



Mellanox MLNX-OS® User Manual for IBM 90Y3474

Rev 2.70

Software Version 3.3.5064

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 NON-INFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL MELLANOX BE LIABLE TO CUSTOMER OR ANY THIRD PARTIES FOR ANY DIRECT, INDIRECT, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING, BUT NOT LIMITED TO, PAYMENT FOR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY FROM THE USE OF THE PRODUCT(S) AND RELATED DOCUMENTATION EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



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

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

© Copyright 2014. Mellanox Technologies. All Rights Reserved.

Mellanox®, Mellanox logo, BridgeX®, ConnectX®, Connect-IB®, CORE-Direct®, InfiniBridge®, InfiniHost®, InfiniScale®, MetroX®, MLNX-OS®, PhyX®, ScalableHPC®, SwitchX®, UFM®, Virtual Protocol Interconnect® and Voltaire® are registered trademarks of Mellanox Technologies, Ltd.

ExtendX™, FabricIT™, Mellanox Open Ethernet™, Mellanox Virtual Modular Switch™, MetroDX™, TestX™, Unbreakable-Link™ are trademarks of Mellanox Technologies, Ltd.

All other trademarks are property of their respective owners.

Table of Contents

Document Revision History	7
About this Manual	10
Chapter 1 Introduction	13
1.1 System Features	13
1.2 Ethernet Features	14
Chapter 2 Getting Started	15
2.1 Configuring the Switch for the First Time	15
2.2 Starting the Command Line (CLI)	15
2.3 Starting the Web User Interface	16
2.4 Licenses	18
2.4.1 Installing MLNX-OS® License (CLI)	19
2.4.2 Installing MLNX-OS License (Web)	19
2.4.3 Retrieving a Lost License Key	22
2.4.4 Commands	23
Chapter 3 User Interfaces	24
3.1 Command Line Interface (CLI) Overview	24
3.1.1 CLI Modes	24
3.1.2 Syntax Conventions	25
3.1.3 Getting Help	25
3.1.4 Prompt and Response Conventions	26
3.1.5 Using the “no” Form	27
3.1.6 Parameter Key	28
3.1.7 Command Output Filtering	29
3.2 Web Interface Overview	30
3.2.1 Setup Menu	31
3.2.2 System Menu	32
3.2.3 Security Menu	33
3.2.4 Ports Menu	33
3.2.5 Status Menu	34
3.2.6 IB SM Mgmt	34
3.2.7 Fabric Inspector	35
3.2.8 ETH Mgmt	36
3.3 Secure Shell (SSH)	36
3.3.1 Adding a Host and Providing an SSH Key	36
3.3.2 Retrieving Return Codes when Executing Remote Commands	37
3.4 Commands	38
3.4.1 CLI Session	38
3.4.2 Banner	44
3.4.3 SSH	49
3.4.4 Remote Login	62
3.4.5 Web Interface	64
Chapter 4 System Management	78
4.1 Management Interface	78

4.1.1	Configuring Management Interfaces with Static IP Addresses	78
4.1.2	Configuring IPv6 Address on the Management Interface.....	78
4.1.3	Dynamic Host Configuration Protocol (DHCP).....	78
4.1.4	Default Gateway	79
4.1.5	In-Band Management	79
4.1.6	Commands.....	81
4.2	NTP, Clock & Time Zones	122
4.2.1	Commands.....	123
4.3	Software Management.....	129
4.3.1	Upgrading MLNX-OS Software – Preconditions.....	129
4.3.2	Upgrading MLNX-OS Software.....	129
4.3.3	Deleting Unused Images.....	132
4.3.4	Downgrading MLNX-OS Software	133
4.3.5	Upgrading System Firmware	136
4.3.6	Commands.....	138
4.4	Configuration Management.....	148
4.4.1	Saving a Configuration File	148
4.4.2	Loading a Configuration File	148
4.4.3	Managing Configuration Files	148
4.4.4	Commands.....	150
4.5	Logging	175
4.5.1	Monitor	175
4.5.2	Remote Logging	175
4.5.3	Switch Power-On Self-Test.....	175
4.5.4	Commands.....	177
4.6	Debugging	194
4.6.1	Commands.....	195
4.7	Event Notifications	209
4.7.1	Supported Events	209
4.7.2	SNMP Trap Notifications	210
4.7.3	Terminal Notifications	210
4.7.4	Email Notifications	211
4.7.5	Commands.....	213
4.8	mDNS	229
4.8.1	Commands.....	230
4.9	User Management and Security.....	231
4.9.1	Authentication, Authorization and Accounting (AAA)	231
4.9.2	User Accounts.....	232
4.9.3	Commands.....	233
4.10	Cryptographic (X.509, IPSec).....	273
4.10.1	Commands.....	273
4.11	Scheduled Jobs.....	285
4.11.1	Commands.....	285
4.12	Statistics and Alarms	295
4.12.1	Commands.....	295
4.12.2	Power Management.....	312
4.12.3	System Reboot	313
4.12.4	Commands.....	315

4.13	Network Management Interfaces.....	341
4.13.1	SNMP	341
4.13.2	XML API	346
4.13.3	Commands.....	347
4.14	Puppet Agent	362
4.14.1	Setting the Puppet Server	362
4.14.2	Accepting the Switch Request	362
4.14.3	Installing Modules on the Puppet Server	363
4.14.4	Writing Configuration Classes	363
4.14.5	Supported Configuration Capabilities.....	365
4.14.6	Supported Resources for Each Type.....	370
4.14.7	Troubleshooting	370
4.14.8	Commands.....	372
Chapter 5	Ethernet Switching	379
5.1	Interface.....	379
5.1.1	Break-Out Cables	379
5.1.2	Transceiver Information	382
5.1.3	Commands.....	383
5.2	Link Aggregation Group (LAG)	397
5.2.1	Configuring Static Link Aggregation Group (LAG)	397
5.2.2	Configuring Link Aggregation Control Protocol (LACP)	397
5.2.3	Commands.....	399
5.3	VLANs.....	411
5.3.1	Configuring Access Mode and Assigning Port VLAN ID (PVID).....	411
5.3.2	Configuring Hybrid Mode and Assigning Port VLAN ID (PVID).....	412
5.3.3	Configuring Trunk Mode VLAN Membership.....	412
5.3.4	Configuring Hybrid Mode VLAN Membership.....	413
5.3.5	Commands.....	414
5.4	MAC Address Table	421
5.4.1	Configuring Unicast Static MAC Address	421
5.4.2	Commands.....	422
5.5	Spanning Tree	427
5.5.1	Port Priority and Cost	427
5.5.2	Port Type.....	427
5.5.3	BPDU Filter	428
5.5.4	Loop Guard	428
5.5.5	Root Guard	428
5.5.6	MSTP	429
5.5.7	Commands.....	430
5.6	OpenFlow	451
5.6.1	Flow Table	451
5.6.2	Configuring OpenFlow	452
5.6.3	Commands.....	453
5.7	IGMP Snooping.....	460
5.7.1	Configuring IGMP Snooping	460
5.7.2	Defining a Multicast Router Port on a VLAN	460
5.7.3	IGMP Snooping Querier	462
5.7.4	Commands.....	463

5.8	Link Layer Discovery Protocol (LLDP)	479
5.8.1	Configuring LLDP	479
5.8.2	DCBX	479
5.8.3	Commands	481
5.9	Quality of Service (QoS)	497
5.9.1	Priority Flow Control and Link Level Flow Control	497
5.9.2	Enhanced Transmission Selection (ETS)	498
5.9.3	Commands	501
5.10	Access Control List	511
5.10.1	Configuring Access Control List	511
5.10.2	ACL Actions	511
5.10.3	Commands	513
5.11	Port Mirroring	523
5.11.1	Mirroring Sessions	523
5.11.2	Configuring Mirroring Sessions	526
5.11.3	Verifying Mirroring Sessions	528
5.11.4	Commands	529
5.12	sFlow	537
5.12.1	Flow Samples	538
5.12.2	Statistical Samples	538
5.12.3	sFlow Datagrams	538
5.12.4	Sampled Interfaces	539
5.12.5	Configuring sFlow	539
5.12.6	Verifying sFlow	540
5.12.7	Commands	541
Appendix A	Strict Security Mode	553
A.1	Overview	553
A.2	Web Certificate	553
A.3	Code Signing	554
A.4	SNMP	554
A.5	SSH	555
A.6	HTTPS	555
A.7	LDAP	556
A.8	Password Hashing	558

Document Revision History

Table 1 - Document Revision History

Document Revision	Date	Description
Rev 2.70	30 April, 2014	Added: - Appendix A, “Strict Security Mode,” on page 553 - supported versions note in Section 5.7, “IGMP Snooping,” on page 460 Updated: - the command “show ssh server” on page 61 - the command “web auto-logout” on page 64 - the command “web https” on page 71 - the command “show web” on page 77 - the command “show usernames” on page 235 - the command “ldap base-dn” on page 258 - the command “ldap ssl” on page 268
Rev 2.60	10 April, 2014	Updated: Table 26, “Private MIBs Supported,” on page 343
Rev 2.50	April 2014	Updated: - Section 3.1.7, “Command Output Filtering,” on page 29 - the command “show protocols” on page 338 - Section 5.1.1, “Break-Out Cables,” on page 379 - the command “show mac-address-table” on page 425 - the command “deny/permit (MAC ACL rule)” on page 515 - the command “show mac/ipv4 access-lists” on page 521
Rev 2.40	February, 2014	Updated: - Section 4.3.5.2, “Importing Firmware and Changing the Default Firmware,” on page 137 – updated Step 1 - Command “show running-config” on page 174 - Command “show log” on page 193 - Section 4.10, “Cryptographic (X.509, IPSec),” on page 273 - Section 5.2.1, “Configuring Static Link Aggregation Group (LAG),” on page 397 – removed unnecessary step - Command “lldp tlv-select” on page 487 - Command “show lldp interface” on page 490 - Command “show ip ospf statistics” on page 713 Added: - Section 3.1.7, “Command Output Filtering,” on page 29
Rev 2.30	January, 2014	Updated: - Section 4.14.4, “Writing Configuration Classes,” on page 363 - command “crypto certificate generation” on page 278 - command “crypto certificate name” on page 279
Rev 2.20	January, 2014	Updated: Section 4.14.5.11, “Installed Image Capabilities,” on page 369

Table 1 - Document Revision History

Document Revision	Date	Description
Rev 2.10	January, 2014	Added: - Section 4.12.2.1, “Width Reduction Power Saving,” on page 312 Updated: - Section 2.2, “Starting the Command Line (CLI),” on page 15 - Section 2.3, “Starting the Web User Interface,” on page 16 - Section 4.3.2, “Upgrading MLNX-OS Software,” on page 129 with EULA note - Section 4.14, “Puppet Agent,” on page 362 - Section 5.6, “OpenFlow,” on page 451 - command “openflow description” on page 454 - command “show openflow” on page 459 - command “deny/permit (IPv4 ACL rule)” on page 516 - command “load-interval” on page 389 with Config Interface Port Channel - command “switchport {hybrid, trunk} allowed-vlan” on page 419 with Config Interface Port Channel - command “spanning-tree port-priority” on page 434 with Config Interface Port Channel - command “spanning-tree cost” on page 435 with Config Interface Port Channel - command “spanning-tree port type” on page 436 with Config Interface Port Channel - command “spanning-tree guard” on page 437 with Config Interface Port Channel - the command “spanning-tree bpdudfilter” on page 438 with Config Interface Port Channel - command “sflow enable (interface)” on page 551 with Config Interface Port Channel - Section 6.2, “OSPF,” on page 674 - command “router-id” on page 681
Rev 2.00	December 2013	Added Section 5.1.2, “Transceiver Information,” on page 382 Added the command “run-interval” on page 375 Updated Section 4.3.2, “Upgrading MLNX-OS Software,” on page 129 Updated Section 4.3.3, “Deleting Unused Images,” on page 132 Updated Section 4.6, “Debugging,” on page 194 Updated the example of the command “show cpld” on page 323 Updated “Notification Indicator” column in Section 8.2.2, “Configuring Proxy-ARP,” on page 1003 Updated the command “show puppet-agent” on page 377 Updated the command “lldp tlv-select” on page 487 Moved Section 4.5.3, “Switch Power-On Self-Test,” on page 175 from 4.11.1 Moved Section 3.3, “Secure Shell (SSH),” on page 36 from 4.13.2 Removed mention of the MLNX-OS Command Reference Guide Removed the command “lldp tlv-select dcbx”
Rev 1.90	November 2013	Added Appendix A, “MEX6200 System,” on page 1056

Table 1 - Document Revision History

Document Revision	Date	Description
Rev 1.80	October 2013	Added Section 4.14, "Puppet Agent," on page 362 Added Section 5.5.6, "MSTP," on page 429 Added Section 5.6, "OpenFlow," on page 451 Added Section 5.7.3, "IGMP Snooping Querier," on page 462 Added command "ip igmp snooping querier" Added command "igmp snooping querier query-interval" Added command "show ip igmp snooping querier" Added Section 5.8.2, "DCBX," on page 479 Added command "lldp tlv-select dcbx" Added command "dcb application-priority" Added command "show dcb application-priority" Updated command "show lldp interface" Updated command "show lldp interfaces ethernet <inf> remote"
Rev 1.7.0	October 2013	Merged "MLNX-OS Command Reference Guide" Rev. 1.6.9 and "MLNX-OS User Manual" Rev. 1.6.9.

About this Manual

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

Intended Audience

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

Related Documentation

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

Table 2 - Reference Documents

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

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

Glossary

Table 3 - Glossary

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

Table 3 - Glossary

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

1 Introduction

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

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

1.1 System Features

Table 4 - General System Features

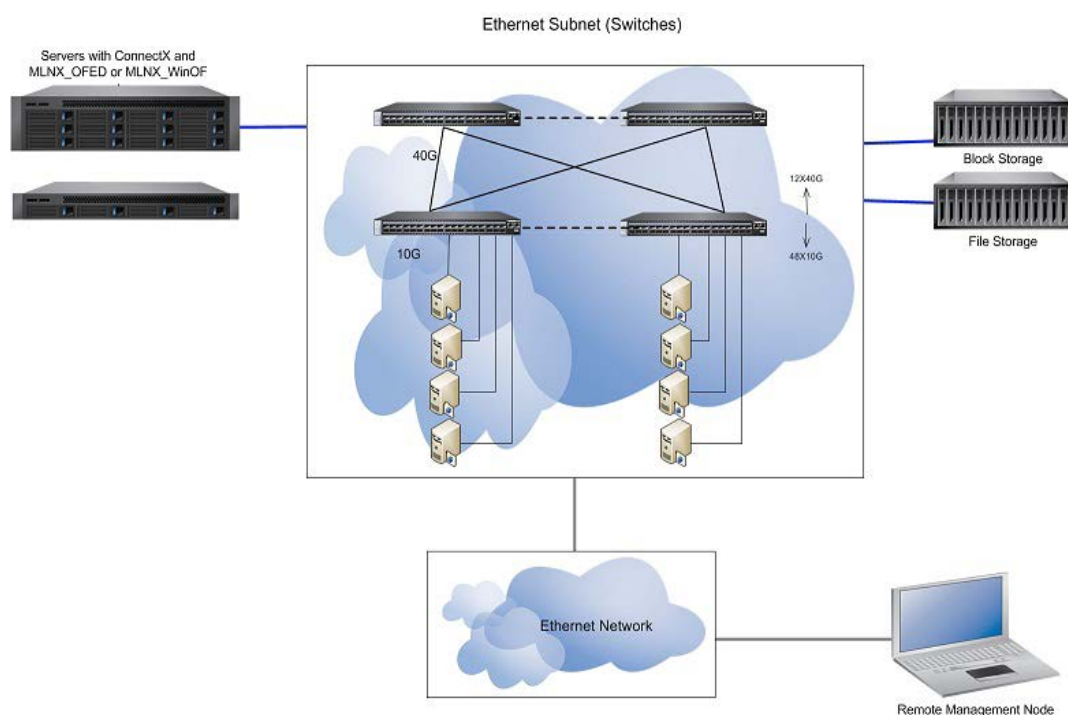
Feature	Description
Software Management	- Dual software image - Software and firmware updates
File management	- FTP - TFTP - SCP
Logging	- Event history log - SysLog support
Management Interface	- DHCP/Zeroconf - IPv6
Chassis Management	Monitoring environmental controls
Network Management Interfaces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

1.2 Ethernet Features

Table 5 - Ethernet Features

Feature	Description
General	- Jumbo Frames (9K) - ACL - 24K rules (permit/deny) - Breakout cables
Ethernet support	48K Unicast MAC addresses - VLAN (802.1Q) - 4K - LAG/LACP (802.3ad), 16 links per LAG (36 LAGs) - Rapid Spanning Tree (802.1w) - Flow control (802.3x) - IGMP snooping v1,2 - LLDP - ETS (802.1Qaz) - PFC (802.1Qbb)
IP routing	- VLAN interface - ECMP - OSPF

Figure 1: Managing an Ethernet Fabric Using MLNX-OS



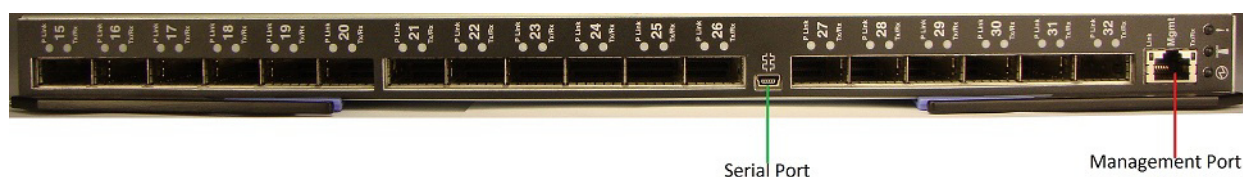
2 Getting Started

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

2.1 Configuring the Switch for the First Time

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

Figure 2: Console Ports



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

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

Table 6 - Serial Terminal Program Configuration for PPC Based Systems

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

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

2.2 Starting the Command Line (CLI)

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

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

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

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

- Step 4.** Read and accept the EULA when prompted.
- Step 5.** Once you get the prompt, you are ready to use the system.

```
Mellanox MLNX-OS Switch Management

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

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

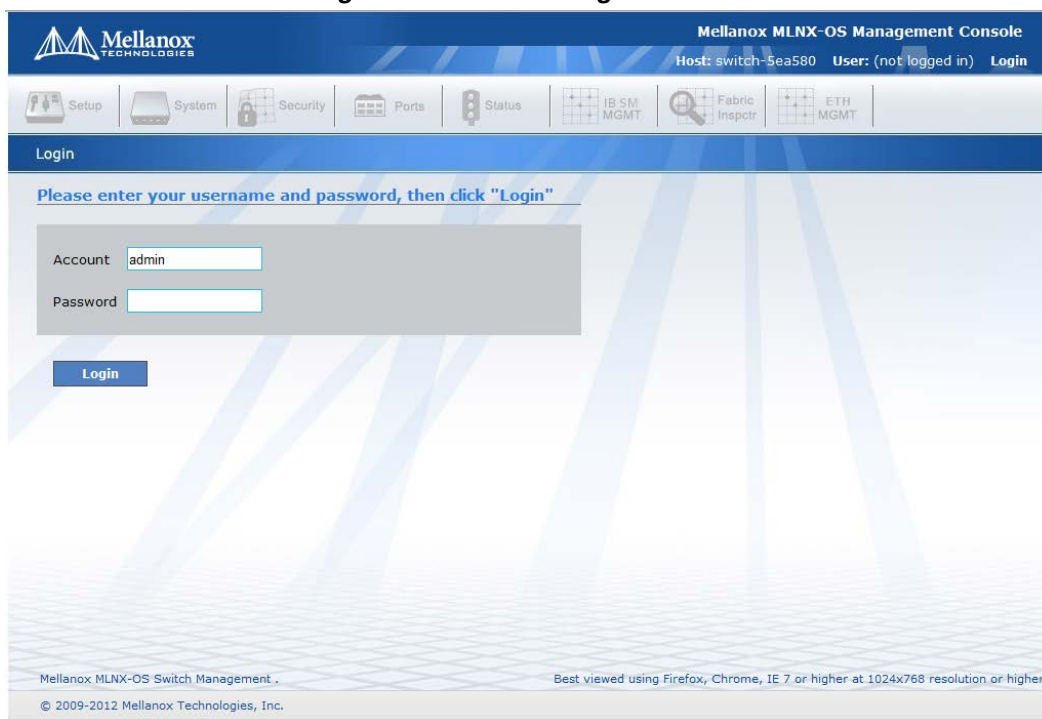
switch >
```

