 Setup Menu

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

Table 9 - WebUI 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 9 - WebUI 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 10 - WebUI 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 10 - WebUI 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 11 - WebUI 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 12 - WebUI 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 13 - WebUI 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.

3.3 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	

terminal

terminal {length <number of lines> | resize | type <terminal type> | width <number of characters>}
no terminal type

Configures default CLI options for all future sessions.
The no form of the command clears the terminal type.

Syntax Description	length	Sets the number of lines for this terminal Range: 5-999
	resize	Resizes the CLI terminal settings (to match with real terminal)
	type	Sets the terminal type. Possible values: ansi, console, dumb, linux, screen, vt52, vt100, vt102, vt220, xterm.
	width	Sets the width of this terminal in characters Range: 34-999
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # terminal length 500` `switch (config) #`	
Related Commands	show terminal	
Note		

terminal sysrq enable

terminal sysrq enable
no terminal sysrq enable

Enable SysRq over the serial connection (RS232 or Console port).
The no form of the command disables SysRq over the serial connection (RS232 or Console port).

Syntax Description	N/A
Default	Enabled
Configuration Mode	Config
History	3.4.3000
Role	admin
Example	`switch (config) # terminal sysrq enable` `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	Any Command Mode
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	
	3.4.2300	Added notes
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
124574979953740101054914168679199879767768820169843759428319155849627969937540659608580427221904245045659870586665814485449313217236506878951713570509420864336951833046700451354269467758379288848962624165330724512160918999830386915710362193855779785962822146445334448137121056286541583022982220576029771297093"
    RSA v2 host key: "switch-5ea5d8 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAA-
IEArB9i5OnukAHNUOkwpCmEl0m88kJgBzL22+F5tfaSn+S0pVYxrceZeyuzXsoZ1VtFTk2-
Fydwy0YvMS0Kcv2PuCrPZV/
GYd31QEnn22rEmrlPrKCrMl1XlUy6DFlr3OgwWm1baobmDlG/gSziWz/gc4Jgqf2CyX-
Fq4pzaR1jar1Vk="
    DSA v2 host key: "switch-5ea5d8 ssh-dss AAAAB3NzaC1kc3MAAAC-
BAMeJ3S+nyaHhRbwv3tJqlWttDC35RZVC5iG4ZEvMMHp28VL94OcyyuGh39VCdM9pEVaI7h
zZrsgHrNqakb/YLD/7anGH3wpl9Fx8lfe0RH3bloJzG+mJ6R5momdoPCrKwEKiKABKE00-
jLzlVznpP0IHxjwF+TbR3dK5HwVzQYw/bAAAAFQCBoDPqBZZa+2KylKlzUsbZ2pKhgQAAA-
IAJK+StiQdtORw1B5UCMzTrTef5L07DSfVreMEYtTRnBBtgVSNqQFWpSQIYbVDHQr9T6qCM
4VO39DuHUGQ1TMDIX7t+9mfbB87YyUu5a/ndbf3GhNhxHWwbzlr9hgLL7FSHA7DYH7bVOZ-
RlqxH64eQKGZqy1ps/F4E31lyn7GC4EQAAAIA/2osHipXf+NRjplgfmHROVVf/mGE9Vzc9/
AMUxlJJn5VhvEJ5CZW9cI+LxMOJojhOj3YW3B1czGxRObDA9vUbKXTNc8bkgoUrxySAH1rH
N0PqJgeT4L009AItSp3m1mxHqdS7jixfTvOTEKWXrgpczlmTB8+zjhUah/YuuBl2H
g=="
switch (config) #
```

Related Commands

show ssh server
system secure-mode enable

Note

When working in secure mode, the commands “ssh server host-key rsa1” and “ssh server host-key generate” do not create RSAv1 key-type.

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 security strict

ssh server security strict

Enables strict security settings.
The no form of the command disables strict security settings.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	`switch (config) # ssh server security strict` `switch (config) #`
Related Commands	show ssh server
Note	

ssh server tcp-forwarding enable

ssh server tcp-forwarding enable

Enables TCP port forwarding.
The no form of the command disables TCP port forwarding.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	`switch (config) # ssh server tcp-forwarding enable` `switch (config) #`
Related Commands	show ssh server
Note	

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
AAAAB3NzaC1yc2EAAAABIwAAAIEArB9i5OnukAHNUOkwpCmEl0m88kJgB-
zL22+F5tfaSn+S0pVYxrceZeyuzXsoZ1VtFTk2Fydwy0YvMS0Kcv2PuCrPZV/
GYd31QEnn22rEmrlPrKCrMl1XlUy6DFlr3OgwWm1baobmDlG/gSziWz/gc4Jgqf2CyX-
Fq4pzaR1jar1Vk="

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

telnet

Logs into another system using telnet.

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

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 cache-enable

	web cache-enable **no web cache-enable** Enables web clients to cache webpages. The no form of the command disables web clients from caching webpages.
Syntax Description	N/A
Default	Enabled
Configuration Mode	Config
History	3.4.1100
Role	admin
Example	`switch (config) # no web cache-enable`
Related Commands	N/A
Note	

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 | TLS | 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 | TLS | TLS1.2}	Sets ciphers 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
		Added TLS parameter to “ssl ciphers”
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 3.4.1100 Updated Example
Role	admin

Example	`switch (config) # show web`
	
	`Web User Interface:`
	`  Web interface enabled: yes`
	`  Web caching 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
switch (config) #
```

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 Commands

4.1.5.1 Interface

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

interface

interface {mgmt0 | mgmt1 | lo | vlan<id> | ib0}

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).
	ib0	IPoIB in-band management, relevant only for Infini-Band switch systems.
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>	
Notes		

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>
Notes	If DHCP is enabled on the specified interface, then the DHCP IP assignment will hold until DHCP is disabled.

ip default-gateway

ip default-gateway <next hop IP address or interface name>
no ip default-gateway

Configures a default route.
The no form of the command removes the current default route.

Syntax Description	next hop IP address or interface name — IP address, lo, mgmt0, or mgmt1.
Default	N/A
Configuration Mode	Config Interface Management
History	3.1.0000
Role	admin
Example	`switch (config) # ip default-gateway mgmt1` `switch (config) #`
Related Commands	
Notes	

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>
Notes	• 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>
Notes	

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>
Notes	• 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>
Notes	• 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

Notes

- 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
Notes	

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
Notes	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
Notes	

ipv6 enable

ipv6 enable
no ipv6 enable

Enables all IPv6 addressing for this interface.
The no form of the command disables all IPv6 addressing for this interface.

Syntax Description	N/A
Default	IPv6 addressing is disabled
Configuration Mode	Config Interface Management
History	3.1.0000
Role	admin

Example

```
switch (config interface mgmt0) # ipv6 enable
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 address show interface <ifname>
Notes	• The interface identifier is a 64-bit long modified EUI-64, which is based on the MAC address of the interface • If IPv6 is enabled on an interface, the system will automatically add a link-local address to the interface. Link-local addresses can only be used to communicate with other hosts on the same link, and packets with link-local addresses are never forwarded by a router. • A link-local address, which may not be removed, is required for proper IPv6 operation. The link-local addresses start with “fe80::”, and are combined with the interface identifier to form the complete address.

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>

Notes

- 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

ipv6 dhcp primary-intf

ipv6 dhcp primary-intf <if-name>
no ipv6 dhcp primary-intf

Sets the interface from which non-interface-specific (resolver) configuration is accepted via DHCPv6.
The no form of the command resets non-interface-specific (resolver) configuration.

Syntax Description	if-name	Interface name: • lo • mgmt0 • mgmt1
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ipv6 dhcp primary-intf mgmt0` `switch (config) #`	
Related Commands	ipv6 enable ipv6 address show interface <ifname>	
Notes		

ipv6 dhcp stateless

ipv6 dhcp stateless
no ipv6 dhcp stateless

Enables stateless DHCPv6 requests.
The no form of the command disables stateless DHCPv6 requests.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	`switch (config) # ipv6 dhcp stateless` `switch (config) #`
Related Commands	ipv6 enable ipv6 address show interface <ifname>
Notes	• This command only gets DNS configuration, not an IPv6 address • The no form of the command requests all information, including an IPv6 address

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
Notes	

4.1.5.2 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	
Notes	• 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	
Notes		

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	
Notes		

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	
Notes		

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
Notes	• 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
Notes	

4.1.5.3 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
Notes	

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	
Notes	• 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	
Notes		

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	
Notes	The configured IPv4 default gateway will not be used if DHCP is enabled.	

4.1.5.4 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`
	
	`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	
Notes		

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. Range: 60-28800.
Default	1500 seconds	
Configuration Mode	Config	
History	3.2.0230	
Role	admin	
Example	`switch (config) # ip arp timeout 2000` `switch (config) #`	
Related Commands	ip arp show ip arp	
Notes	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		
Notes		

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	
Notes	• 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
Notes	• Clearing Neighbor Discovery Protocol (NDP) cache removes only the dynamic entries learned and not the static entries configured • Use the no form of the 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	
Notes		

4.1.5.5 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      DHCP      Valid
Interface   Enabled   Running   lease
-------------------------------------
lo          no        no        no
mgmt0       yes       yes       yes
mgmt1       yes       yes       no

DHCP primary interface:
   Configured: mgmt0
   Active:     mgmt0

DHCP default gateway yields 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]
Notes	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]
Notes	

4.1.5.6 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	http://linux.about.com/od/commands/l/blcm-dl8_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	
Notes		

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	
Notes	

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]
[-D list possible interfaces] [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
Notes	

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	
Notes	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	
Notes		

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	
Notes		

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
Notes	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
Notes	

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
Notes	

4.3 Unbreakable Links

MLNX-OS® offers a phy profile configuration for VPI interfaces.

PHY profile includes Link Level Retransmission (LLR) configuration. A PHY profile is bind to any VPI interface.

4.3.1 Link Level Retransmission (LLR)

Link Level Retransmission (LLR) is used on signal integrity marginal systems to decrease and/or eliminate the impact of physical errors on the system's performance.

- LLR transmitter breaks the transmitted Layer 2 data stream into Cells and adds a CRC checksum to each cell.
- LLR receiver checks the Cell CRC, in case there is no CRC errors, it forwards the cell and acknowledges the peer.

If a cell is dropped by the receiver the transmitter retransmits the cell.

LLR is a Mellanox proprietary feature and will only work with Mellanox to Mellanox ports.

LLR is not operational for cables longer then 30m.

LLR Mode

The following LLR modes are applicable per port per speed:

- disable – no LLR
- enable – the port becomes passive, only if it got a request to use LLR it activates, otherwise it remains disabled
- enable-request – the port becomes active, it keeps sending LLR requests to the peer

LLR Negotiation

Both ports on the link perform LLR discovery and negotiation. In order the LLR to be in active state on the link, the following should apply:

- One port must be configured with LLR "enable-request" on the specified speed.
- The other port (peer) may be configured with LLR "enable-request" or "enable" on the same specified speed

If both the local port and remote port configured with LLR "enabled" the LLR negotiation will not be activated - the ports will remain in LLR in-active state.

LLR Status

LLR status is a port parameter that states the current state of the LLR.

- Active – LLR is operationally running
- In-Active – LLR is not running

4.3.2 Configuring Phy Profile & LLR

➢ ***To configure a phy profile:***

Step 1. Create/edit a phy profile and enter a phy profile configuration mode. Run:

```
switch (config) # phy-profile my-profile
switch (config phy profile my-profile) #
```

Step 2. Configure LLR attributes. Run:

All ports mapped to the phy profile must be in shutdown state before editing the profile.

```
switch (config phy profile my-profile) # llr support ib speed FDR enable-request
switch (config phy profile my-profile) # llr support ib speed QDR disable
switch (config phy profile my-profile) # ...
```

Step 3. Bind the profile to the desired interface. Run:

The port must be in shutdown state before binding the phy-profile.

```
switch (config) # interface ib 1/1
switch (config interface ib 1/1) # shutdown
switch (config interface ib 1/1) # phy-profile map my-profile
switch (config interface ib 1/1) # no shutdown
switch (config interface ib 1/1) #
```

Step 4. Verify LLR configuration and status. Run:

```
switch (config) # show interface ib llr

Interface phy-profile LLR status …
ib 1/1    my-profile  Active
ib 1/2     disable    Inactive
...
switch (config) #
```

Step 5. Display phy-profile configuration. Run:

```
switch (config) # show phy-profile my-profile
Profile: my-profile
llr support ib-speed
SDR: disable
DDR: disable
QDR: disable
FDR10: enable-request
FDR: enable-request
switch (config) #
```

4.3.3 Commands

phy-profile

phy-profile <profile-name>
no phy-profile <profile-name>

Creates a PHY profile (port physical parameters), and enter the profile configuration mode.
The no form of the command deletes the phy-profile

Syntax Description	profile-name	40-byte-string.
Default	"high-speed-ber": FDR and FDR10 speeds are LLR enable-request state, all the rest speed options are in disable state.	
Configuration Mode	Config	
History	3.2.0700	First version
	3.3.3000	Default updated
Role	admin	
Example	`switch (config) # phy-profile my-profile` `switch (config phy-profile my-profile) #`	
Related Commands		
Notes	• 10 profiles is the maximum profiles supported. • When deleting a profile, all interface related to that profile need to be in shutdown state.	

llr support ib-speed

llr support ib-speed <speed-options> <speed-actions>
no llr support ib-speed <speed-options>

Sets LLR InfiniBand supported speeds.
The no form of the command disables the llr on this speed.

Syntax Description	speed-options	• sdr • ddr • qdr • fdr10 • fdr
	speed-action	enable: only enable bit is on (passive mode) enable-request: both enable and request bits are on (active mode)
Default	N/A	
Configuration Mode	Config Phy-Profile	
History	3.2.0700	
Role	admin	

Example	`switch (config) # phy-profile my-profile`
	`switch (config phy-profile my-profile) # llr support speed fdr enable`
	`switch (config phy-profile my-profile) #`	

Related Commands		
Notes		

phy-profile map

phy-profile map <profile-name>
no phy-profile map

Binds a phy-profile to the interface.
The no form of the command set the port mapping to the default profile.

Syntax Description	profile-name	40-byte-string.
Default	Default profile - “high-speed-ber” with the following attributes: SDR: disable DDR: disable QDR: disable FDR10: enable-request FDR: enable-request	
Configuration Mode	Config Interface IB	
History	3.2.0700	First version
	3.3.3000	Default updated
Role	admin	

Example	`switch (config) # interface ib 1/1`
	`switch (config interface ib 1/1) #phy-profile map my-profile`
	`switch (config interface ib 1/1) #`	

Related Commands		
Notes		

show phy-profile

show phy-profile [profile-name]

Shows phy-profile list

Syntax Description	profile-name	40-byte-string. Shows a specific profile.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.2.0700	First version
	3.3.3000	Output updated.
Role	admin	

Example	`switch (config) # show phy-profile`
	
	`Profile: high-speed-ber`
	`  --------`
	`  llr support ib-speed`
	`  SDR: disable`
	`  DDR: disable`
	`  QDR: disable`
	`  FDR10: enable-request`
	`  FDR: enable-request`
	
	`switch (config) #`	

Related Commands	phy-profile	
Notes		

show llr

show interface ib [<number>] llr

Shows LLR status

Syntax Description	number	The interface number
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.2.0500	
Role	admin	

Example	`switch (config) # show interface ib llr`
	`Interface phy-profile LLR status`
	`Ib 1/1 high-speed-ber Active`
	`Ib 1/2 high-speed-ber Inactive`
	`Ib 1/3 high-speed-ber Inactive`
	`...`
	`switch (config) #`	

Related Commands		
Notes		

-

4.4 Software Management

4.4.1 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 4.4.2, “Upgrading MLNX-OS Software,” on page 153.

4.4.2 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.

To upgrade the MLNX-OS version of on a gateway, SM, or MLAG cluster, please refer to Section 4.4.3, “Upgrading MLNX-OS HA Groups,” on page 157.

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 3.3.3130 2013-03-20 21:32:25 ppc

  Partition 2:
  SX_PPC_M460EX 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 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-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 4.4.2, “Upgrading MLNX-OS Software,” on page 153.

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).

4.4.3 Upgrading MLNX-OS HA Groups

In case fallback is ever necessary in an HA group, all cluster nodes must have the same MLNX-OS version installed and they must be immediately reloaded.

➢ ***To upgrade MLNX-OS version without affecting an HA group:***

Step 1. Identify the HA group master.

for IB HA. Run:

```
switch (config) # show ib ha
Global HA state
==================
IB Subnet HA name:subnet4
HA IP address: 192.168.10.43/24
Active HA nodes: 2
ID             State Role         IP                SM Priority
-------------------------------------------------------------------
switch         standalone         192.168.10.42       disabled
switch         master             192.168.10.18       disabled
```

Step 2. Upgrade standby nodes in the HA group according to steps 1-8 in section Section 4.4.2, on page 153.

Step 3. Wait until all standby nodes have rejoined the group.

Step 4. Upgrade the master node in the HA group according to steps 1-8 in section Section 4.4.2, on page 153.

4.4.4 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-3.1.1224.img
  SX-OS_PPC_M460EX 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-3.0.1224.img
switch (config) #
```

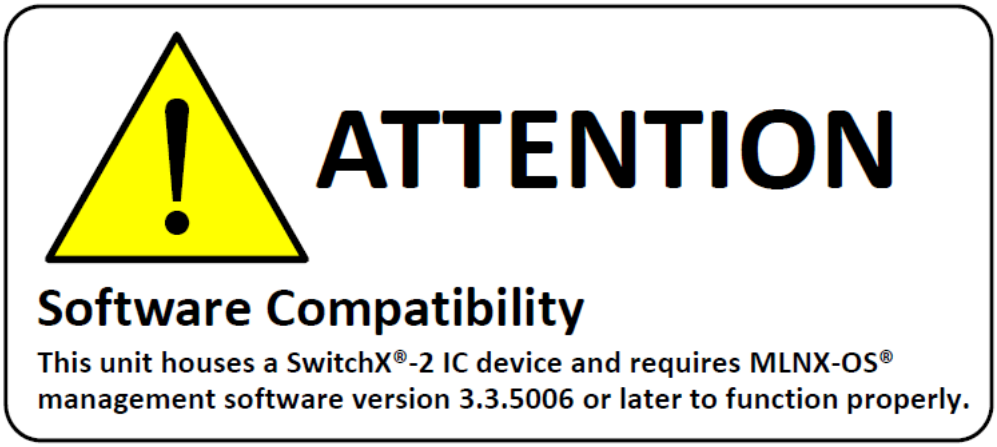
When deleting an image, you delete the file but not the partition. This is recommended so as to not overload system resources.

4.4.5 Downgrading MLNX-OS Software

IMPORTANT NOTE

If in possession of an SX65xx director switch with the notice presented in Figure 11, the lowest MLNX-OS version you can downgrade to is 3.3.5006; otherwise, the switch system will malfunction.

Figure 11: SX65xx Downgrade Attention Sticker



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.

4.4.5.1 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%[################################################ ###############]
```

4.4.5.2 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
```

4.4.5.3 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
```

4.4.6 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.

4.4.6.1 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.

4.4.6.2 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.

4.4.7 Image Maintenance via Mellanox ONIE

Supported only on MSX1710-BS2F2O switch system.

The switch system MSX1710-BS2F2O allows booting ONIE and burning a different OS on the switch system.

When booting or rebooting the switch system an ONIE entry has been added to the boot loader options. For example:

```
                            GNU GRUB version 2.02~beta2

X86_64 3.4.1932 2015-04-24 18:04:12 x86_64 1
X86_64 3.4.1932 2015-04-24 18:04:12 x86_64 2
ONIE
```

While MLNX-OS is installed, editing grub entry and grub command line are restricted.

ONIE may be selected from this prompt to allow ONIE functionality over this system. To do so, the MLNX-OS image burned must be uninstalled from the system. Once MLNX-OS is uninstalled, ONIE boots and the user is presented with ONIE command prompt which allows regular ONIE functionality according to Mellanox SwitchX ONIE Switch User Manual.

To return to MLNX-OS mode, MLNX-OS must be reinstalled using the ONIE Network OS installer file according to the preferred ONIE Network OS installation flow.

The switch system then loads from factory set configurations (automatically saved configuration is not supported).

All previous MLNX-OS installation flows are supported, therefore, the command “image fetch” or “image install” may be used to save previous configuration.

4.4.8 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	
Notes		

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 next fallback-reboot enable` `switch (config) #`
Related Commands	show images
Notes	• 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.

boot system

boot system {location | next}
no boot system next

Configures which system image to boot by default.
The no form of the command resets the next boot location to the current active one.

Syntax Description	location	Specifies location from which to boot system • 1 – installs to location 1 • 2 – installs to location 2
	next	Boots system from next location after one currently booted
Default	N/A	
Configuration Mode	Config	
History	3.2.0506	
Role	admin	
Example	`switch (config) # boot system location 2` `switch (config) #`	
Related Commands	show images	
Notes		

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	
Notes		

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	
Notes		

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	
Notes	• 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	
Notes	• 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	
Notes		

image options

image options {require-sig | serve}
no image options {require-sig | serve all}

Configures options and defaults for image usage.
The no form of the command disables options and defaults for image usage.

Syntax Description	require-sig	Requires images to be signed by a trusted signature
	serve all	Configures options for serving image files from this appliance
	all	Makes all image files on this appliance available for HTTP and HTTPS download
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	
Notes		

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
Notes	

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
Notes	

4.5 Configuration Management

4.5.1 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) #
```

4.5.2 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) #
```

4.5.3 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.

4.5.3.1 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`.

4.5.3.2 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 4.5.3.1) 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.

4.5.4 Commands

4.5.4.1 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
Notes	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	
Notes		

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>	
Notes		

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	
Notes		

reload

reload [force immediate | halt [noconfirm] | noconfirm]

Reboots or shuts down the system.

Syntax Description	force immediate	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	
Notes		

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	
Notes		

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	
Notes		

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
Notes	

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
Notes	

4.5.4.2 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	
Notes	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		
Notes	• 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	
Notes	• 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	
Notes	• 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
Notes	• 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		
Notes	• 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	
Notes	• 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	
Notes		

configuration revert

configuration revert {factory [keep-basic | keep-connect]| saved}

Reverts the system configuration to a previous state.

Syntax Description	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).
	saved	Reverts running configuration to last saved configuration.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # configuration revert saved` `switch (config) #`	
Related Commands	show configuration	
Notes	This command is only available when working with an InfiniBand profile.	

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
Notes	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	
Notes		

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	
Notes		

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	
Notes		

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	
Notes	No configuration file may have the name “active”.	

configuration write

configuration write [local | to <filename> [no-switch]]

Saves the running configuration to the active configuration file.

Syntax Description	local	Saves the running configuration locally (same as "write memory local")
	to <filename>	Saves the running configuration to a new file under a different name and makes it the active file
	no-switch	Saves the running configuration to this file but keep the current one active
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # configuration write` `switch (config) #`	
Related Commands	write	
Notes		

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	
Notes		

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		

```
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) #
```

Related Commands	
Notes	

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	
Notes	

4.6 Logging

4.6.1 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 15, “Supported Event Notifications and MIB Mapping,” on page 225.

4.6.2 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> priority <level>
```

4.6.3 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 14 lists the POST return codes and their meanings.

Table 14 - POST Return Codes

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

Table 14 - 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

4.6.4 Commands

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
Notes	

logging debug-files

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

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
	upload	Uploads debug log file to a remote host
	log-file	Possible values: 1-7, or current
	upload URL	HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported (e.g.: scp://username[:password]@hostname/path/filename)
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	`switch (config) # logging debug-files delete current` `switch (config) #`	
Related Commands		
Notes		

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
Notes	

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
Notes	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 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	
Notes		

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
Notes	

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	
Notes		

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
Notes	

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	
Notes		

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		
Notes		

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
Notes	• 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 trap

logging trap
no logging trap

Configures the minimum severity of log messages sent to syslog servers.
The no form of the command disables sending event log messages to syslog servers.

Syntax Description	severity level	The minimum severity level for all configured syslog servers: • none – disable logging • emerg – emergency: system is unusable • alert – action must be taken immediately • crit – critical conditions • err – error conditions • warning – warning conditions • notice – normal but significant condition • info – informational messages • debug – debug-level messages
Default	Receiving logging is disabled	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # logging trap info` `switch (config) #`	
Related Commands		
Notes		

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>
Notes	

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	
Notes	When using a regular expression containing | (OR), the expression should be surrounded by quotes ("<expression>"), otherwise it is parsed as filter (PIPE) command.	

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 15 - 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 15 - 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 mismatch	Mellanox-EFM-MIB: powerRedundancyMismatch	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 triggered by a local bridge	Bridge-MIB: topologyChange	Supported for Ethernet
unexpected-shutdown	Unexpected system shutdown	Mellanox-EFM-MIB: unexpectedShutdown	
To send, use the CLI command: `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 enable

email autosupport enable
no email autosupport enable

Sends automatic support notifications via email.
The no form of the command stops sending automatic support notifications via email.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.2.3000
Role	admin
Example	`switch (config) # email autosupport enable`
Related Commands	N/A
Notes	

email autosupport event

email autosupport event <event>
no email autosupport event

Specifies for which events to send auto-support notification emails.
The no form of the command resets auto-support email security mode to its default.

Syntax Description	event	• process-crash – a process has crashed • process-exit – a process unexpectedly exited • liveness-failure – a process iss detected as hung • cpu-util-high – CPU utilization has risen too high • cpu-util-ok – CPU utilization has fallen back to normal levels • paging-high – paging activity has risen too high • paging-ok – paging activity has fallen back to normal levels • disk-space-low – filesystem free space has fallen too low • disk-space-ok – filesystem free space is back in the normal range • memusage-high – memory usage has risen too high • memusage-ok – memory usage has fallen back to acceptable levels • netusage-high – network utilization has risen too high • netusage-ok – network utilization has fallen back to acceptable 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 • unexpected-cluster-join – node has unexpectedly joined the cluster • unexpected-cluster-leave – node has unexpectedly left the cluster • unexpected-cluster-size – the number of nodes in the cluster is unexpected • unexpected-shutdown – unexpected system shutdown • interface-up – an interface's link state has changed to up • interface-down – an interface's link state has changed to down • user-login – a user has logged into the system • user-logout – a user has logged out of the system • health-module-status – health module Status • temperature-too-high – temperature has risen too high • low-power – low power supply • low-power-recover – low power supply Recover • insufficient-power – insufficient power supply • power-redundancy-mismatch – power redundancy mismatch • insufficient-fans – insufficient amount of fans in system • insufficient-fans-recover – insufficient amount of fans in system recovered • asic-chip-down – ASIC (Chip) Down • internal-bus-error – internal bus (I2C) Error • internal-link-speed-mismatch – internal links speed mismatch

Default	N/A
Configuration Mode	Config
History	3.2.3000
Role	admin
Example	`switch (config) # email autosupport event process-crash`
Related Commands	N/A
Notes	

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	
Notes		

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
Notes	

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	
Notes		

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	
Notes		

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
Notes	

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]
Notes	

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
Notes	

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	
Notes	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	
Notes		

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	
Notes		

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
Notes	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]
Notes	

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	
Notes		

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
Notes	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	
Notes	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
Notes	

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	
Notes	

4.9 User Management and Security

4.9.1 User Accounts

There are two general 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 16 - User Roles (Accounts) and Default Passwords

User Role	Default Password
admin	admin
monitor	monitor
xmladmin	xmladmin
xmluser	xmluser

To remove passwords from the XML users, run the command `username <username> nopassword`.

4.9.2 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.

4.9.2.1 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

4.9.2.2 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

4.9.2.3 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
```

4.9.3 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.
	capability <cap>	Defines user capabilities. • admin - full administrative capabilities • monitor - read only capabilities, can not change the running configuration • unpriv – can only query the most basic information, and cannot take any actions or change any configuration • v_admin – basic administrator capabilities
	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
	3.4.1100	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       Password set (SHA512)
xmluser     XML Monitor User        monitor     Password set (SHA512)
switch (config) #
```

Related Commands

show usernames
show users

Notes

- To enable a user account, just set a password on it (or use the command `username <user> nopassword` 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 command `show configuration`, 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
Notes	

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	
Notes		

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
Notes	

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	
Notes	• 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	
Notes	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

aaa authentication attempts track {downcase | enable}
no aaa authentication attempts track {downcase | enable}

Configure tracking for failed authentication attempts.
The no form of the command clears configuration for tracking authentication failures.

Syntax Description	downcase	Does not convert all usernames to lowercase (for authentication failure tracking purposes only).
	enable	Disables tracking of failed authentication attempts
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config) # aaa authentication attempts track enable`	
Related Commands	N/A	
Notes	• 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
Notes	

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	
Notes		

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	
Notes		

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	
Notes		

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.
	order <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
Notes	• 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 is given monitor permissions. • If AAA authorization order policy is configured to remote-only, then when upgrading to 3.4.3000 or later from an older MLNX-OS version, this policy is changed to remote-first.

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
Notes	

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
Notes	

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	
Notes	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> | prompt-key | retransmit <retries> | timeout <seconds>]
no radius-server host <IP address> [auth-port | enable]

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
	auth-port	Configures authentication port to use with this RADIUS server
	port	RADIUS server UDP port number
	key	Configures shared secret to use with this RADIUS server
	prompt-key	Prompt for key, rather than entering on command line
	retransmit	Configures retransmit count to use with this RADIUS server
	retries	Number of retries (0-5) before exhausting from the authentication
	timeout	Configures timeout between each try
	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
Notes	• 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
Notes	

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	
Notes	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> | prompt-key | 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
	auth-port	Configures authentication port to use with this TACACS+ server
	port	TACACS+ server UDP port number
	auth-type	Configures authentication type to use with this TACACS+ server
	type	Authentication type. Possible values are: • ASCII • PAP (Password Authentication Protocol)
	key	Configures shared secret to use with this TACACS+ server
	secret	Sets a secret key (shared hidden text string), known to the system and to the TACACS+ server
	prompt-key	Prompts for key, rather than entering key on command line
	retransmit	Configures retransmit count to use with this TACACS+ server
	retries	Number of retries (0-5) before exhausting from the authentication
	timeout	Configures timeout to use with this TACACS+ server
	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

Notes

- 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
Notes	

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
Notes	

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
Notes	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
Notes	• 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
Notes	• 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
Notes	

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
Notes	

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
Notes	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
Notes	

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

Notes

- 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

Notes

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

Notes

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
Notes	

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 ike

crypto ipsec ike {clear sa [peer {any | <IPv4 or IPv6 address>} local <IPv4 or IPv6 address>] | restart}

Manage the IKE (ISAKMP) process or database state

Syntax Description	clear	Clears IKE (ISAKMP) peering state
	sa	Clears IKE generated ISAKMP and IPSec security associations (remote peers are affected)
	peer	Clears security associations for the specified IKE peer (remote peers are affected) all – clears security associations for all IKE peerings with a specific local address (remote peers are affected) IPv4 or IPv6 address – clears security associations for specific IKE peering with a specific local address (remote peers are affected)
	IPv4 or IPv6 address	Clears security associations for the specified IKE peering (remote peer is affected)
	local	Clear security associations for the specified/all IKE peering (remote peer is affected)
	restart	Restarts the IKE (ISAKMP) daemon (clears all IKE state, peers may be affected)
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	`switch (config)# crypto ipsec ike restart` `switch (config)#`	
Related Commands	N/A	
Notes		

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
Notes	

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	
Notes	• 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	
Notes	• 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	
Notes	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	
Notes		

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	
Notes		

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:              fe6df38dd26801971cb2d44f62d-
be492b6063c5f

    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

Notes

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
Notes	

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	
Notes	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	
Notes	• 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	
Notes		

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
Notes	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
Notes	• 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
Notes	

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	
Notes		

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	
Notes	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	
Notes	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
Notes	

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	
Notes		

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	
Notes		

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	
Notes		

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	
Notes	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	
Notes		

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 • eth_ip_day • eth_ip_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	
Notes		

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	
Notes		

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
Notes	

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 • eth-abs • eth_ip • 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	
Notes		

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	
Notes		

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	
Notes		

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
Notes	

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	
Notes		

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	
Notes		

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	
Notes		

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
Notes	

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	
Notes		

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 339.