2.3 Starting the Web User Interface

➤ To start a WebUI connection to the switch platform:

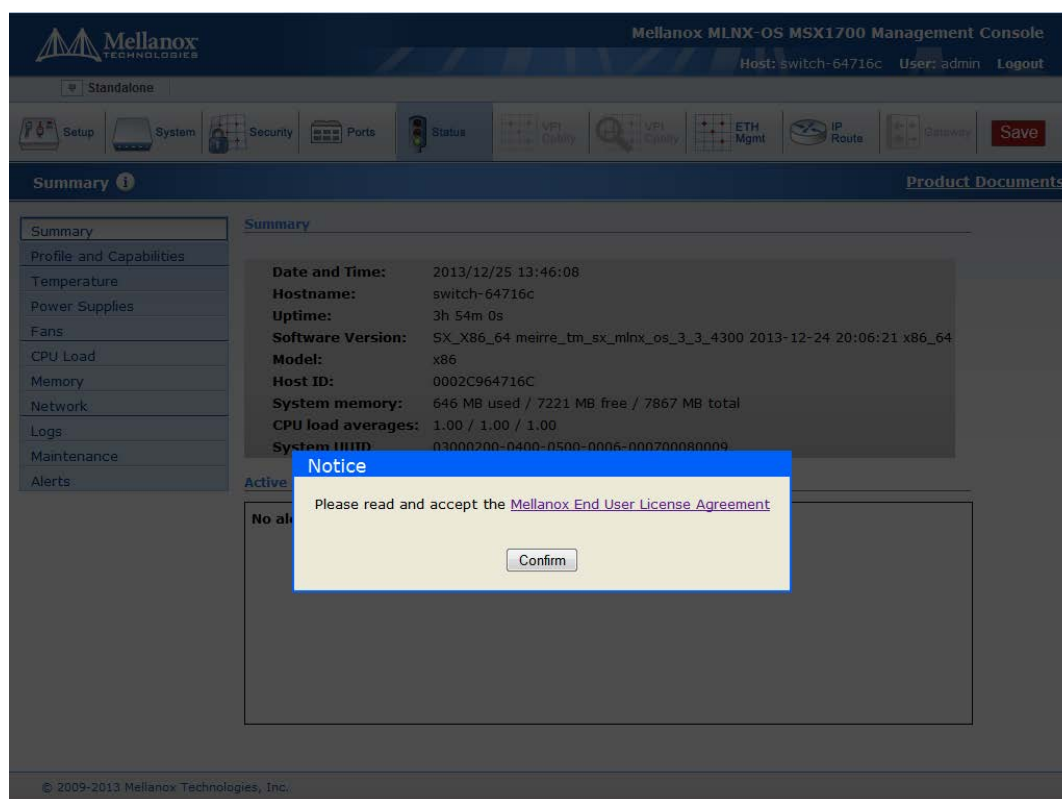
- Step 1.** Set up an Ethernet connection between the switch and a local network machine using a standard RJ-45 connector.
- Step 2.** Open a web browser – Internet Explorer 7.0 Chrome or Mozilla Firefox 3.0.
Note: Make sure the screen resolution is set to 1024*768 or higher.
- Step 3.** Type in the IP address of the switch or its DNS name in the format: `http://<switch_IP_address>`.
- Step 4.** Login to the switch (default user name is *admin*, password *admin*).

Figure 3: MLNX-OS Login Window



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

Figure 4: EULA Prompt



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

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

Figure 5: Display After Login

Mellanox MLNX-OS SX1016 Management Console
Host: switch-5e0aee User: admin Logout

Standalone

Setup System Security Ports Status VPI Cpbity VPI Cpbity ETH MGMT Save

Summary

Summary System Capabilities Temperature Power Supplies Fans CPU Load Memory Network Logs Maintenance Alerts

Summary

Date and Time: 2012/02/07 16:04:06
Hostname: switch-5e0aee
Uptime: 4h 36m 47s
Version: SX_PPC_M460EX 3.0.0000-dev-HA 2012-02-06 08:49:05 ppc
Model: ppc
Host ID: 0002c95e0aee
System memory: 372 MB used / 1655 MB free / 2027 MB total
CPU load averages: 0.41 / 0.36 / 0.25

Active alerts

No alerts

Save

© 2009-2012 Mellanox Technologies, Inc.

2.4 Licenses

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



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

The following licenses are offered with MLNX-OS software:

Table 7 - MLNX-OS Licenses

OPN	Valid on Product	Description
UPGR-6012-GW	SX6012	Ethernet L2/L3, Gateway
UPGR-6012F-56E	SX6012	56GbE link speed
UPGR-1012-GW	SX1012	InfiniBand, Ethernet L3, Gateway
UPGR-1012-56E	SX1012	56GbE link speed
UPGR-6018-GW	SX6018	Ethernet L2/L3, Gateway
UPGR-6018F-56E	SX6018	56GbE link speed
UPGR-6036-GW	SX6036	Ethernet L2/L3, Gateway
UPGR-6036F-56E	SX6036	56GbE link speed

Table 7 - MLNX-OS Licenses

OPN	Valid on Product	Description
UPGR-1036-GW	SX1036	InfiniBand, Ethernet L3, Gateway
UPGR-1036F-56E	SX1036	56GbE link speed
UPGR-1024-GW	SX1024	InfiniBand, Ethernet L3, Gateway
UPGR-1024-56E	SX1024	56GbE link speed
UPGR-1700-GW	SX1700	InfiniBand, Ethernet L3, Gateway
LIC-fabric-inspector	SX6036F/T; SX65xx	InfiniBand fabric inspector monitoring and health.
UPGR-xxxx-FCoE-J	All systems supporting Ethernet directly or via license.	Enables FCoE protocol.

2.4.1 Installing MLNX-OS® License (CLI)

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

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

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

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

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

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

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

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

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

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



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

2.4.2 Installing MLNX-OS License (Web)

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

Step 1. Log in as *admin*.

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

Figure 6: No Licenses Installed

Mellanox MLNX-OS SX6506 Management Console
 Host: switch-113dc8 User: admin Logout
 Standalone Virtual IP Active node Chassis master Subnet Manager is not running.

Setup System Security Ports Status IB SM MGMT Fabric Inspector ETH MGMT Save

Licensing

Interfaces
 HA
 Routing
 DNS
 Hostname
 Hosts
ARP
 Neighbors
 Virtual Switch Mgmt
 Web
 SNMP
 Email Alerts
 XML gateway
 Logs
 Configurations
 Date and Time
 NTP
 Licensing

System Serial Number
 MXXXXXXXXXX7

Installed Licenses

License	Key	Feature	Valid	Max num ufm ports supported	Active
☐	LK2-EFM_SX-5P26-85G2-3488-A3MG-VD3V-E7U	EFM_SX	yes	200	yes

Remove

Add New License(s)

Please enter one or more licenses, each on a separate line.

Add Licenses **Save**

© 2009-2012 Mellanox Technologies, Inc.

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



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

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

Mellanox MLNX-OS SX6506 Management Console
 Host: switch-113dc8 User: admin Logout
 Standalone Virtual IP Active node Chassis master Subnet Manager is not running.

Licensing

System Serial Number
 MXXXXXXXXXX7

Installed Licenses

License
☐ Key Feature: EFM_SX Valid: yes Max num ufm ports supported: 200 Active: yes

Add New License(s)

Please enter one or more licenses, each on a separate line.

<your license key>

Add Licenses **Save**

© 2009-2012 Mellanox Technologies, Inc.

All installed licenses should now be displayed.

Figure 8: Installed License

Mellanox MLNX-OS SX6506 Management Console
 Host: switch-113dc8 User: admin Logout
 Standalone Virtual IP Active node Chassis master Subnet Manager is not running.

Licensing

System Serial Number
 MXXXXXXXXXX7

Installed Licenses

License
☐ Key Feature: EFM_SX Valid: yes Max num ufm ports supported: 200 Active: yes

Add New License(s)

Please enter one or more licenses, each on a separate line.

Add Licenses **Save**

© 2009-2012 Mellanox Technologies, Inc.

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



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

2.4.3 Retrieving a Lost License Key

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

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

Step 1. Login to the switch.

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

```
switch (config) # show inventory
=====
Module                Type                Part number        Serial Number
=====
CHASSIS               SX1035              MSX6036F-1BFR      MT1121X02692
MGMT                  SX1035              MSX6036F-1BFR      MT1121X02692
FAN                   SXX0XX_FAN          MSX60-FF            MT1121X02722
PS1                   SXX0XX_PS           N/A                 N/A
CPU                   CPU                 SA000103            MT1120X01027
switch (config) #
```

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

- The chassis serial number
- The type of license you need to retrieve. Refer to [“MLNX-OS Licenses” on page 18](#).

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

2.4.4 Commands

show licenses

show licenses

Displays a list of all installed licenses. For each license, the following is displayed:

- a unique ID which is a small integer
- the text of the license key as it was added
- whether or not it is valid and active
- which feature(s) it is activating
- a list of all licensable features specifying whether or not it is currently activated by a license

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	monitor/admin
Example	switch (config) # show licenses License 1: <license key> Feature: SX_CONFIG Valid: yes Active: yes switch (config) #
Related Commands	license
Note	

3 User Interfaces

3.1 Command Line Interface (CLI) Overview

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

3.1.1 CLI Modes

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

Table 8 - CLI Modes and Config Context

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

3.1.2 Syntax Conventions

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

Table 9 - Syntax Conventions

Syntax Convention	Description	Example
< > Angled brackets	Indicate a value/variable that must be replaced.	<1...65535> or <switch inter-face>
[] 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 10 - 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 10 - Angled Brackets Parameter Description

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

3.1.7 Command Output Filtering

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

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

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

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

Examples:

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

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

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

```

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

```

3.2 Web Interface Overview

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

The following web browsers are supported:

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

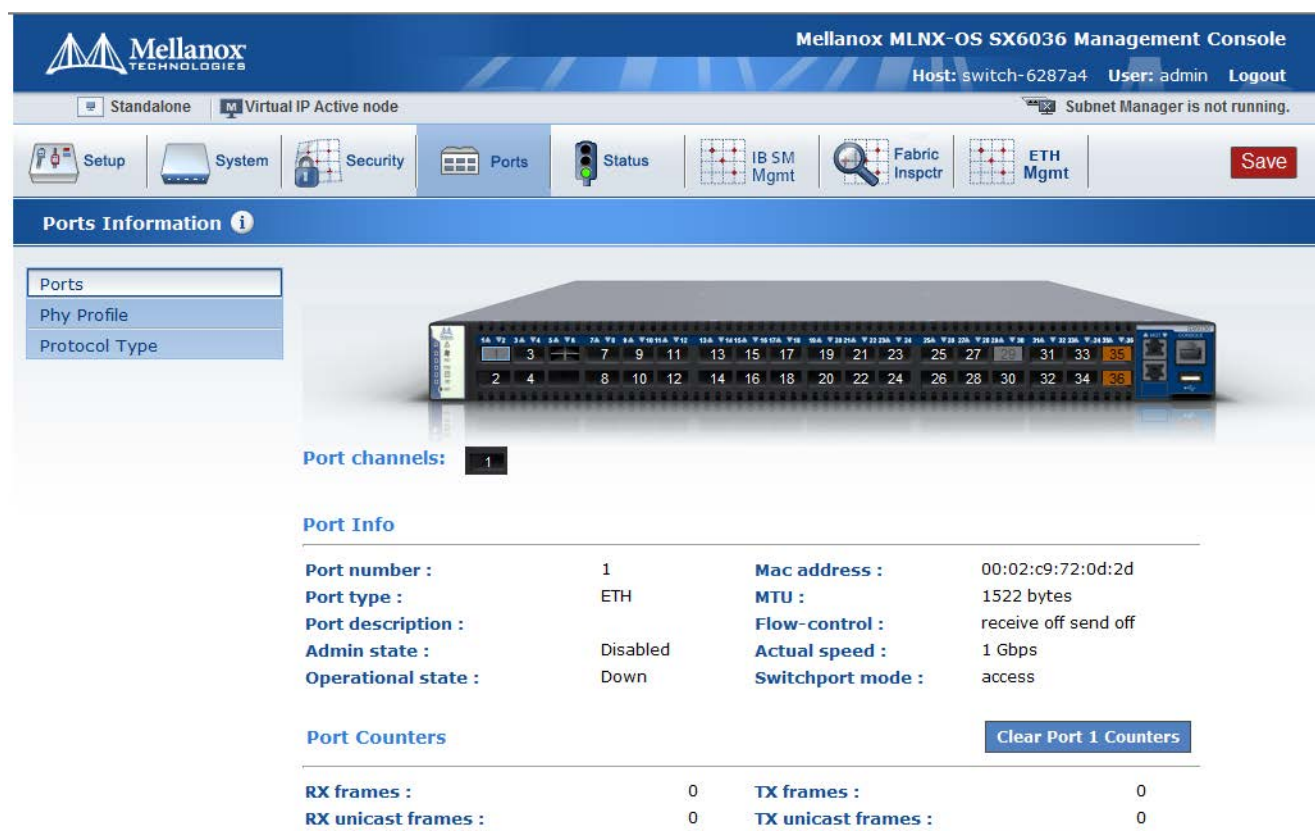
The web interface makes available the following perspective tabs:

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



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

Figure 9: WebUI



3.2.1 Setup Menu

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

Table 11 - Setup Submenus

Submenu Title	Description
Interfaces	Used to obtain the status of, configure, or disable 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	Not functional.
Routing	Used to set, remove or display the default gateway, and the static and dynamic routes.
Hostname	Used to set or modify the hostname. Used to set or delete static hosts. Note: Changing hostname stamps a new HTTPS certificate.
DNS	Used to set, remove, modify or display static and dynamic name servers.

Table 11 - Setup Submenus

Submenu Title	Description
Login Messages	Used to edit the login messages: Message of the Day (MOTD), Remote Login message, and Local Login message.
ARP	Used to add static and dynamic ARP entries, and to clear the dynamic ARP cache.
IPSec	Used to configure IPSec feature.
Neighbors	Used to display IPv6 neighbor discovery protocol.
Virtual Switch Mgmt	Used to set the system profile.
Web	Used to configure Web user interface and proxy settings.
SNMP	Used to configure SNMP attributes, SNMP admin user, and trap sinks.
Email Alerts	Used to define 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	Used to set up system log files, remote log sinks, and log formats.
Configurations	Used to manage, activate, save, and import MLNX-OS SwitchX configuration files, and to execute CLI commands.
Date and Time	Used to set the date, time, and time zone of the switch system.
NTP	Used to set NTP (Network Time Protocol) and NTP servers.
Licensing	Used to manage 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 12 - 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.

Table 12 - System Submenus

Submenu Title	Description
MLNX-OS Upgrade	Displays the installed MLNX-OS images (and the active partition), to upload a new image, and to install a new image.
Reboot	Used to reboot 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 13 - Security Submenus

Submenu Title	Description
Users	Used to manage (setting up, removing, modifying) user accounts.
Admin Password	Used to modify the system administrator password.
SSH	Used to display and generate host keys.
AAA	Used to configure AAA (Authentication, Authorization, and Accounting) security services such as authentication methods and authorization.
Login Attempts	Used to manage login attempts
RADIUS	Used to manage Radius client.
TACACS+	Used to manage TACACS+ client.
LDAP	Used to manage LDAP client.
Certificate	Used to manage 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 14 - 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.
Protocol type	Manages the link protocol type

3.2.5 Status Menu

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

Table 15 - 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	Used to perform specific maintenance operations automatically on a predefined schedule.
Alerts	Used to display a list of the recent health alerts and enables the user to configure health settings.

3.2.6 IB SM Mgmt



The IB SM MGMT menu is not supported in Ethernet systems.

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

Table 16 - IB SM Mgmt Submenus

Submenu Title	Description
Summary	Displays the local Subnet Manager (SM) status (running time, failures, etc).

Table 16 - IB SM Mgmt Submenus

Submenu Title	Description
Base SM	Used to manage basic SM configuration (enabling SM, priority level, and restoring initial configuration).
Advanced SM	Used to manage basic SM configuration (enabling SM, priority level, and restoring initial configuration).
Expert SM	Used to configure security and GUID based prefixes (m_key, sm_key, sa_key, etc), and to manage special SM attributes that should not be changed except by expert users of the Subnet Manager who understand the risks of manipulating these attributes.
Compute nodes	Used to add compute nodes using network adapter port GUIDs.
Root nodes	Used to add root nodes using switch GUIDs.
Partitions	Manages partition keys (sets removes or displays the partition keys).
Basic Qos	Used to configure basic QoS attributes such as default QoS settings, and VL arbitration low and high entries. It is also used to display and manage SL to VL mappings.

3.2.7 Fabric Inspector



The Fabric Inspctr menu is not applicable when the switch profile is not InfiniBand.



The Fabric Inspctr menu requires a license (LIC-fabric-inspector)

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

Table 17 - Fabric Inspctr Submenus

Submenu Title	Description
Summary	Displays a fabric status summary, including the time of last fabric update, what systems are in the fabric, what InfiniBand devices are identified, etc.
IB Systems	Displays information about all identified InfiniBand systems in the fabric (adapters, switches, etc).
IB Nodes	Displays information about InfiniBand nodes in the fabric. It is possible to filter display by the type of InfiniBand node (HCA adapter, switch, etc).

Table 17 - Fabric Inspctr Submenus

Submenu Title	Description
IB Ports	Displays all active InfiniBand ports in the fabric. It is possible to filter display by the type of InfiniBand port (HCA port, switch port, switch management port, etc), by the port rate (speed or width), by the Subnet Manager status on the node, by node traffic, etc.
Connections	Displays all active connections in the fabric. It is possible to filter display by the link type (switch to switch, switch to HCA, etc) and by the link rate (speed or width).
System Names	Allows the mapping of System Names to GUIDs to ease system identification.

3.2.8 ETH Mgmt



The Eth Mgmt menu is not applicable when the switch profile is not ethernet.

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

Table 18 - ETH Mgmt Submenus

Submenu Title	Description
Spanning Tree	Used for configuring and monitoring spanning tree protocol.
MAC Table	Used for configuring static mac addresses in the switch, and displaying the mac address table.
Link Aggregation	Used for configuring and monitoring aggregated Ethernet links (LAG) as well as configuring LACP.
VLAN	Used for managing the switch VLAN table.
IGMP Snooping	Used for managing IGMP snooping in the switch.
ACL	Used for managing Access Control in the switch.

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
AAAAB3NzaC1yc2EAAAABIwAAAIEAsXek1qc8T0EN2mnMcVcfhueaRYzIVqt4rVsrERijm1Jh4mkYYIa8hGGikNa+
t5xw2dRrNxnHYLK51bUsSG1ZNwZT1Dpme3pAZeMY7G4ZMgGIW9x0uaXgAA3eBeoUjFdi6+1BqchWk0nTb+gMfI/
MK/heQNns7AtTrvqg/05ryIc="
switch [standalone: master] (config) #
```

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

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

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

No SSH user identities configured.

No SSH authorized keys configured.

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

3.3.2 Retrieving Return Codes when Executing Remote Commands

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

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

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

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

3.4 Commands

3.4.1 CLI Session

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

cli clear-history

cli clear-history

Clears the command history of the current user.

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

cli default

cli default {auto-logout <minutes> | paging enable | prefix-modes {enable | show-config} | progress enable | prompt {confirm-reload | confirm-reset | confirm-unsaved | empty-password}}

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

Configures default CLI options for all future sessions.

The no form of the command deletes or disables the default CLI options.

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

Example

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

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

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

Related Commands show cli

Note

cli session

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

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

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

Example	switch (config) # cli session auto-logout switch (config) #
----------------	--

Related Commands	show terminal
-------------------------	---------------

Note	
-------------	--

show cli

show cli

Displays the CLI configuration and status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
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	<pre>switch (config) # banner login example switch (config) # show banner Banners: MOTD: Mellanox Switch Login: example switch (config) #</pre>
Related Commands	show banner
Note	If more than 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 contents of the /etc/motd file.
 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	<pre>switch (config) # banner motd Testing switch (config) # show banner Banners: MOTD: Testing Login: Mellanox MLNX-OS Switch Management switch (config) #</pre>	
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").	

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	<pre>switch (config) # show banner Banners: MOTD: Testing Login: Mellanox MLNX-OS Switch Management switch (config) #</pre>
Related Commands	<pre>banner login banner motd</pre>
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	<pre> 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) # </pre>
Related Commands	show ssh server
Note	Disabling SSH server does not terminate existing SSH sessions, it only prevents new ones from being established.

ssh server host-key

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

Manipulates host keys for SSH.

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

Example

```

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

  Interface listen enabled: yes
  No Listen Interfaces.

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

Host Keys:
  RSA v1 host key: "switch-5ea5d8 1024 35
12457497995374010105491416867919987976776882016984375942831915584962796
99375406596085804272219042450456598705866658144854493132172365068789517
13570509420864336951833046700451354269467758379288848962624165330724512
16091899983038691571036219385577978596282214644533444813712105628654158
3022982220576029771297093"
  RSA v2 host key: "switch-5ea5d8 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEArB9i50nukAHNU0kwpCmEl0m88kJgBzL22+F5tfaSn+S
0pVYxrceZeyuzXsoZ1VtFTk2FydwY0YvMS0Kcv2PuCrPZV/
GYd31QEnn22rEmrlPrKCrMl1XlUy6DFlr30gWwm1baobmDlG/gSziWz/
gc4Jgqf2CyXFq4pzaR1jar1Vk="
  DSA v2 host key: "switch-5ea5d8 ssh-dss
AAAAB3NzaC1kc3MAAACBAMEJ3S+nyaHhRbwv3tJqlWttDC35RZVC5iG4ZEVMHhp28VL940c
yyuGh39VCdM9pEvaI7hzZrsgHrNqakb/YLD/
7anGH3wpl9Fx8lfe0RH3bloJzG+mJ6R5momdoPCrKwEKiKABKE00jLz1VznpP0IHxjwF+Tb
R3dK5HwVzQYw/
bAAAAFQCBODPqBZZa+2Ky1K1zUsbZ2pKhgQAAAAIAJK+StiQdtORw1B5UCmZTrTef5L07DSf
VreMEYtTRnBBtgVSNqQFWpSQIYbVDHQR9T6qCM4V039DuHUGQ1TMDIX7t+9mfB87YyUu5a
/ndbf3GhNhXHWwbzlr9hgLL7FSHA7DYH7bV0ZRlqxH64eQKGZqy1ps/
F4E31lyn7GC4EQAAIA/2osHipXf+NRjplgfmHROVVf/mGE9Vzc9/
AMUx1JJn5VhvEJ5CZW9cI+LxMOJojh0j3YW3B1czGxR0bDA9vUbKXTNc8bkgoUrxySAH1rH
N0PqJgeT4L009AItSp3m1mxHqdS7jixfTv0TEKWxrgpczlmTB8+zjhUah/YuuB12H
g=="
switch (config) #

```

Related Commands

```
show ssh server
```

Note

ssh server listen

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

Enables the listen interface restricted list for SSH. If enabled, and at least one non-DHCP interface is specified in the list, the SSH connections are only accepted on those specified interfaces.

The no form of the command disables the listen interface restricted list for SSH. When disabled, SSH connections are not accepted on any interface.

Syntax Description	enable	Enables SSH interface restrictions on access to this system.
	interface <inf>	Adds interface to SSH server access restriction list. Possible interfaces are “lo”, and “mgmt0”.
Default	SSH listen is enabled	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
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	<pre>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) #</pre>	
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	<pre>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) #</pre>	
Related Commands	show ssh server	
Note	- Multiple ports can be specified by repeating the <port> parameter - The command will remove any previous ports if not listed in the command	

ssh server x11-forwarding

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

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

Syntax Description	N/A
Default	X11-forwarding is disabled.
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
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	<pre>switch (config) # ssh client global host-key-check no switch (config) # ssh client global known-host "72.30.2.2 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEArB9i50nukAHNUOkwpCmEl0m88kJgBzL22+F5tfaSn+S 0pVYxrceZeyuzXsoZ1VtFTk2FydwY0YvMS0Kcv2PuCrPZV/ GYd31QEnn22rEmr1PrKCrM11XlUy6DFlr30gwWm1baobmDlG/gSziwz/ gc4Jgqf2CyXFq4pzaR1jar1Vk=" switch (config) # show ssh client SSH client Strict Hostkey Checking: ask SSH Global Known Hosts: Entry 1: 72.30.2.2 Finger Print: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6 No SSH user identities configured. No SSH authorized keys configured. switch (config) #</pre>	

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	<pre>switch (config) # slogin 192.168.10.70 The authenticity of host '192.168.10.70 (192.168.10.70)' can't be established. 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) #</pre>	
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	<pre>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) #</pre>
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	<pre>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) #</pre>
Related Commands	ssh server
Note	

3.4.4 Remote Login

telnet-server enable

telnet-server enable
no telnet-server enable

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

Syntax Description	N/A
Default	Telnet server is disabled
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	switch (config) # telnet-server enable switch (config) # show telnet-server Telnet server enabled: yes
Related Commands	show telnet-server
Note	

show telnet-server

show telnet-server

Displays telnet server settings.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	switch (config) # show telnet-server Telnet server enabled: yes switch (config) #
Related Commands	telnet-server enable
Note	

3.4.5 Web Interface

web auto-logout

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

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

Syntax Description	number of minutes	The length of user inactivity in minutes. 0 will disable the inactivity timer (same as a “no web auto-logout” command).
Default	60 minutes	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show web	
Note	The no form of the command does not automatically log users out due to inactivity.	

web client cert-verify

web client cert-verify
no web client cert-verify

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

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

web client ca-list

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

Configures supplemental CA certificates for verification of server certificates during HTTPS file transfers.

The no form of the command uses no supplemental certificates.

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

web enable

web enable
no web enable

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

Syntax Description	N/A
Default	enable
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>switch (config) # web enable switch (config) # show web</pre> Web User Interface: <pre>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.</pre> <pre>Inactivity timeout: 1 hr Session timeout: 2 hr 30 min Session renewal: 30 min</pre> Web file transfer proxy: <pre>Proxy enabled: no</pre> Web file transfer certificate authority: <pre>HTTPS server cert verify: yes HTTPS supplemental CA list: default-ca-list switch (config) #</pre>
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	
Role	admin	
Example	<pre> 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) # </pre>	

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

web https

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

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

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

Example

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

Web User Interface:

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

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

```
Web file transfer proxy:
Proxy enabled: no
```

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

Related Commands

```
show web
web enable
```

Note

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

web session

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

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

Syntax Description	renewal <minutes>	Configures time before expiration to renew a session.
	timeout <minutes>	Configures time after which a session expires.
Default	timeout - 2.5 hours renewal - 30 min	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre> 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) # </pre>	
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	<pre>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) #</pre>	
Related Commands	web proxy auth	
Note		

show web

show web

Displays the web configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
	3.3.5050 Updated Example
Role	admin
Example	<pre>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) #</pre>
Related Commands	<pre>show web web proxy auth</pre>
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. Change to Config mode. Run:

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

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

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

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

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

4.1.2 Configuring IPv6 Address on the Management Interface

Step 1. Enable IPv6 on this interface.

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

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

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

Step 3. Verify the IPv6 address is configured correctly.

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

4.1.3 Dynamic Host Configuration Protocol (DHCP)

DHCP is used for automatic retrieval of management IP addresses.

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



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

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

In such case the serial connection should be used.

4.1.4 Default Gateway

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

```
switch (config)# ip route 0.0.0.0 0.0.0.0 10.209.0.2
switch (config)# show ip route
```

Destination	Mask	Gateway	Interface	Source
default	0.0.0.0	10.209.0.2	mgmt0	static
10.209.0.0	255.255.254.0	0.0.0.0	mgmt0	direct

```
switch (config)#
```

4.1.5 In-Band Management

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

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

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

Step 1. Create a VLAN. Run:

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

Step 2. Create a VLAN interface. Run:

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

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

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

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

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

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

RX bytes:      0          TX bytes:      250
RX packets:    0          TX packets:     3
RX mcast packets: 0      TX discards:  0
RX discards:   0          TX errors:   0
RX errors:     0          TX overruns: 0
RX overruns:   0          TX carrier:  0
RX frame:      0          TX collisions: 0
                                TX queue len: 0

switch (config) #
```

4.1.6 Commands

4.1.6.1 Interface

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

interface

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

Enters a management interface context.

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

interface vlan create

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

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

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

ip address

ip address <IP address> <netmask>

no ip address

Sets the IP address and netmask of this interface.

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

Syntax Description	IP address	IPv4 address	
	netmask	Subnet mask of IP address	
Default	0.0.0.0/0		
Configuration Mode	Config Interface Management		
History	3.1.0000		
Role	admin		
Example	<pre>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) #</pre>		
Related Commands	show interfaces <ifname>		
Note	If DHCP is enabled on the specified interface, then the DHCP IP assignment will hold until DHCP is disabled.		

alias

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

Adds an additional IP address to the specified interface. The secondary address will appear in the output of “show interface” under the data of the primary interface along with the alias.

The no form of the command removes the secondary address to the specified interface.

Syntax Description	index	A number that is to be aliased to (associated with) the secondary IP.	
	IP address	Additional IP address.	
	netmask	Subnet mask of the IP address.	
Default	N/A		
Configuration Mode	Config Interface Management		
History	3.1.0000		
Role	admin		
Example	<pre>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) #</pre>		

Related Commands

show interfaces <ifname>

Note

- If DHCP is enabled on the specified interface, then the DHCP IP assignment will hold until DHCP is disabled
 - More than one additional IP address can be added to the interface
-

mtu

mtu <bytes>
no mtu <bytes>

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

Syntax Description	bytes	The entry range is 68-1500.
Default	1500	
Configuration Mode	Config Interface Management	
History	3.1.0000	
Role	admin	
Example	<pre> 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: </pre> RX bytes: 2970074221 RX packets: 44983023 RX mcast packets: 0 RX discards: 0 RX errors: 0 RX overruns: 0 RX frame: 0 TX bytes: 468579522 TX packets: 1390539 TX discards: 0 TX errors: 0 TX overruns: 0 TX carrier: 0 TX collisions: 0 TX queue len: 1000 <pre> switch (config interface mgmt0) # </pre>	
Related Commands	show interfaces <ifname>	
Note		

duplex

duplex <duplex>

no duplex

Sets the interface duplex.

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

Syntax Description	duplex	Sets the duplex mode of the interface. The following are the possible values: • half - half duplex • full - full duplex • auto - auto duplex sensing (half or full)	
Default	auto		
Configuration Mode	Config Interface Management		
History	3.1.0000		
Role	admin		
Example	switch (config interface mgmt0) # duplex auto switch (config interface mgmt0) # show interfaces mgmt0 Interface mgmt0 state Admin up: yes Link up: yes IP address: 172.30.2.2 Netmask: 255.255.0.0 Secondary address: 9.9.9.9/32 (alias: 'mgmt0:2') IPv6 enabled: yes Autoconf enabled: no Autoconf route: yes Autoconf privacy: no IPv6 addresses: 1 IPv6 address: fe80::202:c9ff:fe5e:a5d8/64 Speed: 1000Mb/s (auto) Duplex: full (auto) Interface type: ethernet Interface ifindex: 2 Interface source: physical MTU: 1500 HW address: 00:02:C9:5E:A5:D8 Comment: RX bytes: 2970074221 TX bytes: 468579522 RX packets: 44983023 TX packets: 1390539 RX mcast packets: 0 TX discards: 0 RX discards: 0 TX errors: 0 RX errors: 0 TX overruns: 0 RX overruns: 0 TX carrier: 0 RX frame: 0 TX collisions: 0 TX queue len: 1000 switch (config interface mgmt0) #		

Related Commands	show interfaces <ifname>
-------------------------	--------------------------

- | | |
|-------------|---|
| Note | <ul style="list-style-type: none">• 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	<pre> 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 RX packets: 44983023 RX mcast packets: 0 RX discards: 0 RX errors: 0 RX overruns: 0 RX frame: 0 TX bytes: 468579522 TX packets: 1390539 TX discards: 0 TX errors: 0 TX overruns: 0 TX carrier: 0 TX collisions: 0 TX queue len: 1000 switch (config interface mgmt0) # </pre>	

Related Commands	show interfaces <ifname>
-------------------------	--------------------------

- | | |
|-------------|--|
| Note | <ul style="list-style-type: none">• 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	<pre>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:</pre>	
Related Commands	show interfaces <ifname> configured	
Note	- When enabling DHCP, the IP address and netmask are received via DHCP hence, the static IP address configuration is ignored - Enabling DHCP disables zeroconf and vice versa - Setting a static IP address and netmask does not disable DHCP. DHCP is disabled by using the “no” form of this command, or by enabling zeroconf.	

shutdown

shutdown
no shutdown

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

Syntax Description	N/A
Default	no shutdown
Configuration Mode	Config Interface Management
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	show interfaces <ifname> configured
Note	

zeroconf

zeroconf
no zeroconf

Enables zeroconf on the specified interface. It randomly chooses a unique link-local IPv4 address from the 169.254.0.0/16 block. This command is an alternative to DHCP.

The no form of the command disables the use of zeroconf on the specified interface.

Syntax Description	N/A
Default	no zeroconf
Configuration Mode	Config Interface Management
History	3.1.0000
Role	admin
Example	<pre>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:</pre>
Related Commands	show interfaces <ifname> configured
Note	Enabling zeroconf disables DHCP and vice versa.

comment

comment <comment>

no comment

Adds a comment for an interface.

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

Syntax Description	comment	A free-form string that has no semantics other than being displayed when the interface records are listed.	
Default	no comment		
Configuration Mode	Config Interface Management		
History	3.1.0000		
Role	admin		
Example	<pre>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) #</pre>		
Related Commands	N/A		
Note			

ipv6 address

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

Configures IPv6 address and netmask to this interface, static or autoconfig options are possible.

The no form of the command removes the given IPv6 address and netmask or disables the autoconfig options.

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

Example

```

switch (config interface mgmt0) # ipv6 fe80::202:c9ff:fe5e:a5d8/64
switch (config interface mgmt0) # show interfaces mgmt0
Interface mgmt0 state
  Admin up:          yes
  Link up:           yes
  IP address:        172.30.2.2
  Netmask:           255.255.0.0
  IPV6 enabled:      yes
  Autoconf enabled:  no
  Autoconf route:    yes
  Autoconf privacy:  no
  IPV6 addresses:    1
  IPV6 address:      fe80::202:c9ff:fe5e:a5d8/64
  Speed:             1000Mb/s (auto)
  Duplex:            full (auto)
  Interface type:    ethernet
  Interface ifindex: 2
  Interface source:  physical
  MTU:               1500
  HW address:        00:02:C9:5E:A5:D8
  Comment:           my-interface

  RX bytes:          962067812      TX bytes:          40658219
  RX packets:        3738865       TX packets:        142345
  RX mcast packets:  0             TX discards:       0
  RX discards:       0             TX errors:         0
  RX errors:         0             TX overruns:       0
  RX overruns:       0             TX carrier:        0
  RX frame:          0             TX collisions:     0
                                   TX queue len:    1000

switch (config interface mgmt0) #

```

Related Commands

```

ipv6 enable
show interface <ifname>

```

Note

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

show interface

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

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

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

Related Commands

N/A

Note

4.1.6.2 Hostname Resolution

hostname

hostname <hostname>
no hostname

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

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

ip name-server

ip name-server <IPv4/IPv6 address>

no name-server <IPv4/IPv6 address>

Sets the static name server.

The no form of the command clears the name server.

Syntax Description	IPv4/v6 address	IPv4 or IPv6 address.
Default	No server name	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show hosts	
Note		

ip domain-list

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

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

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

ip/ipv6 host

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

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

Syntax Description	hostname	The hostname in a string form.
	IP Address	The IPv4 or IPv6 address.
Default	No static domain name.	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show hosts	
Note		

ip/ipv6 map-hostname

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

Maps between the currently-configured hostname and the loopback address 127.0.0.1.

The no form of the command clears the mapping.

Syntax Description	N/A
Default	IPv4 mapping is enabled by default IPv6 mapping is disabled by default
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre> 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 </pre>
Related Commands	show hosts
Note	- If no mapping is configured, a mapping between the hostname and the IPv4 loopback address 127.0.0.1 will be added - The no form of the command maps the hostname to the IPv6 loopback address if there is no statically configured mapping from the hostname to an IPv6 address (disabled by default) - Static host mappings are preferred over DNS results. As a result, with this option set, you will not be able to look up your hostname on your configured DNS server; but without it set, some problems may arise if your hostname cannot be looked up in DNS.

show hosts

show hosts

Displays hostname, DNS configuration, and static host mappings.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	N/A
Note	

4.1.6.3 Routing

ip/ipv6 route

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

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

Syntax Description	network-prefix	IPv4 or IPv6 network prefix.			
	netmask	IPv4 netmask formats are: • /24 • 255.255.255.0 IPv6 netmask format is: • /48 (as a part of the network prefix)			
	nexthop-address	The IPv4 or IPv6 address of the next hop router for this route.			
	ifname	The interface name (e.g., mgmt0, mgmt1).			
Default	N/A				
Configuration Mode	Config				
History	3.1.0000				
Role	admin				
Example	switch (config) # ip route 20.20.20.0 255.255.255.0 mgmt0				
	switch (config) # show ip route				
	Destination	Mask	Gateway	Interface	Source
	default	0.0.0.0	172.30.0.1	mgmt0	DHCP
	10.10.10.10	255.255.255.255	0.0.0.0	mgmt0	static
	20.10.10.10	255.255.255.255	172.30.0.1	mgmt0	static
	20.20.20.0	255.255.255.0	0.0.0.0	mgmt0	static
172.30.0.0	255.255.0.0	0.0.0.0	mgmt0	interface	
Related Commands	show ip route				
Note					

ipv6 default-gateway

ipv6 default-gateway {<ip-address> | <ifname>}

no ipv6 default-gateway

Sets a static default gateway.

The no form of the command deletes the default gateway.

Syntax Description	ip address	The default gateway IP address (IPv4 or IPv6).
	ifname	The interface name (e.g., mgmt0, mgmt1).
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	Initial version
	3.2.0500	removed IPv4 configuration option
Role	admin	
Example	<pre>switch (config) # ip default-gateway ::1 switch (config) # show ip default-gateway static Configured default gateways: ::1 switch (config) #</pre>	
Related Commands	show ip route	
Note	- The configured default gateway will not be used if DHCP is enabled. - In order to configure ipv4 default-gateway use 'ip route' command.	

show ip/ipv6 route

show {ip | ipv6} route [static]

Displays the routing table in the system.