Table 17 - 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`	
Related Commands		
Notes		

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	
Notes		

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	
Notes	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 IB	
History	3.3.4000	
Role	admin	
Example	`switch (config interface ib 1/1) # power-management width auto` `switch (config) #`	
Related Commands	show interface	
Notes		

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
Notes	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
Notes	

show version

show version

Displays version information for the currently running system image.

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

Example	`switch (config) # show version`
	`Product name:      MLNX-OS`
	`Product release:   3.1.0000`
	`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
Notes	

show version concise

show version concise

Displays concise version information for the currently running system image.

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

Example	`switch (config) # show version concise`
	`SX_PPC_M460EX SX_3.4.0000 2014-10-14 20:26:41 ppc`
	`switch (config) #`

Related Commands	N/A
Notes	

show uboot

show uboot

Displays u-boot version.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.5006 3.4.1110 Updated output
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 - 17:53:54)`
	`switch (config) #`

Related Commands	N/A
Notes	

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
Notes	

show inventory

show inventory

Displays system inventory.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000 3.4.1604 Removed CPU module output from Example
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`
	`switch (config) #`

Related Commands	N/A
Notes	

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
	3.4.2008	Updated command output
	3.4.3000	Updated command output and added note
Role	admin	

Example	`switch (config) # show module`
	`=====================`
	` Module    Status`
	`=====================`
	` MGMT      ready`
	` FAN1      ready`
	` FAN2      ready`
	` PS1       ready`
	` PS2       not-present`
	`switch (config) #`	

Related Commands	N/A	
Notes	The Status column may have one of the following values: error, fatal, not-present, powered-off, powered-on, ready.	

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
Notes	

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 3.4.2008 Updated Example
Role	admin

Example	`switch (config) # show asic-version`
	`==========`
	`Module Device Version`
	`==========`
	`MGMT SX 9.2.9160`
	
	`switch (config) #`

Related Commands	N/A
Notes	

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
Notes	

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
Notes	

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
Notes	

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
Notes	

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	
Notes		

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
Notes	

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
Notes	

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	
Notes		

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
Notes	

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 Example
	3.4.1100 Updated Example
Role	admin

Example	`switch (config) # show protocols`
	
	`Infiniband enabled`
	`switch (config) #`

Related Commands	N/A
Notes	

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 <time>}
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.
	time	In seconds. Range: 20-500.
Default	Enabled. Interval: 60 secs	
Configuration Mode	Config	
History	3.2.3000	
	3.4.1100	Added time parameter and updated notes
Role	admin	
Example	`switch (config) # snmp-server auto-refresh interval 120`	
Related Commands	show snmp	
Notes	• When configuring an interval lower than 60 seconds, the following warning message appears asking for confirmation: “Warning: this configuration may increase CPU utilization, Type 'YES' to confirm: YES”. • When disabling SNMP auto-refresh, information is retrieved no more than once every 60 seconds just like SNMP tables that do not have an auto-refresh mechanism.	

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	
Notes	• 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	
Notes		

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
Notes	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

Notes

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
Notes	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
Notes	

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

Notes

- 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	
Notes		

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>] | require-privacy}
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
	require-privacy	Requires privacy (encryption) for requests from this user
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
Notes	• The username chosen here may be anything that is valid as a local UNIX username (alpha-numeric, plus '-', '_', and '.'), but these usernames are unrelated to, and independent of, local user accounts. That is, they need not have the same capability level as a local user account of the same name. Note that these usernames should not be longer than 31 characters, or they will not work. • The hash algorithm specified is used both to create digests of the authentication and privacy passwords for storage in configuration, and also in HMAC form for the authentication protocol itself. • If the command ends after the auth password, the privacy algorithm is set to its default, which is AES-128, and the privacy password is set to whatever was specified for the authentication password. You may also specify the privacy algorithm while still not specifying a separate password. • There are three variants of the command, which branch out after the “v3” keyword. If “auth” is used next, the passwords are specified in plaintext on the command line. If “encrypted” is used next, the passwords are specified encrypted (hashed) on the command line. If “prompt-pass” is used, the passwords are not specified on the command line the user is prompted for them when the command is executing. If “priv” is not specified, only the auth password is prompted for. If “priv” is specified, the privacy password is prompted for; entering an empty string for this prompt will result in using the same password specified for authentication.

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	
Notes		

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
Notes	

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
Notes	

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
Notes	

5 InfiniBand Switching

5.1 Node Name

5.1.1 Commands

ib nodename

ib nodename <guid> name <name>
no ib nodename <guid>

Maps between GUID and node name.

Syntax Description	guid	The system GUID.
	name	User defined string.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib nodename 00:00:00:00:60:04:03:30 name my-name`
	`switch (config) # show ib nodename`
	`  GUID='00:00:00:00:60:04:03:30', name='my-name', discovered='no'`
	`switch (config) #`	

Related Commands		
Notes	If an entry with GUID exists, the existing name will be replaced with a new name.	

show ib nodename

show ib nodename

Maps between GUID and node name.

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

Example	`switch (config) # show ib nodename`
	`  GUID='00:00:00:00:60:04:03:30', name='my-name', discovered='no'`
	`switch (config) #`

Related Commands	ib nodename
Notes	

5.2 Fabric

5.2.1 Commands

fabric zero-counters

fabric zero-counters

Clears the performance counters of the node.

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

Example	`switch (config) # fabric zero-counters`
	`Counters zeroed successfully`
	`switch (config) #`

Related Commands	
Notes	

show fabric

show fabric {pm | sm}

Displays InfiniBand fabric details.

Syntax Description	pm	Displays InfiniBand fabric performance measurements.
	sm	Displays InfiniBand fabric SMs.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	First version
	3.4.0000	Added note
Role	admin	
Example		

```
switch (config) # show fabric sm
% # This database file was automatically generated by IBDIAG


ibdiagnet fabric SM report

  SM - master
    Port=0 lid=0x0005 guid=0x0002c903004a2980 dev=51000 priority:15

  SM - standby
    Port=0 lid=0x0001 guid=0x0000000000000111 dev=51000 priority:0
switch (config) #
```

Related Commands	
Notes	This command requires a fabric inspector license (LIC-fabric-inspector).

show guids

show guids

Displays GUIDs per ASIC in the chassis.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000 3.4.2008 Updated Example
Role	admin

Example	`switch (config) # show guids`
	`==========================================`
	`Module Device GUID`
	`==========================================`
	`SYSTEM - 00:02:C9:03:00:46:B3:A0`
	`S01 SX 00:02:C9:03:00:97:F1:10`
	`S02 SX 00:02:C9:03:00:97:F1:80`
	`S03 SX 00:02:C9:03:00:97:F1:00`
	`S04 SX 00:02:C9:03:00:97:F1:E0`
	`S05 SX 00:02:C9:03:00:97:F1:A0`
	`S06 SX 00:02:C9:03:00:97:F1:C0`
	`S07 SX 00:02:C9:03:00:97:F1:F0`
	`S08 SX 00:02:C9:03:00:97:F2:10`
	`S09 SX 00:02:C9:03:00:97:F1:30`
	`L01 SX 00:02:C9:03:00:97:FD:70`
	`L02 SX 00:02:C9:03:00:97:F8:90`
	`L03 SX 00:02:C9:03:00:97:FA:10`
	`L04 SX 00:02:C9:03:00:97:FD:10`
	`L05 SX 00:02:C9:03:00:97:F9:B0`
	`L06 SX F4:52:14:03:00:0D:82:00`
	`L07 SX 00:02:C9:03:00:97:FE:F0`
	`L08 SX 00:02:C9:03:00:97:FE:30`
	`L09 SX 00:02:C9:03:00:97:F6:B0`
	`L10 SX 00:02:C9:03:00:97:FA:D0`
	`L11 SX 00:02:C9:03:00:97:F8:30`
	`L12 SX 00:02:C9:03:00:97:FA:70`
	`L13 SX 00:02:C9:03:00:97:F9:50`
	`L14 SX 00:02:C9:03:00:97:FE:90`
	`L15 SX 00:02:C9:03:00:61:E9:90`
	`L16 SX 00:02:C9:03:00:97:FD:D0`
	`L17 SX 00:02:C9:03:00:61:E9:F0`
	`L18 SX 00:02:C9:03:00:97:F7:10`
	`switch (config) #`

Related Commands	
Notes	

show system guid

show {guids | system guid}

Displays the system GUID.

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

Example	`switch (config) # show system guid`
	`00:02:C9:03:00:43:D9:00`
	`switch (config) #`

Related Commands	
Notes	

show lids

	show lids Displays the LIDs of each module in the switch system
Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000 3.4.2008 Updated Example
Role	admin/monitor

Example	`switch (config) # show lids`
	`==========================================`
	`Module Device LID`
	`==========================================`
	`MGMT SIB 1`
	`switch (config) #`

Related Commands	
Notes	

5.3 Interface

5.3.1 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 ib 1/36 transceiver
Slot 1 port 36 state
        identifier             : QSFP+
        cable/ module type     : Passive copper, unequalized
        infiniband speeds      : SDR , DDR , QDR , FDR
        vendor                 : Mellanox
        cable length           : 2m
        part number            : MC2207130-0A1
        revision               : A3
        serial number          : MT1324VS02215

switch (config) #
```

The indicated cable length is rounded up to the nearest natural number.

5.3.2 Commands

interface ib

interface ib [internal] {<inf> | <inf-range>}

Enters the InfiniBand interface configuration mode.

Syntax Description	[internal] <inf>	For 1U switches: interface 1/<interface> For director switches: interface ib <interface> interface ib internal leaf <interface> interface ib internal spine <interface>
	inf-range	Enters the configuration mode of a range of interfaces. Format: <slot>/<port>-<slot>/<port>
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
	3.4.2008	Added internal leaf and spine options
Role	admin	
Example	`switch (config) # interface ib 1/1` `switch (config interface ib 1/1) #`	
Related Commands	show interface ib	
Notes	Interface range (inf-range) option is not valid on SX65xx systems.	

mtu

mtu <frame-size>

Configures the Maximum Transmission Unit (MTU) frame size for the interface.

Syntax Description	frame-size	Possible Value for MTU • 256 256 bytes • 512 512 bytes • 1K 1K bytes • 2K 2K bytes • 4K 4K bytes
Default	4096 bytes	
Configuration Mode	Config Interface IB	
History	3.1.0000	
Role	admin	
Example	`switch (config interface ib 1/1) # mtu 4K` `switch (config interface ib 1/1) #`	
Related Commands	show interface ib	
Notes		

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 IB
History	3.1.0000
Role	admin
Example	`switch (config interface ib 1/1) # shutdown` `switch (config interface ib 1/1) #`
Related Commands	show interface ib
Notes	N/A

description

description <string>

Sets an interface description.

Syntax Description	string	40 bytes
Default	“”	
Configuration Mode	Config Interface IB	
History	3.1.0000	
Role	admin	
Example	`switch (config interface ib 1/1) # description my-interface` `switch (config interface ib 1/1) #`	
Related Commands	show interface ib	
Notes		

speed

speed <port speed> [force]

Sets the speed negotiation of the interface.

Syntax Description	port speed	The following options are available: • sdr – 10.0Gb/s rate on 4 lane width • ddr – 20.0Gb/s rate on 4 lane width • qdr – 40.0Gb/s rate on 4 lane width • fdr10 – 40.0Gb/s rate on 4 lane width • fdr – 56.0Gb/s rate on 4 lane width • edr – 100.0Gb/s rate on 4 lane width
	force	Forces configuration of speed-list not containing SDR bit
Default	Depends on the port module type, not all interfaces support all speed options	
Configuration Mode	Config Interface IB	
History	3.1.0000	
	3.4.1604	Updated Syntax Description and Example
Role	admin	
Example	`switch (config interface ib 1/1) # speed fdr10 fdr edr` `switch (config interface ib 1/1) #`	
Related Commands	show interface ib	
Notes	• This command is backwards compatible so old configuration file containing this command with the old form (with legal bit mask) are still supported • Configuring more than one speed is possible by typing in consecutive speed names separated by spaces • If the speed-options list does not include SDR speed, it is configured automatically. However, if the force option is used, SDR does not get configured. • The force option is applicable only to FDR10 speed configuration • If the other side of the link is a SwitchX® or ConnectX®-3 device, to allow the link to raise in FDR speed, QDR speed must also be allowed	

op-vls

op-vls <value>

Sets the operational VLs of the interface.
The no form of the command sets the operational VLs to its default value.

Syntax Description	value	Possible value for operational VLs • 1 VL0 • 2 VL0, VL1 • 4 VL0 - VL3 • 8 VL0 - VL7
Default	8 (VL0 - VL7)	
Configuration Mode	Config Interface IB	
History	3.1.0000	
Role	admin	
Example	`switch (config interface ib 1/1) # op-vls 1` `switch (config interface ib 1/1) #`	
Related Commands	show interface ib	
Notes		

width

width <value>

Sets the width of the interface.
The no form of the command sets the speed of the interface to its default value.

Syntax Description	value	Possible value for width: • 1 – 1X • 5 – 1X, 4X
Default	5 (1X, 4X)	
Configuration Mode	Config Interface IB	
History	3.1.0000	
Role	admin	
Example	`switch (config interface ib 1/1) # width 1` `switch (config interface ib 1/1) #`	
Related Commands	show interface ib	
Notes		

clear counters

clear counters

Clears the interface counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config Interface IB
History	3.1.0000
Role	admin
Example	`switch (config interface ib 1/1) # clear counters` `switch (config interface ib 1/1) #`
Related Commands	show interface ib
Notes	

show interfaces ib

show interfaces ib <inf>

Displays the configuration and status for the interface.

Syntax Description	internal	Internal interfaces.
	inf	• Slot/Port (i.e. 1/1) • LXX/SXX (i.1 L01 or S01)
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
	3.4.1604	Updated Example
Role	admin	
Example		