Syntax Description	static					Filters the table with the static route entries.																																																																		
Default	N/A																																																																							
Configuration Mode	Any Command Mode																																																																							
History	3.1.0000																																																																							
Role	admin																																																																							
Example	switch (config) # show ip route <table><thead><tr><th>Destination</th><th>Mask</th><th>Gateway</th><th>Interface</th><th>Source</th></tr></thead><tbody><tr><td>default</td><td>0.0.0.0</td><td>172.30.0.1</td><td>mgmt0</td><td>DHCP</td></tr><tr><td>10.10.10.10</td><td>255.255.255.255</td><td>0.0.0.0</td><td>mgmt0</td><td>static</td></tr><tr><td>20.10.10.10</td><td>255.255.255.255</td><td>172.30.0.1</td><td>mgmt0</td><td>static</td></tr><tr><td>20.20.20.0</td><td>255.255.255.0</td><td>0.0.0.0</td><td>mgmt0</td><td>static</td></tr><tr><td>172.30.0.0</td><td>255.255.0.0</td><td>0.0.0.0</td><td>mgmt0</td><td>interface</td></tr></tbody></table> switch (config) # show ipv6 route <table><thead><tr><th>Destination prefix</th><th>Gateway</th><th>Interface</th><th>Source</th></tr></thead><tbody><tr><td colspan="4">-----</td></tr><tr><td>::/0</td><td></td><td></td><td></td></tr><tr><td>::</td><td></td><td>mgmt0</td><td>static</td></tr><tr><td>::1/128</td><td></td><td></td><td></td></tr><tr><td>::</td><td></td><td>lo</td><td>local</td></tr><tr><td>2222:2222:2222::/64</td><td></td><td></td><td></td></tr><tr><td>::</td><td></td><td>mgmt1</td><td>interface</td></tr></tbody></table> switch (config) #										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	Destination prefix	Gateway	Interface	Source	-----				::/0				::		mgmt0	static	::1/128				::		lo	local	2222:2222:2222::/64				::		mgmt1	interface
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																																																																				
Destination prefix	Gateway	Interface	Source																																																																					

::/0																																																																								
::		mgmt0	static																																																																					
::1/128																																																																								
::		lo	local																																																																					
2222:2222:2222::/64																																																																								
::		mgmt1	interface																																																																					
Related Commands	show ip default-gateway																																																																							
Note																																																																								

show ip/ipv6 default-gateway

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

Displays the default gateway.

Syntax Description	static	Displays the static configuration of the default gateway.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	
Example	<pre>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</pre>	
Related Commands	show ip default-gateway	
Note	The configured IPv4 default gateway will not be used if DHCP is enabled.	

4.1.6.4 Network to Media Resolution (ARP & NDP)

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

ip arp

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

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

Syntax Description	IP address	IPv4 address.		
	MAC address	MAC address.		
Default	N/A			
Configuration Mode	Config Interface Management			
History	3.2.0500			
Role	admin			
Example	switch (config interface mgmt0) #ip arp 20.20.20.20 aa:aa:aa:aa:aa:aa			
	switch (config interface mgmt0) # show ip arp			
	ARP Timeout: 1500			
	Total number of entries: 6			
	Address	Type	MAC Address	Interface
	10.209.1.103	Dynamic	00:02:C9:11:A1:78	mgmt0
	10.209.1.168	Dynamic	00:02:C9:5E:C3:28	mgmt0
	10.209.1.104	Dynamic	00:02:C9:11:A1:E6	mgmt0
10.209.1.153	Dynamic	00:02:C9:11:A1:86	mgmt0	
10.209.1.105	Dynamic	00:02:C9:5E:0B:56	mgmt0	
10.209.0.1	Dynamic	00:00:5E:00:01:01	mgmt0	
20.20.20.20	Static	AA:AA:AA:AA:AA:AA	mgmt0	
Related Commands	switch (config interface mgmt0) #			
	show ip arp			
	ip route			
Note				

ip arp timeout

ip arp timeout <timeout-value>

no ip arp timeout

Sets the dynamic ARP cache timeout.

The no form of the command sets the timeout to default.

Syntax Description	timeout-value	Time (in seconds) that an entry remains in the ARP cache. Valid values are from 240 to 28800.
Default	1500 seconds	
Configuration Mode	Config	
History	3.2.0230	
Role	admin	
Example	<pre>switch (config) # ip arp timeout 2000 switch (config) # show ip arp ARP Timeout: 2000 Total number of entries: 55 IP Address MAC Address Interface 1.0.0.2 00:02:c9:5c:30:40 Vlan11 1.0.0.3 00:11:22:33:44:55 Vlan11 2.0.0.2 00:02:c9:5c:30:40 Vlan12 3.0.0.2 00:02:c9:5c:30:40 Vlan13 4.0.0.2 00:02:c9:5c:30:40 Vlan14 switch (config) #</pre>	
Related Commands	<pre>ip arp show ip arp</pre>	
Note	This value is used as the ARP timeout whenever a new IP interface is created.	

show ip arp

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

Displays ARP table.

Syntax Description	interface type	Filters the table according to a specific interface (i.e. mgmt0)		
	ip-address	Filters the table to the specific ip-address		
	count	Shows ARP statistics		
Default	N/A			
Configuration Mode	Any Command Mode			
History	3.3.3000			
Role	admin			
Example	switch-626a54 [standalone: master] (config) # show ip arp			
	Total number of entries: 3			
	Address	Type	Hardware Address	Interface

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

ipv6 neighbor

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

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

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

clear ipv6 neighbors

clear ipv6 neighbors

Clears the dynamic neighbors cache.

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

show ipv6 neighbors

show ipv6 neighbors [static]

Displays the Neighbor Discovery Protocol (NDP) table.

Syntax Description	static	Filters only the table of the static entries.													
Default	N/A														
Configuration Mode	Config														
History	3.1.0000														
Role	admin														
Example	switch (config) # show ipv6 neighbors <table><thead><tr><th>IPv6 Address</th><th>Age</th><th>MAC Address</th><th>State</th><th>Interf</th></tr></thead><tbody><tr><td>2001::2</td><td>9428</td><td>AA:AA:AA:AA:AA:AA</td><td>permanent</td><td>mgmt0</td></tr></tbody></table> switch (config) #					IPv6 Address	Age	MAC Address	State	Interf	2001::2	9428	AA:AA:AA:AA:AA:AA	permanent	mgmt0
IPv6 Address	Age	MAC Address	State	Interf											
2001::2	9428	AA:AA:AA:AA:AA:AA	permanent	mgmt0											
Related Commands	ipv6 neighbor clear ipv6 neighbor show ipv6														
Note															

4.1.6.5 DHCP

ip dhcp

ip dhcp {default-gateway yield-to-static| hostname <hostname>| primary-intf <iface> | 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 <iface>	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	<pre> switch (config) # ip dhcp default-gateway yield-to-static switch (config) # show ip dhcp DHCP primary interface: Configured: mgmt0 Active: mgmt0 DHCP: yield default gateway to static configuration: yes DHCP Client Options: Send Hostname: no Client Hostname: switch (using system hostname) switch (config) # </pre>	
Related Commands	show ip dhcp dhcp [renew]	
Note	DHCP is supported for IPv4 networks only.	

show ip dhcp

show ip dhcp

Displays the DHCP configuration and status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	<pre>ip dhcp dhcp [renew]</pre>
Note	

4.1.6.6 IP Diagnostic Tools

ping

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

Sends ICMP echo requests to a specified host.

Syntax Description	Linux Ping options http://linux.about.com/od/commands/l/blcmdl8_ping.htm
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	tracert
Note	

traceroute

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

Traces the route packets take to a destination.

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

Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	
Note	

tcpdump

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

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

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	N/A
Note	

4.2 NTP, Clock & Time Zones

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

4.2.1 Commands

clock set

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

Sets the time and date.

Syntax Description	hh:mm:ss	Time.
	yyyy/mm/dd	Date.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show clock	
Note	If not specified, the date will be left the same.	

clock timezone

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

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

- A nearby city whose time zone rules to follow. The system has a large list of cities which can be displayed by the help and completion system. They are organized hierarchically because there are too many of them to display in a flat list. A given city may be required to be specified in two, three, or four words, depending on the city.
 - An offset from UTC. This will be in the form UTC-offset UTC, UTC-offset UTC+<0-14>, UTC-offset UTC-<1-12>.
 - UTC (Universal Time, which is almost identical to GMT), and this is the default time zone
- The no form of the command resets time zone to its default (GMT).

Syntax Description	zone word	The possible forms this could take include: continent, city, continent, country, city, continent, region, country, city, ocean, and/or island.
Default	GMT	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show clock	
Note		

ntp

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

Configures NTP.

The no form of the command negates NTP options.

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

ntpdate

ntpdate <IP address>

Sets the system clock using the specified SNTP server.

Syntax Description	IP address	IP.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	N/A	
Note	This is a one-time operation and does not cause the clock to be kept in sync on an ongoing basis. It will generate an error if SNTP is enabled since the socket it requires will already be in use.	

show clock

show clock

Displays the current system time, date and time zone.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>switch (config) # show clock Time: 04:21:44' Date: 2012/02/26 Time zone: America North United_States Other New_York switch (config) #</pre>
Related Commands	N/A
Note	

show ntp

show ntp

Displays the current NTP settings.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>switch (config) # show ntp NTP is enabled. Clock is unsynchronized. No NTP peers or servers configured. switch (config) #</pre>
Related Commands	N/A
Note	

-
-

4.3 Software Management

4.3.1 Upgrading MLNX-OS Software – Preconditions

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

To remove old configuration:

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

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

Step 2. Follow the steps described in Section 4.3.2, “Upgrading MLNX-OS Software,” on page 129.

4.3.2 Upgrading MLNX-OS Software



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



The system being upgraded becomes indisposed throughout the upgrade procedure.



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



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

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

Step 1. Change to Config mode.

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

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

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

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

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

Images available to be installed:

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

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

No image install currently in progress.

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

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

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



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

- Step 4.** Fetch the new software image.

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

- Step 5.** Display the available images.



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

```
image boot next
image boot location.
```

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

```

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

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

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

No image install currently in progress.

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

```

Step 6. Install the new image.

```

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

```



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

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

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

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

```

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

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

```

```

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

Last boot partition: 1
Next boot partition: 2

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

```

Step 9. Save current configuration. Run:

```

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

```

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

```

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

```



After software reboot, the software upgrade will also automatically upgrade the firm-ware version.



On SX65xx systems with dual management, the software must be upgraded on both the Master and the Slave units.



In order to upgrade the system on dual management system refer to Section 4.3.2, “Upgrading MLNX-OS Software,” on page 129.



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

4.3.3 Deleting Unused Images

➤ *To delete unused images:*

Step 1. Enter Config mode. Run:

```

switch >
switch > enable
switch # configure terminal

```

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

```
switch (config) # show images
Images available to be installed:
  image-PPC_M460EX-SX_3.1.1224.img
  SX-OS_PPC_M460EX SX_3.1.1224 2011-04-28 12:29:48 ppc
Installed images:
Partition 1:
SX-OS_PPC_M460EX 3.1.0000-dev-HA 2011-04-10 12:02:49 ppc
Partition 2:
SX-OS_PPC_M460EX 3.1.0000-dev-HA 2011-04-10 12:02:49 ppc

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

Step 3. Delete the unused images. Run:

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



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

4.3.4 Downgrading MLNX-OS Software

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

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

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

1. Change to Config mode. Run:

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

2. Disable paging of CLI output. Run:

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

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

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

4. Copy the output to a text file.

4.3.4.1 Downloading Image

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

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

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

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

Step 3. Enter your username and password when prompted.

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

Step 5. Change to Config mode. Run:

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

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

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

Step 7. Fetch the requested software image. Run:

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

4.3.4.2 Downgrading Image



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

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

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

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

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

```
switch (config) # image install <image_name>
Step 1 of 4: Verify Image
```

```

100.0% [#####]
Step 2 of 4: Uncompress Image
100.0% [#####]
Step 3 of 4: Create Filesystems
100.0% [#####]
Step 4 of 4: Extract Image
100.0% [#####]
switch (config) #

```

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

```

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

```

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

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



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



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

```

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

```

Step 7. Reload the switch. Run:

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

4.3.4.3 Switching to Partition with Older Software Version

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

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

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

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

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

Step 1. Run the command:

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

Step 2. Set the boot partition. Run:

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

Step 3. Save the configuration. Run:

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

Step 4. Reload the system. Run:

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

4.3.5 Upgrading System Firmware

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

4.3.5.1 After Updating MLNX-OS Software

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

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



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

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

Some subsystems are not updated with a default firmware.



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

4.3.5.2 Importing Firmware and Changing the Default Firmware

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

Default Firmware Change on Standalone Systems

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

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

Step 2. Save the configuration. Run:

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

Step 3. Reboot the system to enable auto update.

Step 4.

4.3.6 Commands

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

image boot

image boot {location <location ID> | next}

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

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

boot next

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

Sets the default setting for next boot. Normally, if the system fails to apply the configuration on startup (after attempting upgrades or downgrades, as appropriate), it will reboot to the other partition as a fallback.

The no form of the command tells the system not to do that, only for the next boot.

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

image default-chip-fw

image default-chip-fw <file name>

Sets the default firmware package to be installed.

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

image delete

image delete <image name>

Deletes the specified image file.

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

image fetch

image fetch <URL> [<filename>]

Downloads an image from the specified URL or via SCP.

Syntax Description	URL	HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username[:password]@host-name/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	<pre>switch (config) # image fetch scp://<username>@192.168.10.125/var/www/ html/<image_name> Password ***** 100.0%[#####] switch (config) #</pre>	
Related Commands	show images	
Note	• Please delete the previously available image, prior to fetching the new image • See section “Upgrading MLNX-OS SX Software,” in the <i>Mellanox SwitchX® User Manual</i> 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	<pre>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) #</pre>	
Related Commands	show images	
Note	- The image cannot be installed on the “active” location (the one which is currently being booted) - On a two-location system, the location is chosen automatically if no location is specified	

image move

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

Renames the specified image file.

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

image options

image options require-sig
no image options require-sig

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

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

show bootvar

show bootvar

Displays the installed system images and the boot parameters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	N/A
Note	

show images

show image

Displays information about the system images and boot parameters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	N/A
Note	

4.4 Configuration Management

4.4.1 Saving a Configuration File

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

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

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

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

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

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

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

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

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

4.4.2 Loading a Configuration File

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

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

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

4.4.3 Managing Configuration Files

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

4.4.3.1 BIN Configuration Files

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

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

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

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

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

➤ **To fetch a BIN configuration file**

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

➤ **To see the available configuration files**

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

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

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

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



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

4.4.3.2 Text Configuration Files

Text configuration files are text based and editable.

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

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

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

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



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

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

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

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

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

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

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



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

4.4.4 Commands

4.4.4.1 File System

debug generate dump

debug generate dump

Generates a debug dump.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	switch (config) # debug generate dump Generated dump sysdump-switch-112104-201140526-091707.tgz switch (config) #
Related Commands	file debug-dump
Note	The dump can then be manipulated using the “file debug-dump...” commands.

file debug-dump

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

Manipulates debug dump files.

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

file stats

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

Manipulates statistics report files.

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

file tcpdump

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

Manipulates tcpdump output files.

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

reload

reload [force | halt [noconfirm] | noconfirm]

Reboots or shuts down the system.

Syntax Description	force	Forces an immediate reboot of the system even if the system is busy.
	halt	Shuts down the system.
	noconfirm	Reboots the system without asking about unsaved changes.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # reload Configuration has been modified; save first? [yes] yes Configuration changes saved. ... switch (config) #</pre>	
Related Commands	reset factory	
Note		

show files debug-dump

show files debug-dump [<filename>]

Displays a list of debug dump files.

Syntax Description	filename	Displays a summary of the contents of a particular debug dump file.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	file debug-dump	
Note		

show files stats

show files stats <filename>

Displays a list of statistics report files.

Syntax Description	filename	Display the contents of a particular statistics report file.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # show files stats memory-201140524-111745.csv switch (config) #</pre>	
Related Commands	file stats	
Note		

show files system

show files system [detail]

Displays usage information of the file systems on the system.

Syntax Description	detail	Displays more detailed information on file-system.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	N/A	
Note		

show files tcpdump

show files tcpdump

Displays a list of statistics report files.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	switch (config) # show files stats test dump3 switch (config) #
Related Commands	file tcpdump tcpdump
Note	

4.4.4.2 Configuration Files

configuration audit

configuration audit max-changes <number>

Chooses settings related to configuration change auditing.

Syntax Description	max-changes	Set maximum number of audit messages to log per change.
Default	1000	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # configuration audit max-changes 100 switch (config) # show configuration audit Maximum number of changes to log: 100 switch (config) #</pre>	
Related Commands	show configuration	
Note	N/A	

configuration copy

configuration copy <source name> <dest name>

Copies a configuration file.

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

configuration delete

configuration delete <filename>

Deletes a configuration file.

Syntax Description	filename	Name of file to delete.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show configuration	
Note	• This command does not affect the current running configuration • The active configuration file may not be deleted	

configuration fetch

configuration fetch <URL or scp or sftp://username:password@hostname[:port]/path/filename> [<name>]

Downloads a configuration file from a remote host.

Syntax Description	name	The configuration file name.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # configuration fetch scp://root:password@ 192.168.10.125/tmp/conf1 switch (config) #</pre>	
Related Commands	configuration switch-to	
Note	• The downloaded file should not override the active configuration file, using the <name> parameter • If no name is specified for a configuration fetch, it is given the same name as it had on the server • No configuration file may have the name “active”	

configuration jump-start

configuration jump-start

Runs the initial-configuration wizard.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	N/A
Note	- The wizard is automatically invoked whenever the CLI is launched when the active configuration file is fresh (i.e. not modified from its initial contents) - This command invokes the wizard on demand – see chapter “Initializing the Switch for the First Time” in the Mellanox <i>MLNX-OS SwitchX User Manual</i>

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	<pre>switch (config) # configuration merge new-config-file switch (config) #</pre>	
Related Commands		
Note	• No configuration files are modified during this process • The configuration name must be a non-active configuration file	

configuration move

configuration move <source name> <dest name>

Moves a configuration file.

Syntax Description	source name	Old name of file to move.
	dest name	New name for moved file.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show configuration	
Note	• This command does not affect the current running configuration • The active configuration file may not be the target of a move	

configuration new

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

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

Syntax Description	filename	Names for new configuration file.
	factory	Creates new file with only factory defaults.
	keep-basic	Keeps licenses and host keys.
	keep-connect	Keeps configuration necessary for connectivity (interfaces, routes, and ARP).
Default	Keeps licenses and host keys	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show configuration	
Note		

configuration switch-to

configuration switch-to <filename>

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

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	show configuration files
Note	The current running configuration is lost and not automatically saved to the previous active configuration file.

configuration text fetch

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

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

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

configuration text file

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

Performs operations on text-based configuration files.

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

configuration text generate

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

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

Syntax Description	active	Generates from currently active configuration.
	running	Uses running configuration.
	saved	Uses saved configuration.
	file <filename>	Generates from inactive saved configuration.
	save	Saves new file to local persistent storage.
	upload <URL>	Supported types are HTTP, HTTPS, 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	<pre>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) #</pre>	
Related Commands	show configuration files	
Note		

configuration upload

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

Uploads a configuration file to a remote host.

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

write

write {memory [local] | terminal}

Saves or displays the running configuration.

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

show configuration

show configuration [audit | files [<filename>] | 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.
	full	Does not exclude commands that set default values.
	text files	Displays names of available text-based configuration files.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5000	Removed “running” and “full” parameters
Role	monitor/admin	
Example	<pre>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) #</pre>	
Related Commands		
Note		

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	<pre> 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) # </pre>
Related Commands	
Note	

4.5 Logging

4.5.1 Monitor

➤ *To print logging events to the terminal:*

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

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

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

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

To see a list of the events, refer to [Table 20, “Supported Event Notifications and MIB Mapping,” on page 209](#).

4.5.2 Remote Logging

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

Step 1. Enter Config mode. Run:

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

Step 2. Set remote syslog server. Run

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

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

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

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

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

4.5.3 Switch Power-On Self-Test

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

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

Table 19 lists the POST return codes and their meanings.

Table 19 - POST Return Codes

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

Table 19 - POST Return Codes

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

4.5.4 Commands

logging local override

logging local override [class <class> priority <log-level>]

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

Enables class-specific overrides to the local log level.

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

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

Example

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

Related Commands