```
switch (config) # show interfaces ib 1/1
IB1/1 state:
        Logical port state     : Down
        Physical port state    : Polling
        Current line rate      : -
        Supported speeds       : sdr, ddr, qdr, fdr, edr
        Speed                  : -
        Supported widths       : 1X, 4X
        Width                  : 4X
        Max supported MTUs     : 4096
        MTU                    : 256
        VL capabilities        : VL0 - VL7
        Operational VLs        : VL0 - VL7
        Description            :
        Phy-profile            : high-speed-ber
        Width reduction mode   :

        RX bytes               : 0
        RX packets             : 0
        RX errors              : 0
        Symbol errors          : 0
        VL15 dropped packets   : 0

        TX bytes               : 0
        TX packets             : 0
        TX wait                : 0
        TX discarded packets   : 0
switch (config) #
```

Related Commands	
Notes	

show interfaces ib status

show interfaces ib [<inf>] status

Displays the status, speed and negotiation mode of the specified interface.

Syntax Description	internal	Internal interfaces
	leaf-ports	filter to leaf-ports only
	inf	Interface number: <slot>/<port>
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.2.0500	
	3.4.1604	Updated Example
Role	admin	

Example

```
switch (config) # show interfaces ib status

Interface    Description                    Speed              Current line rate  Logical port state  Physical port state
---------    -----------                    ---------          -----------------  ------------------  -------------------
IB1/1                                       fdr                56.0 Gbps          Active              LinkUp
IB1/2                                       fdr                56.0 Gbps          Active              LinkUp
IB1/3                                       -                  -                  Down                Polling
IB1/4                                       -                  -                  Down                Polling
IB1/5                                       -                  -                  Down                Polling
IB1/6                                       -                  -                  Down                Polling
IB1/7                                       -                  -                  Down                Polling
IB1/8                                       -                  -                  Down                Polling
IB1/9                                       -                  -                  Down                Polling
IB1/10                                      -                  -                  Down                Polling
IB1/11                                      -                  -                  Down                Polling
....
switch (config) #
```

Related Commands	
Notes	

show interfaces ib internal

show interfaces ib internal [leaf | spine] [<slot/module/port>]

Displays running state for the internal ports of leafs or spines.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0500
Role	admin

Example	`switch (config) # show interfaces ib internal spine 1/1/4`
	`IB1/1/4 state:`
	`  Connected to slot/chip : 4/1`
	`  Connected to port  : 19`
	`  Connected device active: 1`
	`  Error state  : 0`
	`  Logical port state  : Active`
	`  Physical port state  : LinkUp`
	`  Current line rate  : 56.0 Gbps`
	`  Supported speeds  : sdr, ddr, qdr, fdr10, fdr`
	`  Speed  : fdr`
	`  Supported widths  : 1X, 4X`
	`  Width  : 4X`
	`  Max supported MTUs  : 4096`
	`  MTU  : 4096`
	`  VL capabilities  : VL0 - VL7`
	`  Operational VLs  : VL0 - VL7`
	`  Description  :`
	`  Phy-profile  : high-speed-ber`
	`  Width reduction mode  : Unknown`
	
	`switch (config) #`

Related Commands	
Notes	

show interfaces ib internal capabilities

show interfaces ib internal [leaf | spine] [<slot/module/port>] capabilities

Displays capabilities of internal leaf or spine interfaces.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0500
Role	admin

Example	`switch (config) # show interfaces ib internal leaf 1/1/26 capabilities`
	
	`IB1/1/26`
	`LLR: FDR10, FDR,`
	
	`switch (config) #`

Related Commands	
Notes	

show interfaces ib internal llr

show interfaces ib internal [leaf | spine] [<slot/module/port>] llr

Displays LLR state of internal leaf or spine interfaces.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0500
Role	admin

Example	`switch (config) # show interfaces ib internal leaf 1/1/26 llr`
	`Interface phy-profile LLR status`
	`IB1/1/26 high-speed-ber Active`
	`switch (config) #`

Related Commands	
Notes	

show interfaces ib internal status

show interfaces ib internal [leaf | spine] [<slot/module/port>] status

Displays detailed running state of internal leaf or spine interfaces.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0500
Role	admin

Example	`switch (config) # show interfaces ib internal leaf 1/1/26 status`
	
	`Interface Description Speed Current line rate Logical port state Physical port state`
	`--------- ----------- --------- ----------------- ------------------ -------------`
	`IB1/1/26 fdr 56.0 Gbps Active LinkUp`
	
	`switch (config) #`

Related Commands	
Notes	

show interfaces ib transceiver

show interfaces ib [<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 ib 1/1 transceiver`
	`Slot L01 port 13 state`
	`identifier : QSFP+`
	`cable/ module type : Passive copper, unequalized`
	`infiniband speeds : SDR , DDR , QDR`
	`vendor : Mellanox`
	`cable length : 2 m`
	`part number : MC2207130-002`
	`revision : B0`
	`serial number : AA051150077`
	`switch (config) #`	

Related Commands		
Notes	• For a full list of the supported cables and transceivers, please refer to the LinkX™ Cables and Transceivers webpage in Mellanox.com: http://www.mellanox.com/page/cables?mtag=cable_overview.	

show interface ib capabilities

show interface ib <inf> capabilities

Shows interface capabilities.

Syntax Description	inf	Slot/port (i.e. 1/1).
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.2.0500	
Role	admin	

Example	`switch (config) # show interfaces ib 1/1 capabilities`
	
	`Ib 1/1`
	`LLR: FDR10, FDR,`
	`switch (config)`	

Related Commands		
Notes		

When leaving an SM HA cluster, SM configuration is not saved on the node leaving the cluster. After leaving, the configuration is reset to its default values.

ib fabric import

ib fabric import <filename>

Imports a “snapshot” of fabric data. It retrieves fabric data from the following ibdiagnet output files: ibdiagnet.db, ibdiagnet.sm and ibdiagnet.pm.

Syntax Description	filename	The imported file. It is an output of the ibdiagnet tool that has previously run on any node connected to the fabric, and is assumed to be a zip file with a .gz or .tgz extension.
Default	N/A	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	
Example	`switch (config) # ib fabric import snapshot.tgz` `switch (config) #`	

Related Commands	show ib fabric nodes
Notes	• To display the results of this import, you may run “show ib fabric” commands (e.g., “show ib fabric nodes type switch”) • Imported data can be displayed as long as you do not run the command “ib fabric refresh”, which overwrites the imported data • The import command cannot execute without the ibdiagnet.db file

ib fabric monitor

ib fabric monitor
no ib fabric monitor

Enables fabric monitoring.
The no form of the command disables fabric monitoring.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.1400
Role	admin

Example	`switch (config) # ib fabric monitor`
	`switch (config) # show ib fabric monitor`
	`enable`
	`switch (config) #`

Related Commands	show ib fabric monitor
Notes	

ib fabric nodenames

ib fabric nodenames
no ib fabric nodenames

Imports fabric SysNames.
The no form of the command removes imported SysNames.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.1400
Role	admin
Example	`switch (config) # ib fabric nodenames` `switch (config) #`
Related Commands	
Notes	

ib fabric refresh

ib fabric refresh

Takes a “snapshot” of the current fabric data.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.1400
Role	admin
Example	`switch (config) # ib fabric refresh` `switch (config) #`
Related Commands	show ib fabric nodes
Notes	If the fabric is large, this command may take a long time to complete. this command requires license (LIC-fabric-inspector)

ib fabric transceiver-info

ib fabric transceiver-info enable
no ib fabric transceiver-info enable

Enables collection of active cable info.
The no form of the command disables collection of active cable info.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.1400
Role	admin

Example	`switch (config) # ib fabric transceiver-info enable`
	`switch (config) # show ib fabric transceiver-info enable`
	`enable`
	`switch (config) #`

Related Commands	show ib fabric nodes
Notes	

test ib fabric

test ib fabric [route]

Perform infiniband fabric test

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

Example

```
switch (config) # (config) # test ib fabric
% ----------
-I- Plugins load will be skipped

-----------------------------------------------
Discovery
-I- Discovering ... 1 nodes (1 Switches & 0 CA-s) discovered.
-I- Discovery finished successfully

-I- Duplicated GUIDs detection finished successfully

-I- Duplicated Nodes Descriptions detection finished successfully

-----------------------------------------------
Lids Check
-E- Lids Check finished with errors
-E- IBM-QA-Bay3:SX90Y3245/U1/P0 - Configured with ZERO lid

-----------------------------------------------
Links Check
-I- Links Check finished successfully

-----------------------------------------------
Subnet Manager
-I- SM Info retrieving finished successfully

-E- Subnet Manager Check finished with errors
-E- Not found master subnet manager in fabric

-----------------------------------------------
Port Counters
-I- Lids Check failed, no response for some MADs can occurred
-I- Ports counters retrieving finished successfully

-I- Ports counters value Check finished successfully

-I- Ports counters Difference Check will be skipped - pause time is zero
-----------------------------------------------
Nodes Information
-I- Lids Check failed, no response for some MADs can occurred
-W- Nodes Info retrieving finished with errors
-W- IBM-QA-Bay3:SX90Y3245/U1 - No response for MAD VSGeneralInfo

-I- FW Check finished successfully

-----------------------------------------------
Speed / Width checks
-I- Link Speed Check (Compare to supported link speed)
-I- Links Speed Check finished successfully

-I- Link Width Check (Compare to supported link width)
-I- Links Width Check finished successfully

-----------------------------------------------
Summary
-I- Stage                    Warnings   Errors     Comment
-I- Discovery                0          0
-I- Lids Check               0          1
-I- Links Check              0          0
-I- Subnet Manager           0          1
-I- Port Counters            0          0
-I- Nodes Information        1          0
-I- Speed / Width checks     0          0
...
switch (config) #
```

Related Commands
Notes

show ib fabric connections

show ib fabric connections [attrib <speed/width>] [details] [type]

Displays the ib fabric connections with optional relevant filter.

Syntax Description	attrib <speed/width>	Attribute of connection to filter on.
	details	Displays details info.
	type	Filter connections by type. • sw-2-sw-any - Any sort of switch to switch connection • sw-2-sw-int - Internal switch to switch connection • sw-2-sw-ext - External switch to switch connection • sw-2-ca - Switch to host connection • ca-2-ca - Host to host connection
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
Role	admin	

Example	`switch (config) # show ib fabric connections`
	`PORT-1 PORT-2 DESCRIPTION`
	`00:08:F1:00:01:08:B5:C0-0001 00:08:F1:05:00:20:2F:7B-0035 Active 4X @ 5.0 Gbps mtu=4096 VL0`
	`00:02:C9:03:00:61:FA:20-0001 00:08:F1:05:00:20:2F:7B-0011 Active 4X @ 10 Gbps mtu=4096 VL0, VL1`
	`00:02:C9:03:00:61:FA:30-0002 00:08:F1:05:00:20:2F:7B-0013 Active 4X @ 10 Gbps mtu=4096 VL0, VL1`
	`00:02:C9:03:00:61:FA:30-0001 00:08:F1:05:00:20:2F:7B-0014 Active 4X @ 10 Gbps mtu=4096 VL0, VL1`
	`00:02:C9:03:00:5D:30:72-0004 00:08:F1:05:00:20:2F:7B-0017 Active 4X @ 10 Gbps mtu=4096 VL0 - VL7`
	`00:02:C9:03:00:5D:30:72-0001 00:08:F1:05:00:20:2F:7B-0034 Active 4X @ 10 Gbps mtu=4096 VL0 - VL7`
	`00:02:C9:03:00:30:95:90-0001 00:02:C9:03:00:5D:D7:B0-0003 Active 4X @ 10 (FDR10) mtu=2048 VL0 - VL7`
	`00:02:C9:03:00:4A:E6:FE-0001 00:02:C9:03:00:5D:D7:B0-0007 Active 4X @ 10 Gbps mtu=2048 VL0 - VL7`
	`00:02:C9:03:00:30:95:A0-0001 00:02:C9:03:00:5D:D7:B0-0008 Active 4X @ 10 (FDR10) mtu=2048 VL0 - VL7`
	`00:02:C9:03:00:2E:E3:F0-0001 00:02:C9:03:00:5D:D7:B0-0011 Active 4X @ 10 (FDR10) mtu=2048 VL0 - VL7`
	`switch (config) #`	

Related Commands		
Notes		

show ib fabric messages

show ib fabric messages

Displays the InfiniBand fabric error and warning messages.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin

Example	`switch (config) # show ib fabric messages`
	`Warning Invalid(0x02) LinkWidthSupported`
	`  port 00:02:C9:03:00:30:95:90-0001`
	
	`Warning Invalid(0x02) LinkWidthSupported`
	`  port 00:02:C9:03:00:30:95:A0-0001`
	`Error   Internal SXX506 map error L02-19 should be S01/U1.7, not S01-10(L02/U1.22)`
	`  port 00:02:C9:03:00:49:7D:C0-0019`
	`  port 00:02:C9:03:00:5D:30:70-0010`
	
	`Error   Internal SXX506 map error L02-20 should be S01/U1.8, not S01-7(L02/U1.19)`
	`  port 00:02:C9:03:00:49:7D:C0-0020`
	`  port 00:02:C9:03:00:5D:30:70-0007`
	`switch (config) #`

Related Commands	
Notes	

show ib fabric monitor

show ib fabric monitor [<type>]

Displays the InfiniBand fabric monitor admin state and statistics count.

Syntax Description	type	• active-links - Displays number of active point-to-point links • active-ports - Displays number of active ports in subnet • host-ports - Displays number of CA ports in subnet • nodes - Displays number of active IB chips in subnet • snapshot-time - Date/time of this snapshot • switches - Displays number of switches in subnet • systems - Displays number of active systems in subnet • unique-GUIDs - Displays total number of unique GUIDs on fabric • warnings - Displays number of topology warnings issued
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
Role	admin	

Example	`switch (config) # show ib monitor active-links`
	`17`
	`switch (config) # show ib monitor`
	`enable`
	`switch (config) #`	

Related Commands		
Notes		

show ib fabric node

show ib fabric node <system-guid> [ports]

Displays InfiniBand fabric info on one node.

Syntax Description	system-guid	The node GUID.
	ports	Displays the info on the ports on this node.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
Role	admin	

Example

```
switch (config) # show ib fabric node 00:02:C9:03:00:5D:D7:B0 ports
System - switch node 00:02:C9:03:00:5D:D7:B0 Node details
System GUID     00:02:C9:03:00:5D:D7:B0
  Type            SW SX60XX standalone PCI 51000:713
  Ports           36
  Cable support   Supported
  PCI Device ID   51000
  PCI Vendor ID   0x0002c9
  Base version    1
  Class verson    1
  Revision        161
  Partition cap   8
  Descriptions    MF0;l-supp-SX6036:SX60XX/U1