```
show logging
logging local
```

Note

logging <syslog IP address>

logging <syslog IP address> [trap {<log-level> | override class <class> priority <log-level>}]

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

Enables (by setting the IP address) sending logging messages, with ability to filter the logging messages according to their classes.

The no form of the command stops sending messages to the remote syslog server.

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

Example

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

Related Commands

```
show logging
logging local override
```

Note

logging receive

logging receive
no logging receive

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

Syntax Description	N/A
Default	Receiving logging is disabled
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	<pre>show logging logging local logging local override</pre>
Note	• This does not log to the console TTY port • In-band management should be enabled in order to open a channel from the host to the CPU • If enabled, only log messages matching or exceeding the minimum severity specified with the “logging local” command will be logged, regardless of what is sent from the remote host

logging format

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

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

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

logging fields

logging fields seconds {enable | fractional-digits <f-digit> | whole-digits <w-digit>}

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

Specifies whether to include an additional field in each log message that shows the number of seconds since the Epoch or not.

The no form of the command disallows including an additional field in each log message that shows the number of seconds since the Epoch.

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

Related Commands	show logging
-------------------------	--------------

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

logging level

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

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

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

logging files delete

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

Deletes the current or oldest log files.

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

logging files rotation

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

Sets the rotation criteria of the logging files.

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

Example

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

Related Commands

```
show logging
show log files
```

Note

logging files upload

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

Uploads a log file to a remote host.

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

logging monitor

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

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

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

logging debug-files

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

Configures settings for debug log files.

Syntax Description	delete {current oldest}	Deletes certain debug-log files. - current: Deletes the current active debug-log file - oldest: Deletes some of the oldest debug-log files
	rotation {criteria {frequency {daily weekly monthly} size <size> size-pct <percentage>} force max-num}	Configures automatic rotation of debug-logging files. - criteria: Sets how the system decides when to rotate debug files. - frequency: Rotate log files on a fixed time-based schedule - size: Rotate log files when they pass a size threshold in megabytes - size-pct: Rotate logs when they surpass a specified percentage of disk - forces: Forces an immediate rotation of the log files - max-num: Specifies the maximum number of old log files to keep
	update {<number> current}	Uploads a local debug-log file to a remote host. - current: Uploads log file “messages” to a remote host - number: Uploads compressed log file “debug.<number>.gz” to a remote host. Range is 1-10.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	<pre>switch (config) # logging debug-files delete current switch (config) #</pre>	
Related Commands		
Note		

show logging

show logging

Displays the logging configurations.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	<pre>logging fields logging files rotation logging level logging local logging receive logging <syslog IP address></pre>
Note	

show log

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

Displays the log file with optional filter criteria.

Syntax Description	continues	Displays the last few lines of the current log file and then continues to display new lines as they come in until the user hits Ctrl+C, similar to LINUX “tail” utility.
	files	Displays the list of log files.
	<file-number>	Displays an archived log file, where the number may range from 1 up to the number of archived log files available.
	[not] matching <reg-exp>	The file is piped through a LINUX “grep” utility to only include lines either matching, or not matching, the provided regular expression.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
	3.3.4402	Updated example and added note
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	logging fields logging files rotation logging level logging local logging receive logging <syslog IP address> show logging	
Note	When using a regular expression containing (OR), the expression should be surrounded by quotes (“<expression>”), otherwise it is parsed as filter (PIPE) command.	

4.6 Debugging

➤ *To use the debugging logs feature:*

Step 1. Enable debugging. Run:

Step 2. Display the debug level set. Run:

Step 3. Display the logs. Run:

4.6.1 Commands

debug ethernet all

debug ethernet all
no debug ethernet all

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

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

debug ethernet dcbx

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

Configures the trace level for DCBX.

The no form of the command disables the configured DCBX debug traces.

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

debug ethernet ip

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

Enables debug traces for Ethernet routing specific modules.

The no form of the command disables the debug traces for ethernet routing protocols.

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

Related Commands

Note

debug ethernet lacp

debug ethernet lacp {all | all-resource | data-path | fail-all | init-shut | management | memory | packet}

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

Configures the trace level for LACP.

The no form of the command disables the configured LACP debug traces.

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

debug ethernet lldp

debug ethernet lldp {all | control-panel | critical-event | data-path | fail-all | init-shut | management | memory | neigh-add | neigh-age-out | neigh-del | neigh-drop | neigh-updt | tlv}

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

Configures the trace level for LLDP.

The no form of the command disables the configured LLDP debug traces.

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

debug ethernet port

debug ethernet port all

Configures the trace level for port.

The no form of the command disables the configured port debug traces.

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

debug ethernet qos

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

Configures the trace level for QoS.

The no form of the command disables the configured QoS debug traces.

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

debug ethernet spanning-tree

debug ethernet spanning-tree {all | error | event | filters | init-shut | management | memory | packet | port-info-state-machine | port-receive-state-machine | port-role-selection-state-machine | port-transit-state-machine | port-transmit-state-machine | protocol-migration-state-machine | timers}

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

Configures the trace level for spanning-tree.

The no form of the command disables the configured spanning-tree debug traces.

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

Related Commands

Note

debug ethernet vlan

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

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

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

show debug ethernet

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

Displays debug level configuration on a specific switch.

Syntax Description	dcbx	Displays the trace level for spanning tree.
	ip	Displays debug trace level for ethernet routing module. • arp • dhcp-relay • igmp-snooping • interface • ospf
	lacp	Displays the trace level for LACP.
	lldp	Displays the trace level for LLDP.
	port	Displays the trace level for port.
	qos	Displays the trace level for QoS.
	spanning-tree	Displays the trace level for spanning tree.
	vlan	Displays the trace level for VLAN.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4150	
Role	admin	
Example	<pre>switch (config) # show debug ethernet dcbx dcbx protocol : management is ON fail-all is ON control-panel is ON tlv is ON switch (config) #</pre>	
Related Commands		
Note		

show log debug

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

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

Syntax Description	continuous	Displays new event log messages as they arrive.
	files	Displays archived debug log files.
	matching	Displays event debug logs that match a given regular expression.
	not	Displays event debug logs that do not meet certain criteria.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4150	
Role	admin	
Example	<pre>switch (config) # show log debug Jun 15 16:20:47 switch-627e4c last message repeated 7 times Jun 15 16:20:47 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>QoShwQueueDelete i4IfIndex[137] Jun 15 16:20:47 switch-627e4c last message repeated 7 times Jun 15 16:20:47 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>QoShwQueueDelete i4IfIndex[141] Jun 15 16:20:47 switch-627e4c last message repeated 7 times Jun 15 16:20:48 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: ==FshwSetSpeed sx_api_port_speed_admin_set = 0 Jun 15 16:20:48 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: ==FshwGetSpeed sx_api_port_speed_oper_get = 0 Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[89], u1ConfigOption[6] Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[33], u1ConfigOption[6] Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[73], u1ConfigOption[6] Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[121], u1ConfigOption[6] Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[133], u1ConfigOption[6] Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[13], u1ConfigOption[6] Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[81], u1ConfigOption[6] Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[117], u1ConfigOption[6] Jun 15 16:20:49 switch-627e4c issd[6509]: TID 1274844336: [issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[65], u1ConfigOption[6] . . . switch (config) #</pre>	
Related Commands		
Note		

4.7 Event Notifications

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

4.7.1 Supported Events

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

Table 20 - 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 ² C) 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 20 - 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: <code>snmp-server notify send-test</code>	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 SNMP Trap Notifications

To set SNMP notification see [Section 4.13.1.6, “Configuring an SNMP Notification,”](#) on page 345.

4.7.3 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) #
```

4.7.4 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.

4.7.5 Commands

4.7.5.1 Email Notification

email autosupport ssl mode

email autosupport ssl mode {none | tls | tls-none}

no email autosupport ssl mode

Configures type of security to use for auto-support email.

The no form of the command resets auto-support email security mode to its default.

Syntax Description	none	Does not use TLS to secure auto-support email.
	tls	Uses TLS over the default server port to secure auto-support email and does not send an email if TLS fails.
	tls-none	Attempts TLS over the default server port to secure auto-support email, and falls back on plaintext if this fails.
Default	tls-none	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	switch (config) # email autosupport ssl mode tls	
Related Commands	N/A	
Note		

email autosupport ssl cert-verify

email autosupport ssl cert-verify
no email autosupport ssl cert-verify

Verifies server certificates.

The no form of the command does not verify server certificates.

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

email autosupport ssl ca-list

email autosupport ssl ca-list {<ca-list-name> | default_ca_list | none}
no email autosupport ssl ca-list

Configures supplemental CA certificates for verification of server certificates.
 The no form of the command removes supplemental CA certificate list.

Syntax Description	default_ca_list	Default supplemental CA certificate list.
	none	No supplemental list; uses built-in list only.
Default	default_ca_list	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	switch (config) # email autosupport ssl ca-list default_ca_list	
Related Commands	N/A	
Note		

email dead-letter

email dead-letter {cleanup max-age <duration> | enable}
no email dead-letter

Configures settings for saving undeliverable emails.
 The no form of the command disables sending of emails to vendor auto-support upon certain failures.

Syntax Description	duration	Example: “5d4h3m2s” for 5 days, 4 hours, 3 minutes, 2 seconds.
	enable	Saves dead-letter files for undeliverable emails.
Default	Save dead letter is enabled The default duration is 14 days	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	switch (config) # email dead-letter enable switch (config) #	
Related Commands	show email	
Note		

email domain

email domain <hostname or IP address>

no email domain

Sets the domain name from which the emails will appear to come from (provided that the return address is not already fully-qualified). This is used in conjunction with the system hostname to form the full name of the host from which the email appears to come.

The no form of the command clears email domain override.

Syntax Description	hostname or IP address	IP address.
Default	No email domain	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show emails	
Note		

email mailhub

email mailhub <hostname or IP address>

no email mailhub

Sets the mail relay to be used to send notification emails.

The no form of the command clears the mail relay to be used to send notification emails.

Syntax Description	hostname or IP address	Hostname or IP address.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show email [events]	
Note		

email mailhub-port

email mailhub-port <hostname or IP address>

no email mailhub-port

Sets the mail relay port to be used to send notification emails.
The no form of the command resets the port to its default.

Syntax Description	hostname or IP address	hostname or IP address.
Default	25	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show email	
Note		

email notify event

email notify event <event name>

no email notify event <event name>

Enables sending email notifications for the specified event type.

The no form of the command disables sending email notifications for the specified event type.

Syntax Description	event name	Example event names would include “process-crash” and “cpu-util-high”.
Default	No events are enabled	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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 hung switch (config) # switch (config) #</pre>	
Related Commands	show email	
Note	This does not affect auto-support emails. Auto-support can be disabled overall, but if it is enabled, all auto-support events are sent as emails.	

email notify recipient

email notify recipient <email addr> [class {info | failure} | detail]
no email notify recipient <email addr> [class {info | failure} | detail]

Adds an email address from the list of addresses to which to send email notifications of events.

The no form of the command removes an email address from the list of addresses to which to send email notifications of events.

Syntax Description	email addr	Email address of intended recipient.
	class	Specifies which types of events are sent to this recipient.
	info	Sends informational events to this recipient.
	failure	Sends failure events to this recipient.
	detail	Sends detailed event emails to this recipient.
Default	No recipients are added	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show email	
Note		

email return-addr

email return-addr <username>
no email domain

Sets the username or fully-qualified return address from which email notifications are sent.

- If the string provided contains an “@” character, it is considered to be fully-qualified and used as-is.
- Otherwise, it is considered to be just the username, and we append “@<host-name>.<domain>”. The default is “do-not-reply”, but this can be changed to “admin” or whatnot in case something along the line does not like fictitious addresses.

The no form of the command resets this attribute to its default.

Syntax Description	username	Username.
Default	do-not-reply	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show email	
Note		

email return-host

email return-host
no email return-host

Includes the hostname in the return address for emails.
 The no form of the command does not include the hostname in the return address for emails.

Syntax Description	N/A
Default	No return host
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	show email
Note	This only takes effect if the return address does not contain an "@" character.

email send-test

email send-test

Sends test-email to all configured event and failure recipients.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	switch (config) # email autosupport enable switch (config) #
Related Commands	show email [events]
Note	

email ssl mode

email ssl mode {none | tls | tls-none}

no email ssl mode

Sets the security mode(s) to try for sending email.

The no form of the command resets the email SSL mode to its default.

Syntax Description	none	No security mode, operates in plaintext.
	tls	Attempts to use TLS on the regular mailhub port, with STARTTLS. If this fails, it gives up.
	tls-none	Attempts to use TLS on the regular mailhub port, with STARTTLS. If this fails, it falls back on plaintext.
Default	default-cert	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	switch (config) # email ssl mode tls-none	
Related Commands	N/A	
Note		

email ssl cert-verify

email ssl cert-verify
no email ssl cert-verify

Enables verification of SSL/TLS server certificates for email.
The no form of the command disables verification of SSL/TLS server certificates for email.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.2.3000
Role	admin
Example	switch (config) # email ssl cert-verify
Related Commands	N/A
Note	This command has no impact unless TLS is used.

email ssl ca-list

email ssl ca-list {<ca-list-name> | default-ca-list | none}
no email ssl ca-list

Specifies the list of supplemental certificates of authority (CA) from the certificate configuration database that is to be used for verification of server certificates when sending email using TLS, if any.

The no form of the command uses no list of supplemental certificates.

Syntax Description	ca-list-name	Specifies CA list name.
	default-ca-list	Uses default supplemental CA certificate list.
	none	Uses no list of supplemental certificates.
Default	default-ca-list	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	switch (config) # email ssl ca-list none	
Related Commands	N/A	
Note	This command has no impact unless TLS is used, and certificate verification is enabled.	

show email

show email [events]

Shows email configuration or events for which email should be sent upon.

Syntax Description	events	show event list
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show email	
Note		

4.8 mDNS

Multicast DNS (mDNS) protocol is used by the SM HA to deliver control information between the InfiniBand nodes via the management interface.

- ***In order to block sending mDNS traffic from the management interface use the following command:***

4.8.1 Commands

ha dns enable

ha dns enable
no ha dns enable

Allows mDNS traffic.
The no form of the command blocks mDNS traffic from being sent from mgmt0.

Syntax Description	N/A
Default	Enabled.
Configuration Mode	Config
History	3.3.4000
Role	admin
Example	switch (config) # no ha dns enable switch (config) #
Related Commands	
Note	

4.9 User Management and Security

4.9.1 Authentication, Authorization and Accounting (AAA)

AAA is a term describing a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing the MLNX-OS switch. The MLNX-OS switch supports Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control device Plus (TACACS+) protocols.

- **Authentication** - authentication provides the initial method of identifying each individual user, typically by entering a valid username and password before access is granted. The AAA server compares a user's authentication credentials with the user credentials stored in a database. If the credentials match, the user is granted access to the network or devices. If the credentials do not match, authentication fails and network access is denied.
- **Authorization** - following the authentication, a user must gain authorization for performing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.
- **Accounting** - the last level is accounting, which measures the resources a user consumes during access. This includes the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information, and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

Authentication, authorization, and accounting services are often provided by a dedicated AAA server, a program that performs these functions. Network access servers interface with AAA servers using the Remote Authentication Dial-In User Service (RADIUS) protocol.

4.9.1.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service), widely used in network environments, is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for embedded network devices such as routers, modem servers, switches and so on. RADIUS is currently the de-facto standard for remote authentication. It is prevalent in both new and legacy systems.

It is used for several reasons:

- RADIUS facilitates centralized user administration
- RADIUS consistently provides some level of protection against an active attacker

4.9.1.2 TACACS+

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for providing NAS (Network Access Security). NAS ensures secure access from remotely connected users. TACACS implements the TACACS Client and provides the AAA (Authentication, Authorization and Accounting) functionalities.

TACACS is used for several reasons:

- Facilitates centralized user administration
- Uses TCP for transport to ensure reliable delivery
- Supports inbound authentication, outbound authentication and change password request for the authentication service
- Provides some level of protection against an active attacker

4.9.1.3 LDAP

LDAP (Lightweight Directory Access Protocol) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. LDAP is based on a client/server model. The switch acts as a client to the LDAP server. A remote user (the remote administrator) interacts only with the switch, not the back-end server and database.

LDAP authentication consists of the following components:

- A protocol with a frame format that utilizes TCP over IP
- A centralized server that stores all the user authorization information
- A client: in this case, the switch

Each entry in the LDAP server is referenced by its Distinguished Name (DN). The DN consists of the user-account name concatenated with the LDAP domain name. If the user-account name is John, the following is an example DN:

```
uid=John,ou=people,dc=domain,dc=com
```

4.9.2 User Accounts

There are two user account types: *admin* and *monitor*. As *admin*, the user is privileged to execute all the available operations. As *monitor*, the user can execute operations that display system configuration and status, or set terminal settings.

Table 21 - User Roles (Accounts) and Default Passwords

User Role	Default Password
admin	admin
monitor	monitor

4.9.3 Commands

4.9.3.1 User Accounts

username

username <username> [capability <cap> | disable [login | password] | full-name <name> | nopassword | password [0 | 7] <password>]
no username <username> [capability | disable [login | password] | full-name]

Creates a user and sets its capabilities, password and name.
 The no form of the command deletes the user configuration.

Syntax Description	username	Specifies a username and creates a user account. New users are created initially with admin privileges but is disabled.
	cap	User capabilities: • admin - full administrative capabilities • monitor - read only capabilities and actions, can not change the running configuration
	disable [login password]	• Disable - disable this account • Disable login - disable all logins to this account • Disable password - disable login to this account using a local password
	name	Full name of the user.
	nopassword	The next login of the user will not require password.
	0 7	• 0: specifies a login password in cleartext • 7: specifies a login password in encrypted text
	password	Specifies a password for the user in string form. If [0 7] was not specified then the password is in cleartext.
	Default	The following usernames are available by default: • admin • monitor • xmladmin • xmluser
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	

Example

```

switch (config) # username monitor full-name smith
switch (config) # show usernames
USERNAME      FULL NAME      CAPABILITY  ACCOUNT STATUS
USERID        System Administrator  admin      Password set
admin         System Administrator  admin      Password set
monitor       smith                monitor    Password set (SHA512)
xmladmin      XML Admin User           admin      No password required
xmluser       XML Monitor User          monitor    No password required
switch (config) #

```

Related Commands

```

show usernames
show users

```

Note

- To enable a user account, just set a password on it (or use the "... nopassword" command to enable it with no password required for login)
- Removing a user account does not terminate any current sessions that user has open; it just prevents new sessions from being established
- Encrypted password is useful for the "show configuration" command, since the cleartext password cannot be recovered after it is set

show usernames

show usernames

Displays list of users and their capabilities.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>switch (config) # show usernames USERNAME FULL NAME CAPABILITY ACCOUNT STATUS USERID 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) #</pre>
Related Commands	username show users
Note	

show users

show users [history]

Displays logged in users and related information such as idle time and what host they have connected from.

Syntax Description	history	Displays current and historical sessions.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	username show usernames	
Note		

show whoami

show whoami

Displays username and capabilities of user currently logged in.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	switch (config) # show whoami Current user: admin Capabilities: admin switch (config) #
Related Commands	username show usernames show users
Note	

4.9.3.2 AAA Methods

aaa accounting

aaa accounting changes default stop-only tacacs+
no aaa accounting changes default stop-only tacacs+

Enables logging of system changes to an AAA accounting server.
 The no form of the command disables the accounting.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000 Initial version 3.2.3000 Removed 'time' parameter from the command.
Role	admin
Example	<pre>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) #</pre>
Related Commands	show aaa
Note	• TACACS+ is presently the only accounting service method supported • Change accounting covers both configuration changes and system actions that are visible under audit logging, however this feature operates independently of audit logging, so it is unaffected by the "logging level audit mgmt" or "configuration audit" commands • Configured TACACS+ servers are contacted in the order in which they appear in the configuration until one accepts the accounting data, or the server list is exhausted • Despite the name of the "stop-only" keyword, which indicates that this feature logs a TACACS+ accounting "stop" message, and in contrast to configuration change accounting, which happens after configuration database changes, system actions are logged when the action is started, not when the action has completed

aaa authentication login

aaa authentication login default <auth method> [<auth method> [<auth method> [<auth method> [<auth method>]]]]
no aaa authentication login

Sets a sequence of authentication methods. Up to four methods can be configured. The no form of the command resets the configuration to its default.

Syntax Description	auth-method • local • radius • tacacs+ • ldap
Default	local
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	show aaa
Note	The order in which the methods are specified is the order in which the authentication is attempted. It is required that “local” is one of the methods selected. It is recommended that “local” be listed first to avoid potential problems logging in to local accounts in the face of network or remote server issues.

aaa authentication attempts track enable

aaa authentication attempts track enable
no aaa authentication attempts track enable

Enables tracking of authentication failures.
The no form of the command disables tracking of authentication failures.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.2.3000
Role	admin
Example	switch (config) # aaa authentication attempts track enable
Related Commands	N/A
Note	• This is required for the lockout functionality described below, but can also be used on its own for informational purposes. • Disabling tracking does not clear any records of past authentication failures, or the locks in the database. However, it does prevent any updates to this database from being made: no new failures are recorded. It also disables lockout, preventing new lockouts from being recorded and existing lockouts from being enforced.

aaa authentication attempts logout

aaa authentication attempts logout {enable | lock-time | max-fail | unlock-time}
no aaa authentication attempts logout {enable | lock-time | max-fail | unlock-time}

Configures logout of accounts based on failed authentication attempts.
The no form of the command clears configuration for logout 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 <code>pam_tallybyname</code> 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 logout enable
Related Commands	N/A
Note	

aaa authentication attempts class-override

aaa authentication attempts class-override {admin [no-lockout] | unknown {no-track | hash-username}}

no aaa authentication attempts class-override {admin | unknown {no-track | hash-username}}

Overrides the global settings for tracking and lockouts for a type of account. The no form of the command removes this override and lets the admin be handled according to the global settings.

Syntax Description	admin	Overrides the global settings for tracking and lockouts for the admin account. This applies only to the single account with the username “admin”. It does not apply to any other users with administrative privileges.
	no-lockout	Prevents the admin user from being locked out, though the authentication failure history is still tracked (if tracking is enabled overall).
	unknown	Overrides the global settings for tracking and lockouts for unknown accounts. The “unknown” class here contains the following categories: • Real remote usernames which simply failed authentication • Mis-typed remote usernames • Passwords accidentally entered as usernames • Bogus usernames made up as part of an attack on the system
	hash-username	Applies a hash function to the username, and stores the hashed result in lieu of the original.
	no-track	Does not track authentication for such users (which of course also implies no-lockout).
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	switch (config) # aaa authentication attempts class-override admin no-lockout	
Related Commands	N/A	
Note		

aaa authentication attempts reset

aaa authentication attempts reset {all | user <username>} [{no-clear-history | no-unlock}]

Clears the authentication history for and/or unlocks specified users.

Syntax Description	all	Applies function to all users.
	user	Applies function to specified user.
	no-clear-history	Leaves the history of login failures but unlocks the account.
	no-unlock	Leaves the account locked but clears the history of login failures.
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	switch (config) # aaa authentication attempts reset user admin all	
Related Commands	N/A	
Note		

clear aaa authentication attempts

clear aaa authentication attempts {all | user <username>} [no-clear-history | no-unlock]

Clears the authentication history for and/or unlocks specified users

Syntax Description	all	Applies function to all users.
	user	Applies function to specified user.
	no-clear-history	Clears the history of login failures.
	no-unlock	Unlocks the account.
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	switch (config) # aaa authentication attempts reset user admin no-clear-history	
Related Commands	N/A	
Note		

aaa authorization

aaa authorization map [default-user <username> | order <policy>]
no aaa authorization map [default-user | order]

Sets the mapping permissions of a user in case a remote authentication is done.
 The no form of the command resets the attributes to default.

Syntax Description	username	Specifies what local account the authenticated user will be logged on as when a user is authenticated (via RADIUS or TACACS+) and does not have a local account. If the username is local, this mapping is ignored.
	policy	Sets the user mapping behavior when authenticating users via RADIUS or TACACS+ to one of three choices. The order determines how the remote user mapping behaves. If the authenticated username is valid locally, no mapping is performed. The setting has the following three possible behaviors: - remote-first - If a local-user mapping attribute is returned and it is a valid local username, it maps the authenticated user to the local user specified in the attribute. Otherwise, it uses the user specified by the default-user command. - remote-only - Maps a remote authenticated user if the authentication server sends a local-user mapping attribute. If the attribute does not specify a valid local user, no further mapping is tried. - local-only - Maps all remote users to the user specified by the “aaa authorization map default-user <user name>” command. Any vendor attributes received by an authentication server are ignored.
Default	Default user - admin. Map order - remote-first.	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	

Related Commands	show aaa username
-------------------------	----------------------

Note	If, for example, the user is locally defined to have admin permission, but in a remote server such as RADIUS the user is authenticated as monitor and the order is remote-first, then the user will be given monitor permissions.
-------------	---

show aaa

show aaa

Displays the AAA configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>switch (config) # show aaa AAA authorization: Default User: admin Map Order: remote-first Authentication method(s): local Accounting method(s): tacacs+ switch (config) #</pre>
Related Commands	<pre>aaa accounting aaa authentication aaa authorization show aaa show usernames username</pre>
Note	

show aaa authentication attempts

show aaa authentication attempts [configured | status user <username>]]

Shows the current authentication, authorization and accounting settings.

Syntax Description	authentication attempts	Displays configuration and history of authentication failures.
	configured	Displays configuration of authentication failure tracking.
	status user	Displays status of authentication failure tracking and lockouts for specific user.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.2.1000	
Role	admin	
Example	<pre> 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) # </pre>	
Related Commands	N/A	
Note		

4.9.3.3 RADIUS

radius-server

radius-server {key <secret>| retransmit <retries> | timeout <seconds>}
no radius-server {key | retransmit | timeout}

Sets global RADIUS server attributes.

The no form of the command resets the attributes to their default values.

Syntax Description	secret	Sets a secret key (shared hidden text string), known to the system and to the RADIUS server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry (1-60).
Default	3 seconds, 1 retry	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) #radius-server retransmit 3 switch (config) # show radius RADIUS defaults: Key: 3333 Timeout: 3 Retransmit: 1 No RADIUS servers configured. switch (config) #</pre>	
Related Commands	<pre>aaa authorization radius-server host show radius</pre>	
Note	Each RADIUS server can override those global parameters using the command “radius-server host”.	

radius-server host

radius-server host <IP address> {enable | auth-port <port> | key <secret> |
retransmit <retries> | timeout <seconds>}
no radius-server host <IP address> {enable | auth-port }

Configures RADIUS server attributes.

The no form of the command resets the attributes to their default values and deletes the RADIUS server.

Syntax Description	IP address	RADIUS server IP address.
	enable	Administrative enable of the RADIUS server.
	port	RADIUS server UDP port number.
	secret	Sets a secret key (shared hidden text string), known to the system and to the RADIUS server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry (1-60).
Default	3 seconds, 1 retry Default UDP port is 1812	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	<pre>aaa authorization radius-server show radius</pre>	
Note	• RADIUS servers are tried in the order they are configured • If you do not specify a parameter for this configured RADIUS server, the configuration will be taken from the global RADIUS server configuration. Refer to “radius-server” command.	

show radius

show radius

Displays RADIUS configurations.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	<pre>aaa authorization radius-server radius-server host</pre>
Note	

4.9.3.4 TACACS+

tacacs-server

tacacs-server {key <secret>| retransmit <retries> | timeout <seconds>}
no tacacs-server {key | retransmit | timeout}

Sets global TACACS+ server attributes.

The no form of the command resets the attributes to default values.

Syntax Description	secret	Set a secret key (shared hidden text string), known to the system and to the TACACS+ server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry (1-60).
Default	3 seconds, 1 retry	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) #tacacs-server retransmit 3 switch (config) # show tacacs TACACS+ defaults: Key: 3333 Timeout: 3 Retransmit: 1 No TACACS+ servers configured. switch (config) #</pre>	
Related Commands	<pre>aaa authorization show radius show tacacs tacacs-server host</pre>	
Note	Each TACACS+ server can override those global parameters using the command "tacacs-server host".	

tacacs-server host

tacacs-server host <IP address> {enable | auth-port <port> | auth-type <type> | key <secret> | retransmit <retries> | timeout <seconds>}
no tacacs-server host <IP address> {enable | auth-port}

Configures TACACS+ server attributes.

The no form of the command resets the attributes to their default values and deletes the TACACS+ server.

Syntax Description	IP address	TACACS+ server IP address.
	enable	Administrative enable for the TACACS+ server.
	port	TACACS+ server UDP port number.
	type	Authentication type. Possible values are: • ASCII • PAP (Password Authentication Protocol)
	secret	Sets a secret key (shared hidden text string), known to the system and to the TACACS+ server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry (1-60).
Default	3 seconds, 1 retry Default TCP port is 49 Default auth-type is PAP	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	

Related Commands

aaa authorization
show tacacs
tacacs-server

Note

- TACACS+ servers are tried in the order they are configured
 - A PAP auth-type similar to an ASCII login, except that the username and password arrive at the network access server in a PAP protocol packet instead of being typed in by the user, so the user is not prompted
 - If the user does not specify a parameter for this configured TACACS+ server, the configuration will be taken from the global TACACS+ server configuration. Refer to “tacacs-server” command.
-
-

show tacacs

show tacacs

Displays TACACS+ configurations.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	<pre>aaa authorization tacacs-server tacacs-server host</pre>
Note	

4.9.3.5 LDAP

ldap base-dn

ldap base-dn <string>
no ldap base-dn

Sets the base distinguished name (location) of the user information in the schema of the LDAP server.

The no form of the command resets the attribute to its default values.

Syntax Description	string	A case-sensitive string that specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request. For example: "ou=users,dc=example,dc=com", with no spaces. when: ou - Organizational unit dc - Domain component cn - Common name sn - Surname
Default	ou=users,dc=example,dc=com	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	
Example	<pre> 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) # </pre>	

Related Commands

show ldap

Note

ldap bind-dn/bind-password

ldap {bind-dn | bind-password} <string>

no ldap {bind-dn | bind-password}

Gives the distinguished name or password to bind to on the LDAP server. This can be left empty for anonymous login (the default).

The no form of the command resets the attribute to its default values.

Syntax Description	string	A case-sensitive string that specifies distinguished name or password to bind to on the LDAP server.
Default	""	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	
Example	<pre> 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) # </pre>	
Related Commands	show ldap	
Note	For anonymous login, bind-dn and bind-password should be empty strings "".	

ldap group-attribute/group-dn

ldap {group-attribute {<group-att> | member | uniqueMember} | group-dn <group-dn>}

no ldap {group-attribute | group-dn}

Sets the distinguished name or attribute name of a group on the LDAP server.
The no form of the command resets the attribute to its default values.

Syntax Description	group-att	Specifies a custom attribute name.
	member	groupOfNames or group membership attribute.
	uniqueMember	groupOfUniqueNames membership attribute.
	group-dn	DN of group required for authorization.
Default	group-att: member group-dn: ""	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	
Example	<pre> 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) # </pre>	

Related Commands

show ldap

Note

- The user's distinguished name must be listed as one of the values of this attribute, or the user will not be authorized to log in
 - After login authentication, if the group-dn is set, a user must be a member of this group or the user will not be authorized to log in. If the group is not set ("") - the default) no authorization checks are done.
-
-

ldap host

ldap host <IP Address> [order <number> last]

no ldap host <IP Address>

Adds an LDAP server to the set of servers used for authentication.

The no form of the command deletes the LDAP host.

Syntax Description	IP Address	IPv4 or IPv6 address.
	number	The order of the LDAP server.
	last	The LDAP server will be added in the last location.
Default	No hosts configured	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	<pre>show aaa show ldap</pre>	
Note	- The system will select the LDAP host to try according to its order - New servers are by default added at the end of the list of servers	

ldap login-attribute

ldap login-attribute {<string> | uid | sAMAccountName}

no ldap login-attribute

Sets the attribute name which contains the login name of the user.
The no form of the command resets this attribute to its default.

Syntax Description	string	Custom attribute name.
	uid	LDAP login name is taken from the user login user-name.
	sAMAccountName	SAM Account name, active directory login name.
Default	sAMAccountName	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	
Example	<pre> 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) # </pre>	
Related Commands	<pre> show aaa show ldap </pre>	
Note		

ldap port

ldap port <port>

no ldap port

Sets the TCP port on the LDAP server to connect to for authentication.
The no form of the command resets this attribute to its default value.

Syntax Description	port	TCP port number.
Default	389	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	
Example	<pre> 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) # </pre>	
Related Commands	<pre> show aaa show ldap </pre>	
Note		

ldap referrals

ldap referrals no ldap referrals

Enables LDAP referrals.

The no form of the command disables LDAP referrals.

Syntax Description	N/A
Default	LDAP referrals are enabled
Configuration Mode	Config
History	3.1.0000 3.3.5050 Updated Example
Role	admin
Example	<pre> 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) # </pre>
Related Commands	<pre> show aaa show ldap </pre>
Note	Referral is the process by which an LDAP server, instead of returning a result, will return a referral (a reference) to another LDAP server which may contain further information.

ldap scope

ldap scope <scope>

no ldap scope

Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

The no form of the command resets the attribute to its default value.

Syntax Description	scope	- one-level - searches the immediate children of the base dn - subtree - searches at the base DN and all its children
Default	subtree	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	
Example	<pre> 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) # </pre>	
Related Commands	show aaa show ldap	
Note		

ldap ssl

ldap ssl {ca-list <options> | cert-verify | ciphers {all | TLS1.2} | mode <mode> | port <port-number>}
no ldap ssl {cert-verify | ciphers | mode | port}

Sets SSL parameter for LDAP.

The no form of the command resets the attribute to its default value.

Syntax Description	options	This command specifies the list of supplemental certificates of authority (CAs) from the certificate configuration database that is to be used by LDAP for authentication of servers when in TLS or SSL mode. The options are: • default-ca-list - uses default supplemental CA certificate list • none - no supplemental list, uses the built-in one only CA certificates are ignored if “ldap ssl mode” is not configured as either “tls” or “ssl”, or if “no ldap ssl cert-verify” is configured. The default-ca-list is empty in the factory default configuration. Use the command: “crypto certificate ca-list default-ca-list name” to add trusted certificates to that list. The “default-ca-list” option requires LDAP to consult the system’s configured global default CA-list for supplemental certificates.
	cert-verify	Enables verification of SSL/TLS server certificates. This may be required if the server's certificate is self-signed, or does not match the name of the server.
	ciphers {all TLS1.2}	Sets SSL mode to be used.
	mode	Sets the security mode for connections to the LDAP server. • none – requests no encryption for the LDAP connection • ssl – the SSL-port configuration is used, an SSL connection is made before LDAP requests are sent (LDAP over SSL) • start-tls – the normal LDAP port is used, an LDAP connection is initiated, and then TLS is started on this existing connection
	port-number	Sets the port on the LDAP server to connect to for authentication when the SSL security mode is enabled (LDAP over SSL).
Default	cert-verify: enabled mode: none (LDAP SSL is not activated) port-number: 636 ciphers: all	

Configuration Mode	Config	
History	3.1.0000	Initial version
	3.2.3000	Added ca-list argument.
	3.3.5050	Added “ssl ciphers” parameter Updated Example
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	<pre>show aaa show ldap</pre>	
Note	• If available, the TLS mode is recommended, as it is standardized, and may also be of higher security • The port number is used only for SSL mode. In case the mode is TLS, the LDAP port number will be used.	

Ldap timeout

ldap {timeout-bind | timeout-search} <seconds>

no ldap {timeout-bind | timeout-search}

Sets a global communication timeout in seconds for all LDAP servers to specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

The no form of the command resets the attribute to its default value.

Syntax Description	timeout-bind	Sets the global LDAP bind timeout for all LDAP servers.
	timeout-search	Sets the global LDAP search timeout for all LDAP servers.
	seconds	Range: 1-60 seconds.
Default	5 seconds	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	
Example	<pre> 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) # </pre>	
Related Commands	<pre> show aaa show ldap </pre>	
Note		

ldap version

ldap version <version>

no ldap version

Sets the LDAP version.

The no form of the command resets the attribute to its default value.

Syntax Description	version	Sets the LDAP version. Values: 2 and 3.
Default	3	
Configuration Mode	Config	
History	3.1.0000	
	3.3.5050	Updated Example
Role	admin	
Example	<pre> 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) # </pre>	
Related Commands	show aaa show ldap	
Note		

show ldap

show ldap

Displays LDAP configurations.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
	3.3.5050 Updated Example
Role	admin
Example	<pre> 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) # </pre>
Related Commands	<pre> show aaa show ldap </pre>
Note	

4.10 Cryptographic (X.509, IPSec)

This chapter contains commands for configuring, generating and modifying x.509 certificates used in the system. Certificates are used for creating a trusted SSL connection to the system.

Crypto commands also cover IPSec configuration commands used for establishing a secure connection between hosts over IP layer which is useful for transferring sensitive information.