Type     Port                            Desc               State    Rate
SW       00:02:C9:03:00:5D:D7:B0-0000    Switch port 0       Link Up  10
Gbps
SW       00:02:C9:03:00:5D:D7:B0-0001    Port 1              Polling  Up
to 40 Gbps
SW       00:02:C9:03:00:5D:D7:B0-0002    Port 2              Polling  Up
to 40 Gbps
SW       00:02:C9:03:00:5D:D7:B0-0003    Port 3              Link Up  41
Gbps
SW       00:02:C9:03:00:5D:D7:B0-0004    Port 4              Polling  Up
to 40 Gbps
SW       00:02:C9:03:00:5D:D7:B0-0005    Port 5              Polling  Up
to 40 Gbps
SW       00:02:C9:03:00:5D:D7:B0-0006    Port 6              Polling  Up
to 40 Gbps
switch (config) #
```

Related Commands	
Notes	

show ib fabric nodes

show ib fabric nodes [cable <cable-options>] [role <role-options>] [type <system-type>]

Displays InfiniBand fabric info on all nodes with filtering options.

Syntax Description	cable-options	Filters the list by cable type: • errors - Node with cable errors • no-errors - Node with no cable errors • supports - Node support active cables • no-support - Node does not support active cables
	role-options	Filters the list by role: • multi-chip - Systems with more than 1 nodes • single-chip - Systems with 1 node • leaf - Leaf node • spine - Spine node • <system> - Any supported system
	system-type	Filters the list by system type: • switch - Switches only • host - Hosts only • router - Routers only • unknown - Unknowns systems only
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
Role	admin	

Example	`switch (config) # show ib fabric nodes`
	`System name/GUID Type Node GUID Description`
	`00:02:C9:03:00:5C:F7:20 SW 00:02:C9:03:00:5C:F7:20 PCI 51000:713`
	`00:02:C9:03:00:09:DA:BD CA 00:02:C9:03:00:09:DA:BA PCI 26428:713`
	`00:02:C9:03:00:09:28:17 CA 00:02:C9:03:00:09:28:14 PCI 26428:713`
	`00:02:C9:03:00:5C:6E:00 SW 00:02:C9:03:00:5C:6E:00 PCI 51000:713`
	`switch (config) #`	

Related Commands		
Notes		

show ib fabric port

show ib fabric port <port-guid>

Displays InfiniBand fabric info on one port in the fabric.

Syntax Description	port-guid The port GUID.
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin

Example	`switch (config) # show ib fabric port 00:02:C9:03:00:5C:6E:00-0034`
	`SXCA07156 00:02:C9:03:00:5C:6E:00 port 00:02:C9:03:00:5C:6E:00-0034`
	`  Type  SW  Port state  Polling`
	`  Speed  2.5 Gbps  Supported speeds  2.5 / 5 /`
	`10 Gbps`
	`  Width  4X  Supported widths  1X, 4X`
	`  Operational VLs  VL0 - VL7  VL capabilities  VL0 - VL7`
	`  Port GUID  NA  System`
	`GUID  02:C9:03:00:5C:6E:00  MTU  4096`
	`  Max supported MTUs  4096`
	`  VL arbitration high  8  VL Arbitration low  8`
	`  VL high limit  4  VL stall count  7`
	`  Has errors  false  Has traffic  false`
	
	`switch (config) #`

Related Commands	
Notes	

show ib fabric ports

show ib fabric ports [attrib <attrib-options>] [data <data-options>] [errors <errors-options>] [sm <sm-options>] [state <state-options>] [type <port-type-options>]

Displays InfiniBand fabric info on all ports with filtering options.

Syntax Description	attrib-options	Filters the speed and width.
	data-options	Filters port by data transfer counts: • none - No data • any - Any data • lots - High rate of data • little - Low rate of data
	errors-options	Filters port by error counts: • none- No errors • any - Any errors • symbol - Any symbol errors • recv - Any receive errors • sym-or-recv - Any symbol or receive errors • cable - Any cable errors
	sm-options	Filters port by SM running states: • active - Has an active SM • none - Does not have an SM • master - Has master SM • standby - Has a standby SM
	state-options	Filters port by port state: • linkup - Link up state • polling - Polling state • unusual - Any unusual state • normal - Link up or polling state
	port-type-options	Filters port by port type: • switch-any-port - All switch ports • switch-port0 - Switch port 0 only • switch-not-P0 - Switch ports except 0 • switch-int - Internal switch ports • switch-ext - External switch ports • port-has-lid - CA or switch port 0 • has-cable-info - Port has an active cable • has-no-cable-info - No active cable on port • host - Host ports • router - Router ports • has-valid-LID - Ports with valid LIDs • invalid-LID - Ports with invalid LIDs • unknown - Unknown ports
Default		
Configuration Mode	Any Command Mode	
History	3.1.1400	

Role	admin

Example	`switch (config) # show ib fabric ports`
	`00:02:C9:03:00:5C:F7:20    SW       00:02:C9:03:00:5C:F7:20-0000`
	`Switch port 0       Link Up  10 Gbps`
	`00:02:C9:03:00:5C:F7:20    SW      00:02:C9:03:00:5C:F7:20-0001    Port`
	`1              Link Up  40 Gbps`
	`00:02:C9:03:00:5C:F7:20    SW      00:02:C9:03:00:5C:F7:20-0002    Port`
	`2              Polling  Up to 40 Gbps`
	`00:02:C9:03:00:5C:F7:20    SW      00:02:C9:03:00:5C:F7:20-0003    Port`
	`3              Link Up  40 Gbps`
	`00:02:C9:03:00:5C:F7:20    SW      00:02:C9:03:00:5C:F7:20-0004    Port`
	`4              Polling  Up to 40 Gbps`
	`00:02:C9:03:00:5C:F7:20    SW      00:02:C9:03:00:5C:F7:20-0005    Port`
	`5              Polling  Up to 40 Gbps`
	`00:02:C9:03:00:5C:F7:20    SW      00:02:C9:03:00:5C:F7:20-0006    Port`
	`6              Polling  Up to 40 Gbps`
	`00:02:C9:03:00:5C:F7:20    SW      00:02:C9:03:00:5C:F7:20-0007    Port`
	`7              Polling  Up to 40 Gbps`
	`00:02:C9:03:00:5C:F7:20    SW      00:02:C9:03:00:5C:F7:20-0008    Port`
	`8              Polling  Up to 40 Gbps`
	`00:02:C9:03:00:5C:F7:20    SW      00:02:C9:03:00:5C:F7:20-0009    Port`
	`9              Polling  Up to 40 Gbps`
	`00:02:C9:03:00:5C:F7:20    SW      00:02:C9:03:00:5C:F7:20-0010    Port`
	`10             Polling  Up to 40 Gbps`
	`switch (config) #`

Related Commands	
Notes	

show ib fabric system

show ib fabric system <system-guid> [nodes | ports]

Displays InfiniBand fabric info on a specific system.

Syntax Description	system-guid	The system GUID.
	nodes	Adds list of nodes information.
	ports	Adds list of ports information.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
Role	admin	

Example	`switch (config) # show ib fabric system 00:02:C9:03:00:5C:F7:20 nodes`
	`System - 00:02:C9:03:00:5C:F7:20`
	`  Model  SXCA07156`
	`  Revision Rev  Rev 1`
	`  System  36 port SW`
	`  Element count  1`
	`  Description  BX900S1P00355-CB5`
	
	`Node GUID  Role  Ports  Type  Descrpiton`
	`00:02:C9:03:00:5C:F7:20  standalone  36  SW  PCI 51000:713`
	`switch (config) #`	

Related Commands		
Notes		

show ib fabric sys

show ib fabric sys [config <role-options>] [type <system-type>]

Displays ib fabric info on all systems with filtering options.

Syntax Description	role-options	Filters the list by role: • multi-chip - Systems with more than 1 nodes • single-chip - Systems with 1 node • <system> - Any supported system
	system-type	Filters the list by system type: • switch - Switches only • host - Hosts only • router - Routers only • unknown - Unknowns systems only
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
Role	admin	

Example	`switch (config) # show ib fabric sys`
	`00:02:C9:03:00:5C:F7:20  SXCA07156  36 port SW 1 node`
	`00:02:C9:03:00:09:DA:BD  2 port host 1 node`
	`00:02:C9:03:00:09:28:17  2 port host 1 node`
	`00:02:C9:03:00:5C:6E:00  SXCA07156  36 port SW 1 node`
	`switch (config) #`	

Related Commands		
Notes		

show ib fabric transceiver-info

show ib fabric transceiver-info enable

Displays the admin state of the InfiniBand fabric transceiver info.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.1400
Role	admin

Example	`switch (config) # show ib fabric transceiver-info enable`
	`enable`
	`switch (config) #`

Related Commands	show ib fabric nodes
Notes	If enabled, transceiver info will be gathered by the InfiniBand fabric.

Appendix A: Enhancing System Security According to NIST SP 800-131A

A.1 Overview

This appendix describes how to enhance the security of a system in order to comply with the NIST SP 800-131A standard. This standard is a document which defines cryptographically "acceptable" technologies. This document explains how to protect against possible cryptographic vulnerabilities in the system by using secure methods. Because of compatibility issues, this security state is not the default of the system and it should be manually set.

Some protocols, however, cannot be operated in a manner that complies with the NIST SP 800-131A standard.

A.2 Web Certificate

Mellanox supports signature generation of sha256WithRSAEncryption, sha1WithRSAEncryption self-signed certificates, and importing certificates as text in PEM format.

➢ ***To configure a default certificate:***

Step 1. Create a new sha256 certificate. Run:

```
switch (config) # crypto certificate name <cert name> generate self-signed hash-algorithm
sha256
```

For more details and parameters refer to the command crypto certificate name in the MLNX-OS User Manual.

Step 2. Show crypto certificate detail. Run:

```
switch (config) # show crypto certificate detail
```

Search for "signature algorithm" in the output.

Step 3. Set this certificate as the default certificate. Run:

```
switch (config) # crypto certificate default-cert name <cert name>
```

➢ ***To configure default parameters and create a new certificate:***

Step 1. Define the default hash algorithm. Run:

```
switch (config) # crypto certificate generation default hash-algorithm sha256
```

Step 2. Generate a new certificate with default values. Run:

```
switch (config) # crypto certificate name <cert name> generate self-signed
```

When no options are selected, the generated certificate uses the default values for each field.

To test strict mode connect to the WebUI using HTTPS and get the certificate. Search for "signature algorithm".

There are other ways to configure the certificate to sha256. For example, it is possible to use `certificate generation default hash-algorithm` and then regenerate the certificate using these default values. Please refer to the MLNX-OS User Manual for further details.

It is recommended to delete browsing data and previous certificates before retrying to connect to the WebUI.

Make sure not to confuse "signature algorithm" with "Thumbprint algorithm".

A.3 Code Signing

Code signing is used to verify that the data in the image is not modified by any third-party. MLNX-OS supports signing the image files with SHA256, RSA2048 using GnuPG.

Strict mode is operational by default.

A.4 SNMP

SNMPv3 supports configuring username, authentication keys and privacy keys. For authentication keys it is possible to use MD5 or SHA. For privacy keys AES or DES are to be used.

- ***To configure strict mode, create a new user with HMAC-SHA1-96 and AES-128. Run:***

```
switch (config) # snmp-server user <username> v3 auth sha <password1> priv aes-128 <pass-
word2>
```

- ***To verify the user in the CLI, run:***

```
switch (config) # show snmp user
```

To test strict mode, configure users and check them using the CLI, then run an SNMP request with the new users.
For more information please refer to the MLNX-OS User Manual.

SNMPv1 and SNMPv2 are not considered to be secure. To run in strict mode, only use SNMPv3.

A.5 SSH

The SSH server on the switch by default uses secure and unsecure ciphers, message authentication code (MAC), key exchange methods, and public key algorithm. When configuring SSH server to strict mode, the aforementioned security methods only use approved algorithms as detailed in the NIST 800-181A specification and the user can connect to the switch via SSH in strict mode only.

➢ ***To enable strict security mode, run:***

```
switch (config) # ssh server security strict
```

The no form of the command disables strict security mode.

Make sure to configure the SSH server to work with minimum version 2 since 1 is vulnerable to security breaches.

➢ ***To configure min-version to strict mode, run:***

```
switch (config) # ssh server min-version 2
```

Once this is done, the user cannot revert back to minimum version 1.

A.6 HTTPS

By default, Mellanox switch supports HTTPS encryption using TLS1.0 up to TLS1.2. To work in strict mode you must configure the system to use TLS1.2. Working in TLS1.2 mode also bans MD5 ciphers which are not allowed per NIST 800-131a. In strict mode, the switch supports encryption with TLS1.2 only with the following supported ciphers:

- RSA_WITH_AES_128_CBC_SHA256
- RSA_WITH_AES_256_CBC_SHA256
- DHE_RSA_WITH_AES_128_CBC_SHA256
- DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

➢ ***To enable all encryption methods, run:***

```
switch (config) # web https ssl ciphers all
```

➢ ***To enable only TLS ciphers (enabled by default), run:***

```
switch (config) # web https ssl ciphers TLS
```

- ***To enable HTTPS strict mode, run:***

```
switch (config) # web https ssl ciphers TLS1.2
```

- ***To verify which encryption methods are used, run:***

```
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: TLS1.2
 HTTPS certificate name: default-cert
 Listen enabled: yes
 No Listen Interfaces.

 Inactivity timeout: disabled
 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)#
```

On top of enabling HTTPS, to prevent security breaches HTTP must be disabled.

- ***To disable HTTP, run:***

```
switch (config)# no web http enable
```

A.7 LDAP

By default, Mellanox switch supports LDAP encryption SSL version 3 or TLS1.0 up to TLS1.2. The only banned algorithm is MD5 which is not allowed per NIST 800-131a. In strict mode, the switch supports encryption with TLS1.2 only with the following supported ciphers:

- DHE-DSS-AES128-SHA256
- DHE-RSA-AES128-SHA256
- DHE-DSS-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-DSS-AES256-SHA256
- DHE-RSA-AES256-SHA256
- DHE-DSS-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- ECDH-ECDSA-AES128-SHA256

- ECDH-RSA-AES128-SHA256
- ECDH-ECDSA-AES128-GCM-SHA256
- ECDH-RSA-AES128-GCM-SHA256
- ECDH-ECDSA-AES256-SHA384
- ECDH-RSA-AES256-SHA384
- ECDH-ECDSA-AES256-GCM-SHA384
- ECDH-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- AES128-SHA256
- AES128-GCM-SHA256
- AES256-SHA256
- AES256-GCM-SHA384

➢ ***To enable LDAP strict mode, run:***

```
switch (config) # ldap ssl mode {start-tls | ssl}
```

Both modes operate using SSL. The different lies in the connection initialization and the port used.

➢ ***To enable all encryption methods (enabled by default), run:***

```
switch (config) # ldap ssl ciphers TLS1.2
```

➢ ***To verify which encryption methods are used, run:***

```
switch (config)# show ldap
User base DN : ou=People,dc=test,dc=com
User search scope : subtree
Login attribute : uid
Bind DN : cn=manager,dc=test,dc=com
Bind password : ********
Group base DN :
Group attribute : member
LDAP version : 3
Referrals : yes
Server port : 389 (not active)
Search Timeout : 5
```

```
Bind Timeout : 5
SSL mode : ssl
Server SSL port : 636
SSL ciphers : TLS1.2
SSL cert verify : yes
SSL ca-list : default-ca-list

LDAP servers:
1: 10.134.47.5
switch (config)#
```

Please make sure that “(not active)” does not appear adjacent to the line “SSL ciphers”.

A.8 Password Hashing

To compile with NIST 800-131a, Mellanox switches support password encryption with SHA512 algorithm.

- ***To see the password encryption used, run:***

```
switch (config)# show usernames
USERNAME  FULL NAME             CAPABILITY   ACCOUNT STATUS
admin     System Administrator  admin        No password required for login
monitor   System Monitor        monitor      Password set (SHA512)
xmladmin  XML Admin User        admin        No password required for login
xmluser   XML Monitor User      monitor      No password required for login
```

Using default usernames and passwords or using usernames without passwords is highly not recommended.

When moving to strict mode, the password of each user must be reconfigured to a non-default value using the CLI command `username`.

For example, if you have a user ID “myuser” whose password is hashed with MD5, this user must be recreated manually using the command “username myuser password mypassword”. The password then is automatically hashed using SHA512.

The following output demonstrates the example above:

```
switch (config)# show usernames
USERNAME  FULL NAME             CAPABILITY  ACCOUNT STATUS
admin     System Administrator admin        No password required for login
myuser    System Monitor       monitor      Password set (MD5)
switch (config)# username myuser password mypassword
switch (config)# show usernames
USERNAME  FULL NAME             CAPABILITY  ACCOUNT STATUS
admin     System Administrator admin        No password required for login
myuser    System Monitor       monitor      Password set (SHA512)
```

Appendix B: Security Vulnerabilities and Exposures

Table 18 presents the status of common vulnerabilities and security exposures that may affect MLNX-OS.

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-1999-0517	Not vulnerable: Requires strict mode	An SNMP community name is the default (e.g. public), null, or missing.	3.4.0000
CVE-2006-0175	Not vulnerable	Directory traversal vulnerability in scp for OpenSSH before 3.4p1 allows remote malicious servers to overwrite arbitrary files. NOTE: this may be a rediscovery of CVE-2000-0992.	3.3.3500
CVE-2006-1653	N/A	The default configuration for OpenSSH enables AllowTcpForwarding, which could allow remote authenticated users to perform a port bounce, when configured with an anonymous access program such as AnonCVS.	N/A
CVE-2006-2760	N/A	sshd in OpenSSH 3.5p1, when PermitRootLogin is disabled, immediately closes the TCP connection after a root login attempt with the correct password, but leaves the connection open after an attempt with an incorrect password, which makes it easier for remote attackers to guess the password by observing the connection state, a different vulnerability than CVE-2003-0190. NOTE: it could be argued that in most environments, this does not cross privilege boundaries without requiring leverage of a separate vulnerability.	N/A
CVE-2005-2797	N/A	OpenSSH 4.0, and other versions before 4.2, does not properly handle dynamic port forwarding ("-D" option) when a listen address is not provided, which may cause OpenSSH to enable the GatewayPorts functionality.	N/A
CVE-2005-2798	Not vulnerable	sshd in OpenSSH before 4.2, when GSSAPIDelegateCredentials is enabled, allows GSSAPI credentials to be delegated to clients who log in using non-GSSAPI methods, which could cause those credentials to be exposed to untrusted users or hosts.	3.3.3500
CVE-2006-0225	N/A	scp in OpenSSH 4.2p1 allows attackers to execute arbitrary commands via filenames that contain shell metacharacters or spaces, which are expanded twice.	N/A
CVE-2006-4924	Not vulnerable	sshd in OpenSSH before 4.4, when using the version 1 SSH protocol, allows remote attackers to cause a denial of service (CPU consumption) via an SSH packet that contains duplicate blocks, which is not properly handled by the CRC compensation attack detector.	3.4.0000

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2006-4925	N/A	packet.c in ssh in OpenSSH allows remote attackers to cause a denial of service (crash) by sending an invalid protocol sequence with USERAUTH_SUCCESS before NEWKEYS, which causes newkeys[mode] to be NULL.	N/A
CVE-2006-5051	N/A	Signal handler race condition in OpenSSH before 4.4 allows remote attackers to cause a denial of service (crash), and possibly execute arbitrary code if GSSAPI authentication is enabled, via unspecified vectors that lead to a double-free.	N/A
CVE-2006-5052	N/A	Unspecified vulnerability in portable OpenSSH before 4.4, when running on some platforms, allows remote attackers to determine the validity of usernames via unknown vectors involving a GSSAPI "authentication abort."	N/A
CVE-2006-5229	N/A	OpenSSH portable 4.1 on SUSE Linux, and possibly other platforms and versions, and possibly under limited configurations, allows remote attackers to determine valid usernames via timing discrepancies in which responses take longer for valid usernames than invalid ones, as demonstrated by sshtime. NOTE: as of 20061014, it appears that this issue is dependent on the use of manually-set passwords that causes delays when processing /etc/shadow due to an increased number of rounds.	N/A
CVE-2006-5794	Not vulnerable	Unspecified vulnerability in the sshd Privilege Separation Monitor in OpenSSH before 4.5 causes weaker verification that authentication has been successful, which might allow attackers to bypass authentication. NOTE: as of 20061108, it is believed that this issue is only exploitable by leveraging vulnerabilities in the unprivileged process, which are not known to exist.	3.4.0000
CVE-2007-0726	N/A	The SSH key generation process in OpenSSH in Apple Mac OS X 10.3.9 and 10.4 through 10.4.8 allows remote attackers to cause a denial of service by connecting to the server before SSH has finished creating keys, which causes the keys to be regenerated and can break trust relationships that were based on the original keys.	N/A
CVE-2007-2243	N/A	OpenSSH 4.6 and earlier, when ChallengeResponseAuthentication is enabled, allows remote attackers to determine the existence of user accounts by attempting to authenticate via S/KEY, which displays a different response if the user account exists, a similar issue to CVE-2001-1483.	N/A

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2007-2768	N/A	OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.	N/A
CVE-2007-3102	N/A	Unspecified vulnerability in the linux_audit_record_event function in OpenSSH 4.3p2, as used on Fedora Core 6 and possibly other systems, allows remote attackers to write arbitrary characters to an audit log via a crafted username. NOTE: some of these details are obtained from third party information.	N/A
CVE-2007-4654	N/A	Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.	N/A
CVE-2007-4752	Not vulnerable	ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11 cookie instead, which allows attackers to violate intended policy and gain privileges by causing an X client to be treated as trusted.	3.4.0000
CVE-2007-5715	N/A	DenyHosts 2.6 processes OpenSSH sshd "not listed in AllowUsers" log messages with an incorrect regular expression that does not match an IP address, which might allow remote attackers to avoid detection and blocking when making invalid login attempts with a username not present in AllowUsers, as demonstrated by the root username, a different vulnerability than CVE-2007-4323.	N/A
CVE-2007-6415	N/A	scponly 4.6 and earlier allows remote authenticated users to bypass intended restrictions and execute arbitrary code by invoking scp, as implemented by OpenSSH, with the -F and -o options.	N/A
CVE-2008-1483	Not vulnerable	OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded X connections by causing ssh to set DISPLAY to :10, even when another process is listening on the associated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs.	3.4.0000
CVE-2008-1657	N/A	OpenSSH 4.4 up to versions before 4.9 allows remote authenticated users to bypass the sshd_config ForceCommand directive by modifying the .ssh/rc session file.	N/A

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2008-3234	Only affects OpenSSH version 4.x. MLNX-OS uses 3.8.1p1.	sshd in OpenSSH 4 on Debian GNU/Linux, and the 20070303 OpenSSH snapshot, allows remote authenticated users to obtain access to arbitrary SELinux roles by appending a :/ (colon slash) sequence, followed by the role name, to the username.	N/A
CVE-2008-3259	N/A	OpenSSH before 5.1 sets the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled, which allows local users on some platforms to hijack the X11 forwarding port via a bind to a single IP address, as demonstrated on the HP-UX platform.	N/A
CVE-2008-3844	N/A	Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.	N/A
CVE-2008-4109	Not vulnerable	A certain Debian patch for OpenSSH before 4.3p2-9etch3 on etch; before 4.6p1-1 on sid and lenny; and on other distributions such as SUSE uses functions that are not async-signal-safe in the signal handler for login timeouts, which allows remote attackers to cause a denial of service (connection slot exhaustion) via multiple login attempts. NOTE: this issue exists because of an incorrect fix for CVE-2006-5051.	3.4.0000
CVE-2008-5161	Not vulnerable	Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.	3.4.0000

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2009-2904	N/A	A certain Red Hat modification to the ChrootDirectory feature in OpenSSH 4.8, as used in sshd in OpenSSH 4.3 in Red Hat Enterprise Linux (RHEL) 5.4 and Fedora 11, allows local users to gain privileges via hard links to setuid programs that use configuration files within the chroot directory, related to requirements for directory ownership.	N/A
CVE-2010-4478	N/A	OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.	N/A
CVE-2010-4755	N/A	The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.	N/A
CVE-2010-5298	Not vulnerable	Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.	3.4.0008
CVE-2011-0539	N/A	The key_certify function in usr.bin/ssh/key.c in OpenSSH 5.6 and 5.7, when generating legacy certificates using the -t command-line option in ssh-keygen, does not initialize the nonce field, which might allow remote attackers to obtain sensitive stack memory contents or make it easier to conduct hash collision attacks.	N/A
CVE-2011-3389	Not vulnerable	The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.	3.3.3500

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2011-3607	Not vulnerable	Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.	3.3.3500
CVE-2011-4317	Not vulnerable	The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.	3.3.3500
CVE-2011-4327	N/A	ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.	N/A
CVE-2011-5000	N/A	The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.	N/A
CVE-2012-0031	Not vulnerable	scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.	3.3.3500
CVE-2012-0053	Not vulnerable	protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.	3.3.3500

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2012-0814	Not vulnerable	The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.	3.3.3500
CVE-2012-2687	N/A	Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.	N/A
CVE-2012-4929	Not vulnerable	The TLS protocol 1.2 and earlier, as used in Mozilla Firefox, Google Chrome, Qt, and other products, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a “CRIME” attack.	3.3.3500
CVE-2013-7423	Not vulnerable	The send_dg function in resolv/res_send.c in GNU C Library (aka glibc or libc6) before 2.20 does not properly reuse file descriptors, which allows remote attackers to send DNS queries to unintended locations via a large number of request that trigger a call to the getaddrinfo function.	3.4.3000
CVE-2014-0195	Not vulnerable	The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.	3.4.0008
CVE-2014-0198	Not vulnerable	The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.	3.4.0008

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2014-0221	Not vulnerable	The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.	3.4.0008
CVE-2014-0224	Not vulnerable	OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.	3.4.1000
CVE-2014-0475	Not vulnerable	Multiple directory traversal vulnerabilities in GNU C Library (aka glibc or libc6) before 2.20 allow context-dependent attackers to bypass ForceCommand restrictions and possibly have other unspecified impact via a .. (dot dot) in a (1) LC_*, (2) LANG, or other locale environment variable.	3.4.3000
CVE-2014-1692	N/A	The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.	N/A
CVE-2014-2532	N/A	sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.	N/A
CVE-2014-3470	Not vulnerable	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.	3.4.0008
CVE-2014-3505	Not vulnerable	Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.	3.4.1000

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2014-3506	Not vulnerable	d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.	3.4.1000
CVE-2014-3507	Not vulnerable	Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.	3.4.1000
CVE-2014-3508	Not vulnerable	The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.	3.4.1000
CVE-2014-3509	Not vulnerable	Race condition in the ssl_parse_serverhello_tlsext function in t1_lib.c in OpenSSL 1.0.0 before 1.0.0n and 1.0.1 before 1.0.1i, when multithreading and session resumption are used, allows remote SSL servers to cause a denial of service (memory overwrite and client application crash) or possibly have unspecified other impact by sending Elliptic Curve (EC) Supported Point Formats Extension data.	3.4.1000
CVE-2014-3510	Not vulnerable	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.	3.4.1000
CVE-2014-3511	Not vulnerable	The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-middle attackers to force the use of TLS 1.0 by triggering ClientHello message fragmentation in communication between a client and server that both support later TLS versions, related to a "protocol downgrade" issue.	3.4.1000
CVE-2014-3513	Not vulnerable	Memory leak in d1_srtp.c in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.	3.4.1000

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2014-3566	Not vulnerable	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.	3.4.1000
CVE-2014-3567	Not vulnerable	Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.	3.4.1000
CVE-2014-3569	N/A	The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 0.9.8zc, 1.0.0o, and 1.0.1j does not properly handle attempts to use unsupported protocols, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unexpected handshake, as demonstrated by an SSLv3 handshake to a no-ssl3 application with certain error handling. NOTE: this issue became relevant after the CVE-2014-3568 fix.	N/A
CVE-2014-3570	Not vulnerable	The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.	3.4.3000
CVE-2014-3571	Not vulnerable	OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.	3.4.3000
CVE-2014-3572	Not vulnerable	The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.	3.4.3000
CVE-2014-6040	Not vulnerable	GNU C Library (aka glibc) before 2.20 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via a multibyte character value of "0xffff" to the iconv function when converting (1) IBM933, (2) IBM935, (3) IBM937, (4) IBM939, or (5) IBM1364 encoded data to UTF-8.	3.4.2300

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2014-6271	Not vulnerable	GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.	3.4.0008
CVE-2014-7817	Not vulnerable	The wordexp function in GNU C Library (aka glibc) 2.21 does not enforce the WRDE_NOCMD flag, which allows context-dependent attackers to execute arbitrary commands, as demonstrated by input containing "$((`...`))".	3.4.3000
CVE-2014-8176	Not vulnerable	The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.	3.4.3000
CVE-2014-8275	Not vulnerable	OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.	3.4.3000
CVE-2014-9293	Not vulnerable	The config_auth function in ntpd in NTP before 4.2.7p11, when an auth key is not configured, improperly generates a key, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.	3.4.1000
CVE-2014-9294	Not vulnerable	util/ntp-keygen.c in ntp-keygen in NTP before 4.2.7p230 uses a weak RNG seed, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.	3.4.1000

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2014-9295	Not vulnerable	Multiple stack-based buffer overflows in ntpd in NTP before 4.2.8 allow remote attackers to execute arbitrary code via a crafted packet, related to (1) the crypto_recv function when the Autokey Authentication feature is used, (2) the ctl_putdata function, and (3) the configure function.	3.4.1000
CVE-2014-9296	Not vulnerable	The receive function in ntp_proto.c in ntpd in NTP before 4.2.8 continues to execute after detecting a certain authentication error, which might allow remote attackers to trigger an unintended association change via crafted packets.	3.4.1000
CVE-2014-9297	N/A	This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided	3.4.3000
CVE-2015-0204	Not vulnerable	The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.	3.4.3000
CVE-2015-0205	Not vulnerable	The ssl3_get_cert_verify function in s3_srvr.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k accepts client authentication with a Diffie-Hellman (DH) certificate without requiring a CertificateVerify message, which allows remote attackers to obtain access without knowledge of a private key via crafted TLS Handshake Protocol traffic to a server that recognizes a Certification Authority with DH support.	3.4.3000
CVE-2015-0206	Not vulnerable	Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate records for the next epoch, leading to failure of replay detection.	3.4.3000
CVE-2015-0207	Not vulnerable	The dtls1_listen function in d1_lib.c in OpenSSL 1.0.2 before 1.0.2a does not properly isolate the state information of independent data streams, which allows remote attackers to cause a denial of service (application crash) via crafted DTLS traffic, as demonstrated by DTLS 1.0 traffic to a DTLS 1.2 server.	3.4.2008

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2015-0208	Not vulnerable	The ASN.1 signature-verification implementation in the rsa_item_verify function in crypto/rsa/rsa_ameth.c in OpenSSL 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted RSA PSS parameters to an endpoint that uses the certificate-verification feature.	3.4.2008
CVE-2015-0209	N/A	Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.	3.4.3000
CVE-2015-0235	Not vulnerable	Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka "GHOST."	3.4.2002
CVE-2015-0285	N/A	The ssl3_client_hello function in s3_clnt.c in OpenSSL 1.0.2 before 1.0.2a does not ensure that the PRNG is seeded before proceeding with a handshake, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by sniffing the network and then conducting a brute-force attack.	3.4.3000
CVE-2015-0286	Not vulnerable	The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature.	3.4.3000
CVE-2015-0287	Not vulnerable	The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.	3.4.3000
CVE-2015-0288	Not vulnerable	The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.	3.4.3000

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2015-0289	Not vulnerable	The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.	3.4.3000
CVE-2015-0290	Not vulnerable	The multi-block feature in the ssl3_write_bytes function in s3_pkt.c in OpenSSL 1.0.2 before 1.0.2a on 64-bit x86 platforms with AES NI support does not properly handle certain non-blocking I/O cases, which allows remote attackers to cause a denial of service (pointer corruption and application crash) via unspecified vectors.	3.4.2008
CVE-2015-0291	Not vulnerable	The sigalgs implementation in t1_lib.c in OpenSSL 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) by using an invalid signature_algorithms extension in the ClientHello message during a renegotiation.	3.4.2008
CVE-2015-0292	Not vulnerable	Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.	3.4.3000
CVE-2015-0293	Not vulnerable	The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.	3.4.3000
CVE-2015-1787	Not vulnerable	The ssl3_get_client_key_exchange function in s3_srvr.c in OpenSSL 1.0.2 before 1.0.2a, when client authentication and an ephemeral Diffie-Hellman ciphersuite are enabled, allows remote attackers to cause a denial of service (daemon crash) via a ClientKeyExchange message with a length of zero.	3.4.2008
CVE-2015-1789	Not vulnerable	The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.	3.4.3000

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2015-1790	Not vulnerable	The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_-doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.	3.4.3000
CVE-2015-1791	Not vulnerable	Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.	3.4.3000
CVE-2015-1792	Not vulnerable	The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.	3.4.3000
CVE-2015-1798	N/A	The symmetric-key feature in the receive function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p2 requires a correct MAC only if the MAC field has a nonzero length, which makes it easier for man-in-the-middle attackers to spoof packets by omitting the MAC.	3.4.3000
CVE-2015-1799	N/A	The symmetric-key feature in the receive function in ntp_proto.c in ntpd in NTP 3.x and 4.x before 4.2.8p2 performs state-variable updates upon receiving certain invalid packets, which makes it easier for man-in-the-middle attackers to cause a denial of service (synchronization loss) by spoofing the source IP address of a peer.	3.4.3000
CVE-2015-2808	Not vulnerable: Requires strict mode	The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.	3.4.1120

Table 18 - Common Vulnerabilities and Exposures

CVE	Vulnerability[1]	Description	Fixed in Version
CVE-2015-3456	Not vulnerable	The Floppy Disk Controller (FDC) in QEMU, as used in Xen 4.5.x and earlier and KVM, allows local guest users to cause a denial of service (out-of-bounds write and guest crash) or possibly execute arbitrary code via the (1) FD_CMD_READ_ID, (2) FD_CMD_DRIVE_SPECIFICATION_COMMAND, or other unspecified commands, aka VENOM. Though the VENOM vulnerability is also agnostic of the guest operating system, an attacker (or an attacker's malware) would need to have administrative or root privileges in the guest operating system in order to exploit VENOM.	3.4.3000
CVE-2015-4000	Not vulnerable	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.	3.4.3000
CVE-2015-5119	Not vulnerable	This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.	3.4.3000

1. Vulnerability may take the following three values:
   N/A – not relevant to MLNX-OS
   Not vulnerable – Mellanox products are protected against this vulnerability
   Not vulnerable: Requires strict mode – working in strict mode protects against this vulnerability

Appendix C: UI Changes in Version 3.4.2008

Relevant changes in the CLI in this section are marked in boldface.

In order to improve user interface and unify look and feel across all Mellanox switch platforms, MLNX-OS® versions 3.4.2008 and above introduce some changes in user interface.

C.1 Interface Addressing Change

Interface addressing in interface specific commands has changed in order to align the InfiniBand interface schema with that of Ethernet's, and to support the EDR director switch system which has 2 ASICs per leaf.

C.1.1 CLI Change

Interface referencing for director switches has become <slot/module/port> and their show command output text displays IB<slot/module/port>.

Before:

```
switch (config) # show interfaces ib L01/1
Slot L01 port 1 state
       Logical port state     : Initialize
       Physical port state    : LinkUp
       Current line rate      : 40.0 Gbps
       Supported speeds       : 2.5, 5.0, 10.0(QDR),
10.0(FDR10) or 14.0 Gbos rate
...
```

After:

```
switch (config) # show interfaces ib 1/1/1
IB1/1/1 state:
       Logical port state     : Initialize
       Physical port state    : LinkUp
       Current line rate      : 40.0 Gbps
       Supported speeds       : sdr, ddr, qdr, fdr10
...
```

Internal interface referencing for director switch systems has become as follows:

Before:

```
switch (config) # show interfaces ib internal S01/1
Slot S01 port 1 state
       Connected to slot/chip : 1/1
       Connected to port      : 19
       Connected device active: -
       Error state            : 0
       Logical port state     : Initialize
       Physical port state    : LinkUp
       Current line rate      : 40.0 Gbps
       Supported speeds       : .5, 5.0, 10.0(QDR),
10.0(FDR10) or 14.0 Gbos rate
...
```

After:

```
switch (config) # show interfaces ib internal spine 1/
1/1
IB1/1/1 state:
       Connected to slot/chip : 1/1
       Connected to port      : 19
       Connected device active: -
       Error state            : 0
       Logical port state     : Initialize
       Physical port state    : LinkUp
       Current line rate      : 40.0 Gbps
       Supported speeds       : sdr, ddr, qdr, fdr10
...
```

Interface show command output text on 1U switches has become IB<slot/port>.

Before:

```
switch (config) # show interfaces ib 1/1
Slot 1 port 1 state
        Logical port state     : Down
        Physical port state    : Polling
        Current line rate      : -
        Supported speeds       : 2.5, 5.0, 10.0(QDR),
10.0(FDR10) or 14.0 Gbos rate
...
```

After:

```
switch (config) # show interfaces ib 1/1
IB1/1 state:
        Logical port state     : Down
        Physical port state    : Polling
        Current line rate      : -
        Supported speeds       : sdr, ddr, qdr, fdr10,
fdr
...
```

C.1.2 MIB ifTable Change

The ifDescr column now displays interfaces in the syntax IB<slot/port>.

Figure 12: 1U MIB ifTable Before Screenshot

	ifIndex	ifDescr
1	1	lo
2	2	mgmt0
3	3	mgmt1
4	4	ib0
5	65	/SX/9
6	67	/SX/12
7	69	/SX/11
8	70	/SX/14
9	72	/SX/13
10	74	/SX/16
11	75	/SX/15
12	77	/SX/18
13	79	/SX/17
14	80	/SX/28

Figure 13: 1U MIB ifTable After Screenshot

	ifIndex	ifDescr
1	1	lo
2	2	mgmt0
3	3	mgmt1
4	4	ib0
5	65	IB1/5
6	69	IB1/6
7	70	IB1/7
8	75	IB1/8
9	79	IB1/9
10	80	IB1/13
11	85	IB1/12
12	89	IB1/11
13	91	IB1/10
14	97	IB1/4

For director switches the ifDescr column displays interfaces in the syntax IB<slot/module/port>.

Figure 14: Director Switch MIB ifTable Before Screenshot

	ifIndex	ifDescr
1	1	lo
2	2	mgmt0
3	4	ib0
4	1616	/L01/10
5	1618	/L01/7
6	1620	/L01/8
7	1621	/L01/5
8	1623	/L01/6
9	1625	/L01/3
10	1627	/L01/4
11	1629	/L01/1
12	1631	/L01/2
13	1648	/L01/9
14	1650	/L01/12

Figure 15: Director Switch MIB ifTable After Screenshot

	ifIn...	ifDescr
331	2389	IB1/1/5
332	2391	IB1/1/6
333	2393	IB1/1/3
334	2395	IB1/1/4
335	2397	IB1/1/1
336	2399	IB1/1/2
337	2416	IB1/1/9
338	2418	IB1/1/12
339	2420	IB1/1/11
340	2421	IB1/1/14
341	2423	IB1/1/13
342	2425	IB1/1/16
343	2427	IB1/1/15
344	2429	IB1/1/18

C.1.3 WebUI Ports Page Change

In the “Ports” page of the MLNX-OS® WebUI, the “Port number” field has been modified to reflect the change in the CLI. “Port number” now displays interfaces in the following syntax for director switches: <slot>/<module>/<port>.

C.2 Interface Speed Configuration Change

Interface speed configuration has changed in order to improve user experience when configuring InfiniBand speeds and to support additional permutations for setting allowed speeds.

C.2.1 CLI Change

Interface speed configuration commands accept any of the following speed name combinations: SDR; DDR; QDR; FDR10; FDR; EDR.

Commands with the old syntax, however, are still supported.

Before:

```
switch (config interface ib 1/1) # speed ?
1                       2.5 Gbps
3                       2.5 or 5.0 Gbps
5                       2.5 or 10.0(QDR) Gbps
7                       2.5, 5.0 or 10.0(QDR) Gbps
8                       10.0(FDR10) Gbps
13                      2.5, 10.0(QDR) or 10(FDR10) Gbps
15                      2.5, 5.0, 10.0(QDR) or 10.0(FDR10) Gbps
```

After:

```
switch (config interface ib 1/1) # speed ?
sdr                           10.0 Gbps rate on 4 lane width
ddr                           20.0 Gbps rate on 4 lane width
qdr                           40.0 Gbps rate on 4 lane width
fdr10                         40.0 Gbps rate on 4 lane width
fdr                           56.0 Gbps rate on 4 lane width
force                         Force a speed vector without the
sdr bit
```

Before:

```
switch (config interface ib 1/1) # speed ?
10                            10.0 Gbps rate on 4 lane width
100                           20.0 Gbps rate on 4 lane width
1000                          40.0 Gbps rate on 4 lane width
10000                         40.0 Gbps rate on 4 lane width
auto                          56.0 Gbps rate on 4 lane width
```

After:

```
switch (config interface ib 1/1) # speed ?
sdr                           10.0 Gbps rate on 4 lane width
ddr                           20.0 Gbps rate on 4 lane width
qdr                           40.0 Gbps rate on 4 lane width
fdr10                         40.0 Gbps rate on 4 lane width
fdr                           56.0 Gbps rate on 4 lane width
force                         Force a speed vector without the
sdr bit
```

```
switch (config interface ib 1/1) # speed
ddr     fdr     fdr10      force     qdr     sdr
switch (config interface ib 1/1) # speed sdr fdr qdr
switch (config interface ib 1/1) #
```

Show interface commands display speed names instead of the speed figures.

Before:

```
switch (config) # show interfaces ib L01/1
Slot L01 port 1 state:
        Logical port state     : Down
        Physical port state    : Polling
        Current line rate      : -
        Supported speeds       : 2.5, 5.0, 10.0(QDR),
10.0(FDR10) or 14.0 Gbps
...
```

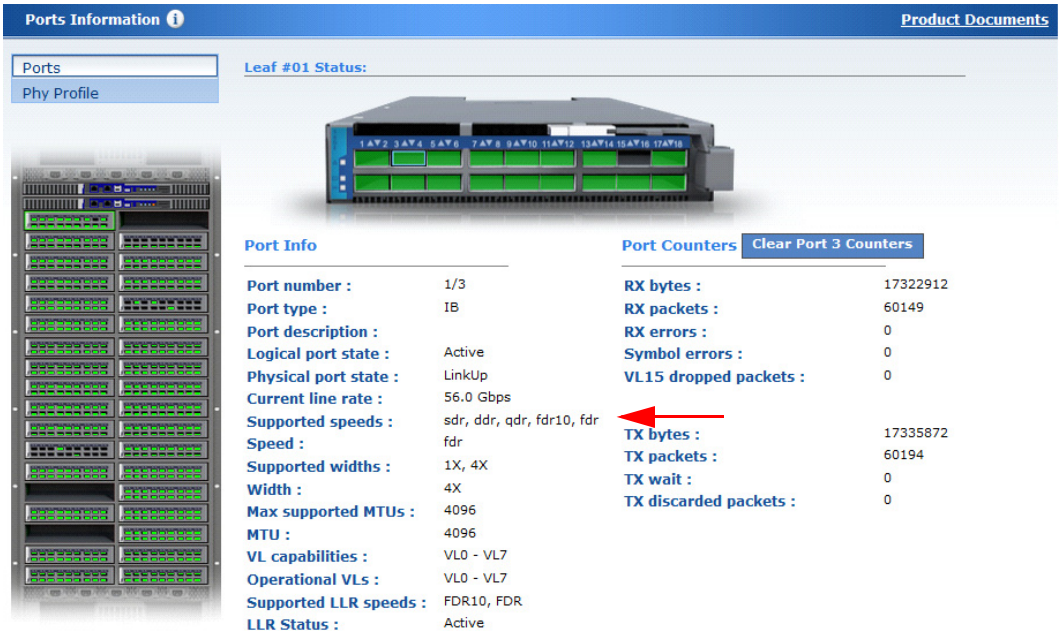
After:

```
switch (config) # show interfaces ib 1/1
IB1/1 state:
        Logical port state     : Down
        Physical port state    : Polling
        Current line rate      : -
       Supported speeds       : sdr, ddr, qdr, fdr10,
fdr
...
```

C.2.2 WebUI Change

In the Ports page of the MLNX-OS WebUI, the “Supported speeds” and “Speed” fields have been modified to reflect the change in the CLI. “Supported speeds” and “Speed” now display speed names instead of the speed figures.

Figure 16: Ports WebUI Page



C.3 IB SM Link Speed Change

IB SM link speed has changed to improve user experience when configuring InfiniBand interface speeds, to support additional permutations for setting allowed speeds, and to display clear default values and negotiation outputs.

IB SM link speed commands accept any of the following speed name combinations: SDR; DDR; QDR; FDR10; FDR; EDR.

Commands with the old syntax, however, are still supported.

Before:

```
switch (config) # ib sm force-link-speed ?
0   Do not modify switch assigned default value
1   Negotiate only 2.5 Gbps rate
3   Negotiate 2.5 or 5.0 Gbps rate
5   Negotiate 2.5 or 10.0 Gbps rate
7   Negotiate 2.5, 5.0, or 10.0 Gbps rate
13  Negotiate 2.5, 10.0(QDR) or 10.0(FDR19) Gbps
15  Negotiate 2.5, 5.0, 10.0(QDR) or 10.0(FDR10) Gbps
21  Negotiate 2.5, 10.0(QDR) or 14.0 Gbps
23  Negotiate 2.5, 5.0, 10.0(QDR) or 14.0 Gbps
29  Negotiate 2.5, 10.0(QDR), 10.0(FDR10) or 14.0 Gbps
31  Negotiate 2.5, 5.0, 10.0(QDR), 10.0(FDR10) or 14.0
Gbps
```

After:

```
switch (config) # ib sm force-link-speed ?
sdr                 10.0 Gbps rate on 4 lane width
ddr                 20.0 Gbps rate on 4 lane width
qdr                 40.0 Gbps rate on 4 lane width
fdr10               40.0 Gbps rate on 4 lane width
fdr                 56.0 Gbps rate on 4 lane width
edr                 100.0 Gbps rate on 4 lane width
```

The command “no ib sm force-link-speed” configures default speed.

Before:	After:
switch (config) # no ib sm force-link-speed switch (config) # show ib sm force-link-speed **15 (Negotiate 2.5, 5.0, 10.0(QDR) or 10.0(FDR10) Gbps)**	switch (config) # no ib sm force-link-speed switch (config) # show ib sm force-link-speed **Default: set to PortInfo:LinkSpeedSupported**

Show IB SM speed command displays negotiation as well as speed names.

Before:	After:
switch (config) # show ib sm force-link-speed **5 (Negotiate 2.5 or 10.0 Gbps rate)**	switch (config) # show ib sm force-link-speed **Negotiate: sdr, qdr**

The output of the command “show ib sm force-link-speed-ext”:

Before:	After:
switch (config) # show ib sm force-link-speed-ext **1 (Allow extended negotiation speeds with 14.0 Gbps rate)**	switch (config) # show ib sm force-link-speed-ext **Negotiate: fdr**

C.4 Multi-ASIC Support

Multi-ASIC support has been added to MLNX-OS in order to support the new EDR director switch systems whose leafs feature two ASICs per leaf, to improve MIB module indexing and better represent module hierarchy, to add an additional hierarchy level with an ASIC device to support more than one ASIC per module, and to add support to all sensors.

C.4.1 CLI Change

Added a new “Device” column to the output of the command “show guids”.

Before:

```
switch (config) # show guids
=============================================
SX module                          GUID
=============================================
SYSTEM                00:05:C9:03:00:42:D8:00
S01                   00:02:C9:03:00:84:3B:60
L17                   00:02:C9:03:00:84:3B:40
L18                   00:02:C9:03:00:84:3A:F0
S05                   00:02:C9:03:00:84:3B:70
L01                   00:02:C9:03:00:84:3B:80
L03                   00:02:C9:03:00:84:3B:90
L04                   00:02:C9:03:00:61:ED:00
L06                   00:02:C9:03:00:84:3B:A0
L09                   00:02:C9:03:00:84:3B:50
L11                   00:02:C9:03:00:84:3B:10
L13                   00:02:C9:03:00:61:EC:B0
L15                   00:02:C9:03:00:66:C9:B0
L16                   00:02:C9:03:00:66:C9:60
...
```

After:

```
switch (config) # show guids
=============================================
Module    Device      GUID
=============================================
SYSTEM    -           00:05:C9:03:00:42:D8:00
S01       SX          00:02:C9:03:00:84:3B:60
S02       SX          00:02:C9:03:00:84:3B:40
S03       SX          00:02:C9:03:00:84:3A:F0
S04       SX          00:02:C9:03:00:84:3B:70
S05       SX          00:02:C9:03:00:84:3B:80
S06       SX          00:02:C9:03:00:84:3B:90
S07       SX          00:02:C9:03:00:61:ED:00
S08       SX          00:02:C9:03:00:84:3B:A0
S09       SX          00:02:C9:03:00:84:3B:50
S10       SX          00:02:C9:03:00:84:3B:10
S11       SX          00:02:C9:03:00:61:EC:B0
S12       SX          00:02:C9:03:00:66:C9:B0
S13       SX          00:02:C9:03:00:66:C9:60
...
```

The output of the command “show guid” on EDR director switch:

```
switch (config) # show guids
=============================================
Module    Device      GUID
=============================================
SYSTEM    -           00:05:C9:03:00:42:D8:00
S01       SIB         00:02:C9:03:00:84:3B:60
S02       SIB         00:02:C9:03:00:84:3B:40
S03       SIB         00:02:C9:03:00:84:3A:F0
S04       SIB         00:02:C9:03:00:84:3B:70
S05       SIB         00:02:C9:03:00:84:3B:80
S06       SIB         00:02:C9:03:00:84:3B:90
S07       SIB         00:02:C9:03:00:61:ED:00
S08       SIB         00:02:C9:03:00:84:3B:A0
S09       SIB         00:02:C9:03:00:84:3B:50
S10       SIB         00:02:C9:03:00:84:3B:10
S11       SIB         00:02:C9:03:00:61:EC:B0
S12       SIB         00:02:C9:03:00:66:C9:B0
S13       SIB         00:02:C9:03:00:66:C9:60
S14       SIB         00:02:C9:03:00:66:C9:50
S15       SIB         00:02:C9:03:00:66:C9:50
S16       SIB         00:02:C9:03:00:66:C9:50
l01       SIB1        00:02:C9:03:00:31:81:80
l01       SIB2        00:02:C9:03:00:31:81:81
...
```

On 1U switches, the command “show guids” displays “MGMT” under the “Module” column instead of “1”.

Before:

```
switch (config) # show guids
=========================================
SX module                      GUID
=========================================
SYSTEM              00:02:C9:03:00:A8:EA:10
1                   00:02:C9:03:00:A8:EA:12
```

After:

```
switch (config) # show guids
=============================================
Module    Device      GUID
=============================================
SYSTEM    -           F4:52:14:03:00:11:E4:F0
MGMT      SX          F4:52:14:03:00:11:E4:F2
```

Added a “Device” column to the command “show asic-version”.

Before:

```
switch (config) # show asic-version
==============================
Module                 Version
==============================
MGMT                   9.3.3150
```

After:

```
switch (config) # show asic-version
================================================
Module             Device              Version
================================================
MGMT               SX                  9.3.3150
```

The output of the command “show asic-version” on an EDR director switch system:

```
switch (config) # show guids
================================================
Module              Device              Version
================================================
101                 SIB1                11.0.1296
101                 SIB2                11.0.1296
102                 SIB1                11.0.1296
102                 SIB2                11.0.1296
103                 SIB1                11.0.1296
103                 SIB2                11.0.1296
104                 SIB1                11.0.1296
104                 SIB2                11.0.1296
105                 SIB1                11.0.1296
105                 SIB2                11.0.1296
106                 SIB1                11.0.1296
106                 SIB2                11.0.1296
...
```

C.4.2 MIB entPhysicalTable Change

The entPhysicalIndex and entPhysicalDescr columns now display and convey module hierarchy.

- entPhysicalDescr in entPhysicalTable revamped now represents ASIC module hierarchy
- entPhysicalIndex in entPhysicalTable now represents a legend and not just a running number. For example (line 9 in Figure 18), “S01/BOARD_MONITOR/T1” has the index 301030011 which indicates the following: 3=Spine, 1=index, 3=BOARD_MONITOR, 1=T, 1=T1.

Figure 17: MIB entPhysicalTable Before Screenshot

	entPhysicalIndex	entPhysicalDescr
1	1	Mellanox SX6512, 216-Port FDR/FDR10 Switch System
2	2	MGMT1
3	3	MGMT2
4	4	S01
5	5	S02
6	6	S03
7	7	S04
8	8	S05
9	9	S06
10	10	L01
11	11	L02
12	12	L03
13	13	L04
14	14	L05

Figure 18: MIB entPhysicalTable After Screenshot

	entPhysicalIndex	entPhysicalDescr
1	1	Mellanox SX6518, 324-Port FDR/FDR10 Switch System
2	201000000	MGMT1
3	201040011	MGMT1/CPU_BOARD_MONITOR/T1
4	201040012	MGMT1/CPU_BOARD_MONITOR/T2
5	202000000	MGMT2
6	301000000	S01
7	301010021	S01/FAN/F1
8	301010022	S01/FAN/F2
9	301030011	S01/BOARD_MONITOR/T1
10	301050000	S01/SX
11	301050011	S01/SX/T1
12	301100011	S01/SX_AMBIENT_TEMP/T1
13	302000000	S02
14	302010021	S02/FAN/F1

C.5 MGMT Module Display Change

The MGMT module display is improved to better represent the actual structure of modules within the system. The commands “show power consumers” and “show temperature” now display information from the MGMT module.

The output of the command “show power consumers” on a 1U PPC switch system:

Before:

```
switch (config) # show power consumers
=============================================================
Module          Device          Power    Voltage  Current  Status
                                (Watts)           (Amp)
=============================================================
CURR_MONITOR    MONITOR         33.31    11.72    2.84     OK

Total power used : 33.31 W
Max power : 235.00 W
```

After:

```
switch (config) # show power consumers
=============================================================
Module          Device          Power    Voltage  Current  Status
                                (Watts)           (Amp)
=============================================================
MGMT            CURR            33.31    11.72    2.84     OK

Total power used : 33.31 W
Max power : 235.00 W
```

The output of the command “show temperature” on a 1U PPC switch system:

Before:

```
switch (config) # show temperature
=====================================================
Module      Component             Reg  CurTemp   Status
                                       (Celsius)
=====================================================
MGMT        BOARD_MONITOR         T1   26.50     OK
MGMT        CPU_MEZZ_TEMP         T1   27.00     OK
CPU_X86     CPU Core Sensor       T1   28.00     OK
CPU_X86     CPU Core Sensor       T2   30.00     OK
CPU_X86     CPU Core Sensor       T3   56.00     OK
CPU_X86     CPU Core Sensor       T4   26.00     OK
CPU_X86     CPU package Sensor    T4   38.00     OK
MGMT        QSFP_TEMP1            T1   27.00     OK
...
```

After:

```
switch (config) # show temperature
=====================================================
Module      Component             Reg  CurTemp   Status
                                       (Celsius)
=====================================================
MGMT        CPU Core Sensor       T1   28.00     OK
MGMT        CPU Core Sensor       T2   30.00     OK
MGMT        CPU Core Sensor       T3   56.00     OK
MGMT        CPU Core Sensor       T4   26.00     OK
MGMT        CPU package Sensor    T4   40.00     OK
MGMT        BOARD_MONITOR         T1   26.50     OK
MGMT        CPU_MEZZ_TEMP         T1   27.00     OK
MGMT        QSFP_TEMP1            T1   27.00     OK
...
```

C.6 MLNX-OS Image Name Change

The “SX_” prefix has been removed from the name of the MLNX-OS image.

C.6.1 CLI Change

The output of the command “show version”:

Before:

```
switch (config) # show version
Product name:      SX_X86_64
Product release:   SX_3.4.0008
Build ID:          #1-dev
Build date:        2014-11-10 20:07:51
Target arch:       x86_64
Target hw:         x86_64
Built by:          jenkins@fit74
Version summary:   SX_X86_64 SX_3.4.0008 2014-11-10 20:07:51
X86_64
...
```

After:

```
switch (config) # show version
Product name:      MLNX-OS
Product release:   3.4.2000
Build ID:          #1-dev
Build date:        2015-05-06 02:16:39
Target arch:       x86_64
Target hw:         m460ex
Built by:          jenkins@fit74
Version summary:   X86_64 3.4.2000 2015-04-12 20:06:05 X86_64

...
```

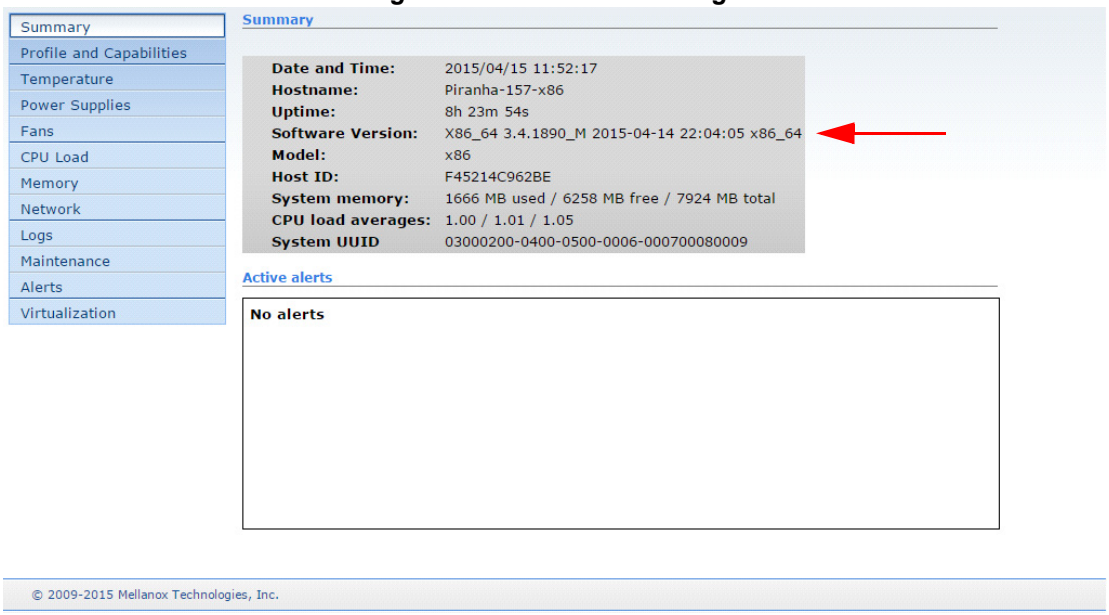
The output of the command “show version”:

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

  Partition 1:
  PPC_M460EX 3.4.2000 2015-05-06 02:16:39 ppc

  Partition 2:
  SX_PPC_M460EX SX_3.4.0000 2014-10-14 20:26:41 ppc //older version with "SX_" suffix

Last boot partition: 1
Next boot partition: 1

...
```

C.6.2 WebUI Status Page Change

In the “Status” page of the MLNX-OS WebUI, the “Software Version” field has been modified to reflect the change in the image file name so now it appears without the prefix “SX_” (Figure 19).

Figure 19: Status WebUI Page



C.7 CPU Module Display Change

The CPU module has been removed from the outputs of the CLI commands “show inventory” and “show modules”.

C.7.1 CLI Change

The command “show inventory” does not list CPU under the “Module” column.

Before

```
switch (config) # show inventory
=============================================================================================
Module          Type            Part number     Serial Number    Asic revision    HW Revision
=============================================================================================
CHASSIS         SX6036          MSX6036F-1SFS   MT1343X02004     N/A              A3
MGMT            SX6036          MSX6036F-1SFS   MT1343X02004     2                A3
FAN             SXX0XX_FAN      MSX60-FF        MT1342X03954     N/A              A1
PS1             SXX0XX_PS       MSX60-PF        MT1342X03824     N/A              A1
CPU             CPU             SA000203-B      MT1140X00201     N/A              A1
```

After

```
switch (config) # show inventory
=============================================================================================
Module          Type            Part number     Serial Number    Asic revision    HW Revision
=============================================================================================
CHASSIS         SX6036          MSX6036F-1SFS   MT1343X02004     N/A              A3
MGMT            SX6036          MSX6036F-1SFS   MT1343X02004     2                A3
FAN             SXX0XX_FAN      MSX60-FF        MT1342X03954     N/A              A1
PS1             SXX0XX_PS       MSX60-PF        MT1342X03824     N/A              A1
```

The command “show module” does not list CPU under the “Module” column.

Before:

```
switch (config) # show module
================================================
 Module    Type              Present Power Is Fatal
================================================
 MGMT      SX6036            1       1     Not Fatal
 FAN       SXX0XX_FAN        1       1     Not Fatal
 PS1       SXX0XX_PS         1       1     Not Fatal
 PS2       SXX0XX_PS         0       0     Not Fatal
 CPU       CPU               1       1     Not Fatal
```

After:

```
switch (config) # show module
================================================
 Module    Type              Present Power Is Fatal
================================================
 MGMT      SX6036            1       1     Not Fatal
 FAN       SXX0XX_FAN        1       1     Not Fatal
 PS1       SXX0XX_PS         1       1     Not Fatal
 PS2       SXX0XX_PS         0       0     Not Fatal
```

C.7.2 WebUI System Inventory Page Change

In the “System > Inventory” page of the MLNX-OS WebUI, the “Module” column does not display the CPU module anymore (Figure 20).

Figure 20: System Inventory WebUI Page