4.10.1 Commands

crypto ipsec peer local

```
crypto ipsec peer <IPv4 or IPv6 address> local <IPv4 or IPv6 address> {enable |  
keying {ike [auth {hmac-md5 | hmac-sha1 | hmac-sha256 | null} | dh-group | dis-  
able | 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	<pre>switch (config)# crypto ipsec peer 10.10.10.10 local 10.7.34.139 enable switch (config)#</pre>	

Related Commands

N/A

Note

crypto certificate ca-list

crypto certificate ca-list [default-ca-list name {<cert-name> | system-self-signed}]

no crypto certificate ca-list [default-ca-list name {<cert-name> | system-self-signed}]

Adds the specified CA certificate to the default CA certificate list.
The no form of the command removes the certificate from the default CA certificate list.

Syntax Description	cert-name	The name of the certificate.
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	switch (config) # crypto certificate default-cert name test	
Related Commands	N/A	
Note	- Two certificates with the same subject and issuer fields cannot both be placed onto the CA list - The no form of the command does not delete the certificate from the certificate database - Unless specified otherwise, applications that use CA certificates will still consult the well-known certificate bundle before looking at the default-ca-list	

crypto certificate default-cert

crypto certificate default-cert name {<cert-name> | system-self-signed}
no crypto certificate default-cert name {<cert-name> | system-self-signed}

Designates the named certificate as the global default certificate role for authentication of this system to clients.

The no form of the command reverts the default-cert name to “system-self-signed” (the “cert-name” value is optional and ignored).

Syntax Description	cert-name	The name of the certificate.
Default	N/A	
Configuration Mode	Config	
History	3.2.3000	
Role	admin	
Example	switch (config) # crypto certificate default-cert name test	
Related Commands	N/A	
Note	• A certificate must already be defined before it can be configured in the default-cert role • If the named default-cert is deleted from the database, the default-cert automatically becomes reconfigured to the factory default, the “system-self-signed” certificate	

crypto certificate generation

crypto certificate generation default {country-code | days-valid | email-addr | hash-algorithm {sha1 | sha256} | key-size-bits | locality | org-unit | organization | state-or-prov}

Configures default values for certificate generation.

Syntax Description	country-code	Configures the default certificate value for country code with a two-alphanumeric-character code or -- for none.
	days-valid	Configures the default certificate value for days valid.
	email-addr	Configures the default certificate value for email address.
	hash-algorithm {sha1 sha256}	Configures the default certificate hashing algorithm.
	key-size-bits	Configures the default certificate value for private key size. (Private key length in bits – at least 1024, but 2048 is strongly recommended.)
	locality	Configures the default certificate value for locality.
	org-unit	Configures the default certificate value for organizational unit.
	organization	Configures the default certificate value for the organization name.
	state-or-prov	Configures the default certificate value for state or province.
Default	N/A	
Configuration Mode	Config	
History	3.2.1000	First version
	3.3.4350	Added “hash-algorithm” parameter
Role	admin	
Example	switch (config) # crypto certificate generation default hash-algorithm sha256	
Related Commands	N/A	
Note	The default hashing algorithm used is sha1.	

crypto certificate name

```
crypto certificate name {<cert-name> | system-self-signed} {comment <new
comment> | generate self-signed [comment <cert-comment> | common-name
<domain> | country-code <code> | days-valid <days> | email-addr <address> |
hash-algorithm {sha1 | sha256} | key-size-bits <bits> | locality <name> | org-unit
<name> | organization <name> | serial-num <number> | state-or-prov <name>]}
| private-key pem <PEM string> | prompt-private-key | public-cert [comment
<comment string> | pem <PEM string>] | regenerate days-valid <days> | rename
<new name>}
no crypto certificate name <cert-name>
```

Configures default values for certificate generation.

The no form of the command clears/deletes certain certificate settings.

Syntax Description		
	cert-name	Unique name by which the certificate is identified.
	comment	Specifies a certificate comment.
	generate self-signed	Generates certificates. This option has the following parameters which may be entered sequentially in any order: - comment: Specifies a certificate comment (free string) - common-name: Specifies the common name of the issuer and subject (e.g. a domain name) - country-code: Specifies the country codtwo-alphanumeric-character country code, or "--" for none) - days-valid: Specifies the number of days the certificate is valid - email-addr: Specifies the email address - hash-algorithm: Specifies the hashing function used for signature algorithm - key-size-bits: Specifies the size of the private key in bits (private key length in bits - at least 1024 but 2048 is strongly recommended) - locality: Specifies the locality name - org-unit: Specifies the organizational unit name - organization: Specifies the organization name - serial-num: Specifies the serial number for the certificate (a lower-case hexadecimal serial number prefixed with "0x") - state-or-prov: Specifies the state or province name
	private-key pem	Specifies certificate contents in PEM format.
	prompt-private-key	Prompts for certificate private key with secure echo.
	public-cert	Installs a certificate.
	regenerate	Regenerates the named certificate using configured certificate generation default values for the specified validity period
	rename	Renames the certificate.
Default	N/A	

Configuration Mode	Config	
History	3.2.3000	First version
	3.3.4402	Added “hash-algorithm” parameter
Role	admin	
Example	switch (config) # crypto certificate name system-self-signed generate self-signed hash-algorithm sha256	
Related Commands	N/A	
Note		

crypto certificate system-self-signed

crypto certificate system-self-signed regenerate [days-valid <days>]

Configures default values for certificate generation.

Syntax Description	days-valid	Specifies the number of days the certificate is valid
Default	N/A	
Configuration Mode	Config	
History	3.2.1000	
Role	admin	
Example	switch (config) # crypto certificate system-self-signed regenerate days-valid 3	
Related Commands	N/A	
Note		

show crypto certificate

show crypto certificate [detail | public-pem | default-cert [detail | public-pem] |
[name <cert-name> [detail | public-pem] | ca-list [default-ca-list]]

Displays information about all certificates in the certificate database.

Syntax Description	ca-list	Displays the list of supplemental certificates configured for the global default system CA certificate role.
	default-ca-list	Displays information about the currently configured default certificates of the CA list.
	default-cert	Displays information about the currently configured default certificate.
	detail	Displays all attributes related to the certificate.
	name	Displays information about the certificate specified.
	public-pem	Displays the uninterpreted public certificate as a PEM formatted data string
Default	N/A	
Configuration Mode	Config	
History	3.2.1000	
Role	admin	

Example

```
switch (config)# show crypto certificate
Certificate with name 'system-self-signed' (default-cert)
  Comment:                               system-generated self-signed certifi-
icate
  Private Key:                           present
  Serial Number:                         0x546c935511bcafc21ac0e8249fbe0844
  SHA-1 Fingerprint:
fe6df38dd26801971cb2d44f62dbe492b6063c5f

  Validity:
    Starts:                               2012/12/02 13:45:05
    Expires:                              2013/12/02 13:45:05

  Subject:
    Common Name:                         IBM-DEV-Bay4
    Country:                             IS
    State or Province:
    Locality:
    Organization:
    Organizational Unit:
    E-mail Address:

  Issuer:
    Common Name:                         IBM-DEV-Bay4
    Country:                             IS
    State or Province:
    Locality:
    Organization:
    Organizational Unit:
    E-mail Address:

switch (config)#
```

Related Commands

N/A

Note

show crypto ipsec

show crypto ipsec [brief | configured | ike | policy | sa]

Displays information ipsec configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.2.1000
Role	admin
Example	<pre>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)#</pre>
Related Commands	N/A
Note	

4.11 Scheduled Jobs

Use the commands in this section to manage and schedule the execution of jobs

4.11.1 Commands

job

job <job ID>
no job <job ID>

Creates a job.
The no form of the command deletes the job.

Syntax Description	job ID	An integer.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	switch (config) # job 100 switch (config job 100) #	
Related Commands	show jobs	
Note	Job state is lost on reboot.	

command

command <sequence #> | <command>

no command <sequence #>

Adds a CLI command to the job.

The no form of the command deletes the command from the job.

Syntax Description	sequence #	An integer that controls the order the command is executed relative to other commands in this job. The commands are executed in an ascending order.
	command	A CLI command.
Default	N/A	
Configuration Mode	Config job	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config)# job 100 switch (config job 100) # command 10 "show power" switch (config job 100) #</pre>	
Related Commands	show jobs	
Note	- The command must be defined with inverted commas (“”) - The command must be added as it was executed from the “config” mode. For example, in order to change the interface description you need to add the command: “interface <type> <number> description my-description”.	

comment

comment <comment>

no comment

Adds a comment to the job.

The no form of the command deletes the comment.

Syntax Description	comment	The comment to be added (string).
Default	""	
Configuration Mode	Config job	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config)# job 100 switch (config job 100) # comment Job_for_example switch (config job 100) #</pre>	
Related Commands	show jobs	
Note		

enable

enable
no enable

Enables the specified job.
The no form of the command disables the specified job.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config job
History	3.1.0000
Role	admin
Example	<pre>switch (config)# job 100 switch (config job 100) # enable switch (config job 100) #</pre>
Related Commands	show jobs
Note	If a job is disabled, it will not be executed automatically according to its schedule; nor can it be executed manually.

execute

execute

Forces an immediate execution of the job.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config job
History	3.1.0000
Role	admin
Example	<pre>switch (config)# job 100 switch (config job 100) # execute switch (config job 100) #</pre>
Related Commands	show jobs
Note	- The job timer (if set) is not canceled and the job state is not changed: i.e. the time of the next automatic execution is not affected - The job will not be run if not currently enabled

fail-continue

fail-continue
no fail-continue

Continues the job execution regardless of any job failures.
 The no form of the command returns fail-continue to its default.

Syntax Description	N/A
Default	A job will halt execution as soon as any of its commands fails
Configuration Mode	Config job
History	3.1.0000
Role	admin
Example	switch (config)# job 100 switch (config job 100) # fail-continue switch (config job 100) #
Related Commands	show jobs
Note	

name

name <job name>

no name

Configures a name for this job.

The no form of the command resets the name to its default.

Syntax Description	name	Specifies a name for the job (string).
Default	“”.	
Configuration Mode	Config job	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config)# job 100 switch (config job 100) # name my-job switch (config job 100) #</pre>	
Related Commands	show jobs	
Note		

schedule type

schedule type <recurrence type>

no schedule type

Sets the type of schedule the job will automatically execute on.
The no form of the command resets the schedule type to its default.

Syntax Description	recurrence type	The available schedule types are: • daily - the job is executed every day at a specified time • weekly - the job is executed on a weekly basis • monthly - the job is executed every month on a specified day of the month • once - the job is executed once at a single specified date and time • periodic - the job is executed on a specified fixed time interval, starting from a fixed point in time.
Default	once	
Configuration Mode	Config job	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config)# job 100 switch (config job 100) # schedule type once switch (config job 100) #</pre>	
Related Commands	show jobs	
Note	A schedule type is essentially a structure for specifying one or more future dates and times for a job to execute.	

schedule <recurrence type>

schedule <recurrence type> <interval and date>

no schedule

Sets the type of schedule the job will automatically execute on.
The no form of the command resets the schedule type to its default.

Syntax Description	recurrence type	The available schedule types are: • daily - the job is executed every day at a specified time • weekly - the job is executed on a weekly basis • monthly - the job is executed every month on a specified day of the month • once - the job is executed once at a single specified date and time • periodic - the job is executed on a specified fixed time interval, starting from a fixed point in time.
	interval and date	Interval and date, per recurrence type.
Default	once	
Configuration Mode	Config job	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config)# job 100 switch (config job 100) # schedule monthly interval 10 switch (config job 100) #</pre>	
Related Commands	show jobs	
Note	A schedule type is essentially a structure for specifying one or more future dates and times for a job to execute.	

show jobs

show jobs [<job-id>]

Displays configuration and state (including results of last execution, if any exist) of all jobs, or of one job if a job ID is specified.

Syntax Description	job-id	Job ID.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show jobs	
Note		

4.12 Statistics and Alarms

4.12.1 Commands

stats alarm <alarm-id> clear

stats alarm <alarm ID> clear

Clears alarm state.

Syntax Description	alarm ID	Alarms supported by the system, for example: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # stats alarm cpu_util_indiv clear switch (config) #</pre>	
Related Commands	show stats alarm	
Note		

stats alarm <alarm-id> enable

stats alarm <alarm-id> enable
no stats alarm <alarm-id> enable

Enables the alarm.

The no form of the command disables the alarm, notifications will not be received.

Syntax Description	alarm ID	Alarms supported by the system, for example: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
Default	The default is different per alarm-id	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # stats alarm cpu_util_indiv enable switch (config) #</pre>	
Related Commands	show stats alarm	
Note		

stats alarm <alarm-id> event-repeat

stats alarm <alarm ID> event-repeat {single | while-not-cleared}

no stats alarm <alarm ID> event-repeat

Configures repetition of events from this alarm.

Syntax Description	alarm ID	Alarms supported by the system, for example: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
	single	Does not repeat events: only sends one event whenever the alarm changes state.
	while-not-cleared	Repeats error events until the alarm clears.
Default	single	
Configuration Mode	Config	
History	3.1.0000	
Role	monitor/admin	
Example	<pre>switch (config) # stats alarm cpu_util_indiv event-repeat single switch (config) #</pre>	
Related Commands	show stats alarm	
Note		

stats alarm <alarm-id> {rising | falling}

stats alarm <alarm ID> {rising | falling} {clear-threshold | error-threshold} <threshold-value>

Configure alarms thresholds.

Syntax Description	alarm ID	Alarms supported by the system, for example: - cpu_util_indiv - Average CPU utilization too high: percent utilization - disk_io - Operating System Disk I/O per second too high: kilobytes per second - fs_mnt - Free filesystem space too low: percent of disk space free - intf_util - Network utilization too high: bytes per second - memory_pct_used - Too much memory in use: percent of physical memory used - paging - Paging activity too high: page faults - temperature - Temperature is too high: degrees
	falling	Configures alarm for when the statistic falls too low.
	rising	Configures alarm for when the statistic rises too high.
	error-threshold	Sets threshold to trigger falling or rising alarm.
	clear-threshold	Sets threshold to clear falling or rising alarm.
	threshold-value	The desired threshold value, different per alarm.
Default	Default is different per alarm-id	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # stats alarm cpu_util_indiv falling clear-threshold 10 switch (config) #</pre>	
Related Commands	show stats alarm	
Note	Not all alarms support all four thresholds.	

stats alarm <alarm-id> rate-limit

stats alarm <alarm ID> rate-limit {count <count-type> <count> | reset | window <window-type> <duration>}

Configures alarms rate limit.

Syntax Description	alarm ID	Alarms supported by the system, for example: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
	count-type	Long medium, or short count (number of alarms).
	reset	Set the count and window durations to default values for this alarm.
	window-type	Long medium, or short count, in seconds.
Default	Short window: 5 alarms in 1 hour Medium window: 20 alarms in 1 day Long window: 50 alarms in 7 days	
Configuration Mode	Config	
History	3.1.0000	
Role	monitor/admin	
Example	switch (config) # stats alarm paging rate-limit window long 2000 switch (config) #	
Related Commands	show stats alarm	
Note		

stats chd <chd-id> clear

stats chd <CHD ID> clear

Clears CHD counters.

Syntax Description	CHD ID	CHD supported by the system, for example: • cpu_util - CPU utilization: percentage of time spent • cpu_util_ave - CPU utilization average: percentage of time spent • cpu_util_day - CPU utilization average: percentage of time spent • disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes • disk_io - Operating system aggregate disk I/O average: KB/sec • eth_day • eth_hour • fs_mnt_day - Filesystem system usage average: bytes • fs_mnt_month - Filesystem system usage average: bytes • fs_mnt_week - Filesystem system usage average: bytes • ib_day • ib_hour • intf_day - Network interface statistics aggregation: bytes • intf_hour - Network interface statistics (same as “interface” sample) • intf_util - Aggregate network utilization across all interfaces • memory_day - Average physical memory usage: bytes • memory_pct - Average physical memory usage • paging - Paging activity: page faults • paging_day - Paging activity: page faults
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # stats chd memory_day clear switch (config) #</pre>	
Related Commands	show stats chd	
Note		

stats chd <chd-id> enable

stats chd <chd-id> enable
no stats chd <chd-id> enable

Enables the CHD.
 The no form of the command disables the CHD.

Syntax Description	chd-id	CHD supported by the system, for example: • cpu_util - CPU utilization: percentage of time spent • cpu_util_ave - CPU utilization average: percentage of time spent • cpu_util_day - CPU utilization average: percentage of time spent • disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes • disk_io - Operating system aggregate disk I/O average: KB/sec • eth_day • eth_hour • fs_mnt_day - Filesystem system usage average: bytes • fs_mnt_month - Filesystem system usage average: bytes • fs_mnt_week - Filesystem system usage average: bytes • ib_day • ib_hour • intf_day - Network interface statistics aggregation: bytes • intf_hour - Network interface statistics (same as “interface” sample) • intf_util - Aggregate network utilization across all interfaces • memory_day - Average physical memory usage: bytes • memory_pct - Average physical memory usage • paging - Paging activity: page faults • paging_day - Paging activity: page faults
Default	Enabled	
Configuration Mode	Config	
History	3.1.0000	
Role	monitor/admin	
Example	<pre>switch (config) # stats chd memory_day enable switch (config) #</pre>	
Related Commands	show stats chd	
Note		

stats chd <chd-id> compute time

stats chd <CHD ID> compute time {interval | range} <number of seconds>

Sets parameters for when this CHD is computed.

Syntax Description	CHD ID	Possible IDs:
		• cpu_util - CPU utilization: percentage of time spent • cpu_util_ave - CPU utilization average: percentage of time spent • cpu_util_day - CPU utilization average: percentage of time spent • disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes • disk_io - Operating system aggregate disk I/O average: KB/sec • eth_day • eth_hour • fs_mnt_day - Filesystem system usage average: bytes • fs_mnt_month - Filesystem system usage average: bytes • fs_mnt_week - Filesystem system usage average: bytes • ib_day • ib_hour • intf_day - Network interface statistics aggregation: bytes • intf_hour - Network interface statistics (same as “interface” sample) • intf_util - Aggregate network utilization across all interfaces • memory_day - Average physical memory usage: bytes • memory_pct - Average physical memory usage • paging - Paging activity: page faults • paging_day - Paging activity: page faults
	interval	Specifies calculation interval (how often to do a new calculation) in number of seconds.
	range	Specifies calculation range, in number of seconds.
	number of seconds	Number of seconds.
Default	Different per CHD	
Configuration Mode	Config	
History	3.1.0000	
Role	monitor/admin	
Example	<pre>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) #</pre>	

Related Commands	show stats chd
-------------------------	----------------

Note

stats sample <sample-id> clear

stats sample <sample ID> clear

Clears sample history.

Syntax Description	sample ID	Possible sample IDs are: • congested • cpu_util - CPU utilization: milliseconds of time spent • disk_device_io - Storage device I/O statistics • disk_io - Operating system aggregate disk I/O: KB/sec • eth • fan - Fan speed • fs_mnt_bytes - Filesystem usage: bytes • fs_mnt_inodes - Filesystem usage: inodes • ib • interface - Network interface statistics • intf_util - Network interface utilization: bytes • memory - System memory utilization: bytes • paging - Paging activity: page faults • power - Power supply usage • power-consumption • temperature - Modules temperature
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # stats sample temperature clear switch (config) #</pre>	
Related Commands	show stats sample	
Note		

stats sample <sample-id> enable

stats sample <sample-id> enable
no stats 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	<pre>switch (config) # stats sample temperature enable switch (config) #</pre>	
Related Commands	show stats sample	
Note		

stats sample <sample-id> interval

stats sample <sample ID> interval <number of seconds>

Sets the amount of time between samples for the specified group of sample data.

Syntax Description	sample ID	Possible sample IDs are: • congested • cpu_util - CPU utilization: milliseconds of time spent • disk_device_io - Storage device I/O statistics • disk_io - Operating system aggregate disk I/O: KB/sec • eth • fan - Fan speed • fs_mnt_bytes - Filesystem usage: bytes • fs_mnt_inodes - Filesystem usage: inodes • ib • interface - Network interface statistics • intf_util - Network interface utilization: bytes • memory - System memory utilization: bytes • paging - Paging activity: page faults • power - Power supply usage • power-consumption • temperature - Modules temperature
	number of seconds	Interval in seconds.
Default	Different per sample	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show stats sample	
Note		

stats clear-all

stats clear all

Clears data for all samples, CHDs, and status for all alarms.

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

stats export

stats export <format> <report name> [{after | before} <yyyy/mm/dd>
<hh:mm:ss>] [filename <filename>]

Exports statistics to a file.

Syntax Description	format	Currently the only supported value for <format> is “csv” (comma-separated value).
	report name	Determines dataset to be exported. Possible report names are: - memory - Memory utilization - paging - Paging I/O - cpu_util - CPU utilization
	after before	Only includes stats collected after or before a specific time.
	yyyy/mm/dd	Date: It must be between 1970/01/01 and 2038/01/19.
	hh:mm:ss	Time: It must be between 00:00:00 and 03:14:07 UTC and is treated as local time.
	filename	Specifies filename to give new report. If a filename is specified, the stats will be exported to a file of that name; otherwise a name will be chosen automatically and will contain the name of the report and the time and date of the export. Any automatically-chosen name will be given a .csv extension.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show files stats	
Note		

show stats alarm

show stats alarm [<Alarm ID> [rate-limit]]

Displays status of all alarms or the specified alarm.

Syntax Description	Alarm ID	May be: • <code>cpu_util_indiv</code> - Average CPU utilization too high: percent utilization • <code>disk_io</code> - Operating System Disk I/O per second too high: kilobytes per second • <code>fs_mnt</code> - Free filesystem space too low: percent of disk space free • <code>intf_util</code> - Network utilization too high: bytes per second • <code>memory_pct_used</code> - Too much memory in use: percent of physical memory used • <code>paging</code> - Paging activity too high: page faults • <code>temperature</code> - Temperature is too high: degrees
	rate-limit	Displays rate limit parameters.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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): (dis- abled) 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) #</pre>	
Related Commands	stats alarm	
Note		

show stats chd

show stats chd [<CHD ID>]

Displays configuration of all statistics CHDs.

Syntax Description	CHD ID	May be: • <code>cpu_util_indiv</code> - Average CPU utilization too high: percent utilization • <code>disk_io</code> - Operating System Disk I/O per second too high: kilobytes per second • <code>fs_mnt</code> - Free filesystem space too low: percent of disk space free • <code>intf_util</code> - Network utilization too high: bytes per second • <code>memory_pct_used</code> - Too much memory in use: percent of physical memory used • <code>paging</code> - Paging activity too high: page faults • <code>temperature</code> - Temperature is too high: degrees
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	stats chd	
Note		

show stats cpu

show stats cpu

Displays some basic stats about CPU utilization:

- the current level
- the peak over the past hour
- the average over the past hour

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	N/A
Note	

show stats sample

show stats sample [<sample ID>]

Displays sampling interval for all samples, or the specified one.

Syntax Description	sample ID	Possible sample IDs are: • congested • cpu_util - CPU utilization: milliseconds of time spent • disk_device_io - Storage device I/O statistics • disk_io - Operating system aggregate disk I/O: KB/sec • eth • fan - Fan speed • fs_mnt_bytes - Filesystem usage: bytes • fs_mnt_inodes - Filesystem usage: inodes • ib • interface - Network interface statistics • intf_util - Network interface utilization: bytes • memory - System memory utilization: bytes • paging - Paging activity: page faults • power - Power supply usage • power-consumption • temperature - Modules temperature
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # show stats sample fan Sample "fan" (Fan speed): Enabled: yes Sampling interval: 1 minute 11 seconds switch (config) #</pre>	
Related Commands	N/A	
Note		

4.12.2 Power Management

4.12.2.1 Width Reduction Power Saving

Link width reduction (LWR) is a Mellanox proprietary power saving feature to be utilized to economize the power usage of the fabric. LWR may be used to manually or automatically configure a certain connection between Mellanox switch systems to lower the width of a link from 4X operation to 1X based on the traffic flow.

LWR is relevant only for 40GbE and InfiniBand FDR speeds in which the links are operational at a 4X width.



When “show interfaces” is used, a port’s speed appears unchanged even when only one lane is active.

LWR has three operating modes per interface:

- Disabled – LWR does not operate and the link remains in 4X under all circumstances.
- Automatic – the link automatically alternates between 4X and 1X based on traffic flow.
- Force – a port is forced to operate in 1X mode lowering the throughput capability of the port. This mode should be chosen in cases where constant low throughput is expected on the port for a certain time period – after which the port should be configured to one of the other two modes, to allow higher throughput to pass through the port.



See command “[power-management width](#)” on page 318.

Table 22 - LWR Configuration Behavior

Switch-A Configuration	Switch-B Configuration	Behavior
Disable	Disable	LWR is disabled.
Disable	Force	Transmission from Switch-B to Switch-A operates at 1X. On the opposite direction, LWR is disabled.
Disable	Auto	Depending on traffic flow, transmission from Switch-B to Switch-A may operate at 1X. On the opposite direction, LWR is disabled.
Auto	Force	Transmission from Switch-B to Switch-A operates at 1 lane. Transmission from Switch-A to Switch-B may operate at 1X depending on the traffic.
Auto	Auto	Width of the connection depends on the traffic flow
Force	Force	Connection between the switches operates at 1X

4.12.3 System Reboot

4.12.3.1 Rebooting 1U Switches

➤ **To reboot a 1U switch system:**

Step 1. Enter Config mode. Run:

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

Step 2. Reboot the system. Run:

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

4.12.4 Commands

4.12.4.1 Chassis Management

clear counters

clear counters [all | interface <type> <number>]

Clears switch counters.

Syntax Description	all	Clears all switch counters.
	type	A specific interface type
	number	The interface number.
Default	N/A	
Configuration Mode	Config Interface Port Channel	
History	3.2.3000	
Role	admin	
Example	switch (config) # clear counters switch (config) #	
Related Commands		
Note		

health

health {max-report-len <length> | re-notif-cntr <counter> | report-clear}

Configures health daemon settings.

Syntax Description	max-report-len <length>	Sets the length of the health report - number of line entries. Possible values: 10-2048.
	re-notif-cntr <counter>	Health control changes notification counter, in seconds. Possible values: 120-7200 seconds.
	report-clear	Clears the health report.
Default	max-report-len: 50 re-notif-cntr:	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	switch (config) # health re-notif-cntr 125 switch (config) #	
Related Commands	show health-report	
Note		

power enable

power enable <module name>
no power enable <module name>

Powers on the module.
 The no form of the command shuts down the module.

Syntax Description	module name	Enables power for selected module.
Default	Power is enabled on all modules.	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # power enable L01 switch (config) #</pre>	
Related Commands	<pre>show power show power consumers</pre>	
Note	This command is not applicable for 1U systems.	

power-management width

power-management width {auto | force}

no power-management width

Sets the width of the interface to be automatically adjusted.

The no form of the command disables power-saving.

Syntax Description	auto	Allows the system to automatically decide whether to work in power-saving mode or not.
	force	Forces power-saving mode on the port.
Default	Disabled	
Configuration Mode	Config Interface Ethernet	
History	3.3.4000	
Role	admin	
Example	switch (config interface ib 1/1) # power-management width auto switch (config) #	
Related Commands	show interface	
Note		

usb eject

usb eject

Gracefully turns off the USB interface.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	switch (config) # usb eject switch (config) #
Related Commands	N/A
Note	Applicable only for systems with USB interface.

show fan

show fan

Displays fans status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	N/A
Note	

show version

show version [concise]

Displays version information for the currently running system image.

Syntax Description	concise	The concise variant fits the description onto one line.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	
Example	<pre> switch (config) # show version Product name: SX_PPC_M460EX Product release: 3.0.0000-dev-HA Build ID: #1-dev Build date: 2012-02-26 08:47:51 Target arch: ppc Target hw: m460ex Built by: root@r-fit16 Uptime: 1d 3h 32m 24.656s Product model: ppc Host ID: 0002c911a15e System memory: 110 MB used / 1917 MB free / 2027 MB total Swap: 0 MB used / 0 MB free / 0 MB total Number of CPUs: 1 CPU load averages: 0.18 / 0.19 / 0.16 switch (config) # </pre>	
Related Commands	N/A	
Note		

show uboot

show uboot

Displays u-boot version.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.5000
Role	admin
Example	switch (config) # show uboot UBOOT version : U-Boot 2009.01 SX_PPC_M460EX SX_3.2.0330-82 ppc (Dec 20 2012) switch (config) #
Related Commands	N/A
Note	

show cpld

show cpld

Displays status of all CPLDs in the system.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
	3.3.4302 Updated example
Role	admin
Example	<pre>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) #</pre>
Related Commands	N/A
Note	

show inventory

show inventory

Displays system inventory.

Syntax Description	N/A																														
Default	N/A																														
Configuration Mode	Any Command Mode																														
History	3.1.0000																														
Role	admin																														
Example	switch (config) # show inventory ===== <table><tr><th>Module</th><th>Type</th><th>Part number</th><th>Serial Number</th><th>Asic revision</th></tr><tr><td>CHASSIS</td><td>SX1036</td><td>MSX1036B-1SFR</td><td>MT1205X01549</td><td>N/A</td></tr><tr><td>MGMT</td><td>SX1036</td><td>MSX1036B-1SFR</td><td>MT1205X01549</td><td>0</td></tr><tr><td>FAN</td><td>SXX0XX_FAN</td><td>MSX60-FF</td><td>MT1206X07209</td><td>N/A</td></tr><tr><td>PS1</td><td>SXX0XX_PS</td><td>MSX60-PF</td><td>MT1206X06697</td><td>N/A</td></tr><tr><td>CPU</td><td>CPU</td><td>SA000203-B</td><td>MT1220X01231</td><td>N/A</td></tr></table> switch (config) #	Module	Type	Part number	Serial Number	Asic revision	CHASSIS	SX1036	MSX1036B-1SFR	MT1205X01549	N/A	MGMT	SX1036	MSX1036B-1SFR	MT1205X01549	0	FAN	SXX0XX_FAN	MSX60-FF	MT1206X07209	N/A	PS1	SXX0XX_PS	MSX60-PF	MT1206X06697	N/A	CPU	CPU	SA000203-B	MT1220X01231	N/A
Module	Type	Part number	Serial Number	Asic revision																											
CHASSIS	SX1036	MSX1036B-1SFR	MT1205X01549	N/A																											
MGMT	SX1036	MSX1036B-1SFR	MT1205X01549	0																											
FAN	SXX0XX_FAN	MSX60-FF	MT1206X07209	N/A																											
PS1	SXX0XX_PS	MSX60-PF	MT1206X06697	N/A																											
CPU	CPU	SA000203-B	MT1220X01231	N/A																											
Related Commands	N/A																														
Note																															

show module

show module

Displays modules status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000 Initial version
	3.3.0000 Added “Is Fatal” column
Role	admin
Example	<pre>switch (config) # show module ===== Module Type Present Power Is Fatal ===== MGMT SX1036 1 N/A Not Fatal FAN SXX0XX_FAN 1 N/A Not Fatal PS1 SXX0XX_PS 1 N/A Not Fatal PS2 SXX0XX_PS 0 N/A Not Fatal CPU CPU 1 N/A Not Fatal switch (config) #</pre>
Related Commands	N/A
Note	

show memory

show memory

Displays memory status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>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</pre> Physical Memory Borrowed for System Buffers and Cache: <pre> Buffers: 0 MB Cache: 452 MB Total Buffers/Cache: 452 MB switch (config) #</pre>
Related Commands	N/A
Note	

show asic-version

show asic-version

Displays firmware ASIC version.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>switch (config) # show asic-version ===== SX module Version ===== SX 9.1.1260 switch (config) #</pre>
Related Commands	N/A
Note	

show power

show power

Displays power supplies and power usage.

Syntax Description	N/A																																																																													
Default	N/A																																																																													
Configuration Mode	Any Command Mode																																																																													
History	3.1.0000																																																																													
Role	admin																																																																													
Example	<pre>switch (config) # show power</pre> <table><thead><tr><th>Module</th><th>Power (Watts)</th><th>Voltage</th><th>Current (Amp)</th><th>Capacity (Watts)</th><th>Grid Group</th><th>Status</th></tr></thead><tbody><tr><td>PS1</td><td>0.00</td><td>47.11</td><td>0.00</td><td>1008</td><td>A</td><td>OK</td></tr><tr><td>PS2</td><td>248.82</td><td>48.05</td><td>5.18</td><td>1008</td><td>A</td><td>OK</td></tr><tr><td>PS3</td><td>0.00</td><td>46.88</td><td>0.00</td><td>1008</td><td>A</td><td>OK</td></tr><tr><td>PS4</td><td>-</td><td>-</td><td>-</td><td>NOT PRESENT</td><td></td><td></td></tr><tr><td>PS5</td><td>46.72</td><td>47.82</td><td>0.98</td><td>1008</td><td>A</td><td>OK</td></tr><tr><td>PS6</td><td>-</td><td>-</td><td>-</td><td>NOT PRESENT</td><td></td><td></td></tr><tr><td>PS7</td><td>-</td><td>-</td><td>-</td><td>NOT PRESENT</td><td></td><td></td></tr><tr><td>PS8</td><td>-</td><td>-</td><td>-</td><td>NOT PRESENT</td><td></td><td></td></tr><tr><td>PS9</td><td>-</td><td>-</td><td>-</td><td>NOT PRESENT</td><td></td><td></td></tr><tr><td>PS10</td><td>-</td><td>-</td><td>-</td><td>NOT PRESENT</td><td></td><td></td></tr></tbody></table> <pre>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) #</pre>	Module	Power (Watts)	Voltage	Current (Amp)	Capacity (Watts)	Grid Group	Status	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		
Module	Power (Watts)	Voltage	Current (Amp)	Capacity (Watts)	Grid Group	Status																																																																								
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																																																																										
Related Commands	N/A																																																																													
Note																																																																														

show power consumers

show power consumers

Displays power consumers.

Syntax Description	N/A
---------------------------	-----

Default	N/A
----------------	-----

Configuration Mode	Any Command Mode
---------------------------	------------------

History	3.1.0000
----------------	----------

Role	admin
-------------	-------

Example	<pre>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) #</pre>
----------------	--

Related Commands	N/A
-------------------------	-----

Note	
-------------	--

show temperature

show temperature

Displays the system's temperature sensors status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	N/A
Note	

show voltage

show voltage

Displays power supplies voltage level.

Syntax Description	N/A																																																																																																								
Default	N/A																																																																																																								
Configuration Mode	Any Command Mode																																																																																																								
History	3.1.0000																																																																																																								
Role	admin																																																																																																								
Example	switch (config) # show voltage ===== <table><thead><tr><th>Module</th><th>Power Meter</th><th>Reg</th><th>Expected Voltage</th><th>Actual Voltage</th><th>Status</th><th>High Range</th><th>Low Range</th></tr></thead><tbody><tr><td>MGMT</td><td>BOARD_MONITOR</td><td>V1</td><td>5.00</td><td>5.15</td><td>OK</td><td>5.55</td><td>4.45</td></tr><tr><td>MGMT</td><td>BOARD_MONITOR</td><td>V2</td><td>2.27</td><td>2.11</td><td>OK</td><td>2.55</td><td>1.99</td></tr><tr><td>MGMT</td><td>BOARD_MONITOR</td><td>V3</td><td>1.80</td><td>1.79</td><td>OK</td><td>2.03</td><td>1.57</td></tr><tr><td>MGMT</td><td>BOARD_MONITOR</td><td>V4</td><td>3.30</td><td>3.28</td><td>OK</td><td>3.68</td><td>2.92</td></tr><tr><td>MGMT</td><td>BOARD_MONITOR</td><td>V5</td><td>0.90</td><td>0.93</td><td>OK</td><td>1.04</td><td>0.76</td></tr><tr><td>MGMT</td><td>BOARD_MONITOR</td><td>V6</td><td>1.20</td><td>1.19</td><td>OK</td><td>1.37</td><td>1.03</td></tr><tr><td>MGMT</td><td>CPU_BOARD_MONITOR</td><td>V1</td><td>12.00</td><td>11.67</td><td>OK</td><td>13.25</td><td>10.75</td></tr><tr><td>MGMT</td><td>CPU_BOARD_MONITOR</td><td>V2</td><td>2.50</td><td>2.46</td><td>OK</td><td>2.80</td><td>2.20</td></tr><tr><td>MGMT</td><td>CPU_BOARD_MONITOR</td><td>V3</td><td>3.30</td><td>3.26</td><td>OK</td><td>3.68</td><td>2.92</td></tr><tr><td>MGMT</td><td>CPU_BOARD_MONITOR</td><td>V4</td><td>3.30</td><td>3.24</td><td>OK</td><td>3.68</td><td>2.92</td></tr><tr><td>MGMT</td><td>CPU_BOARD_MONITOR</td><td>V5</td><td>1.80</td><td>1.79</td><td>OK</td><td>2.03</td><td>1.57</td></tr><tr><td>MGMT</td><td>CPU_BOARD_MONITOR</td><td>V6</td><td>1.20</td><td>1.24</td><td>OK</td><td>1.37</td><td>1.03</td></tr></tbody></table> switch (config) #	Module	Power Meter	Reg	Expected Voltage	Actual Voltage	Status	High Range	Low Range	MGMT	BOARD_MONITOR	V1	5.00	5.15	OK	5.55	4.45	MGMT	BOARD_MONITOR	V2	2.27	2.11	OK	2.55	1.99	MGMT	BOARD_MONITOR	V3	1.80	1.79	OK	2.03	1.57	MGMT	BOARD_MONITOR	V4	3.30	3.28	OK	3.68	2.92	MGMT	BOARD_MONITOR	V5	0.90	0.93	OK	1.04	0.76	MGMT	BOARD_MONITOR	V6	1.20	1.19	OK	1.37	1.03	MGMT	CPU_BOARD_MONITOR	V1	12.00	11.67	OK	13.25	10.75	MGMT	CPU_BOARD_MONITOR	V2	2.50	2.46	OK	2.80	2.20	MGMT	CPU_BOARD_MONITOR	V3	3.30	3.26	OK	3.68	2.92	MGMT	CPU_BOARD_MONITOR	V4	3.30	3.24	OK	3.68	2.92	MGMT	CPU_BOARD_MONITOR	V5	1.80	1.79	OK	2.03	1.57	MGMT	CPU_BOARD_MONITOR	V6	1.20	1.24	OK	1.37	1.03
Module	Power Meter	Reg	Expected Voltage	Actual Voltage	Status	High Range	Low Range																																																																																																		
MGMT	BOARD_MONITOR	V1	5.00	5.15	OK	5.55	4.45																																																																																																		
MGMT	BOARD_MONITOR	V2	2.27	2.11	OK	2.55	1.99																																																																																																		
MGMT	BOARD_MONITOR	V3	1.80	1.79	OK	2.03	1.57																																																																																																		
MGMT	BOARD_MONITOR	V4	3.30	3.28	OK	3.68	2.92																																																																																																		
MGMT	BOARD_MONITOR	V5	0.90	0.93	OK	1.04	0.76																																																																																																		
MGMT	BOARD_MONITOR	V6	1.20	1.19	OK	1.37	1.03																																																																																																		
MGMT	CPU_BOARD_MONITOR	V1	12.00	11.67	OK	13.25	10.75																																																																																																		
MGMT	CPU_BOARD_MONITOR	V2	2.50	2.46	OK	2.80	2.20																																																																																																		
MGMT	CPU_BOARD_MONITOR	V3	3.30	3.26	OK	3.68	2.92																																																																																																		
MGMT	CPU_BOARD_MONITOR	V4	3.30	3.24	OK	3.68	2.92																																																																																																		
MGMT	CPU_BOARD_MONITOR	V5	1.80	1.79	OK	2.03	1.57																																																																																																		
MGMT	CPU_BOARD_MONITOR	V6	1.20	1.24	OK	1.37	1.03																																																																																																		
Related Commands	N/A																																																																																																								
Note																																																																																																									

show health-report

show health-report

Displays health report.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000 Initial version
	3.3.0000 Output update
Role	admin
Example	<pre>switch (config) # show health-report ===== ALERTS CONFIGURATION ===== Re-notification counter (sec):[3600] Report max counter: [50] ===== HEALTH REPORT ===== No Health issues file switch (config) #</pre>
Related Commands	N/A
Note	

show resources

show resources

Displays system resources.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>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) #</pre>
Related Commands	N/A
Note	

show system profile

show system profile

Displays system profile.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0000
Role	admin
Example	switch (config) # show system profile eth-single-switch switch (config) #
Related Commands	system profile
Note	

show system capabilities

show system capabilities

Displays system capabilities.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000 Initial version.
	3.3.0000 Added gateway support.
Role	admin
Example	<pre>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) #</pre>
Related Commands	show system profile
Note	

show system configuration

show system configuration

Displays system configuration progress.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>// If configuration at init time is still in progress // switch (config) # show system configuration status system configuration is in progress switch (config) # // If configuration at init time is completed // switch (config) # show system configuration status system configuration is finished switch (config) #</pre>
Related Commands	N/A
Note	

show system mac

show system mac

Displays system MAC address.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	switch (config) # show system mac 00:02:C9:5E:AF:18 switch (config) #
Related Commands	N/A
Note	

show protocols

show protocols

Displays all protocols enabled in the system.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.3000
	3.3.4550 Updated output
Role	admin
Example	<pre>switch (config) # show protocols Ethernet enabled spanning-tree rstp lacp disabled lldp enabled igmp-snooping disabled ets enabled priority-flow-control disabled sflow disabled openflow enabled IP routing disabled ospf disabled dhcp-relay disabled Infiniband enabled sm enabled switch (config) #</pre>
Related Commands	N/A
Note	

show bios

show bios

Displays the bios version information.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.4150
Role	admin
Example	<pre>switch (config) # show bios BIOS version : 4.6.5 BIOS subversion : Official AMI Release BIOS release date : 07/02/2013 switch (config) #</pre>
Related Commands	
Note	The command is available only on X86 systems (not on PPC).

4.13 Network Management Interfaces

4.13.1 SNMP

Simple Network Management Protocol (SNMP), is a network protocol for the management of a network and the monitoring of network devices and their functions. SNMP supports asynchronous event (trap) notifications and queries.

MLNX-OS supports:

- SNMP versions v1, v2c and v3
- SNMP trap notifications
- Standard MIBs
- Mellanox private MIBs
- EHCM MIB

4.13.1.1 Standard MIBs

Table 23 - Standard MIBs – Textual Conventions and Conformance MIBs

MIB	Standard	Comments
INET-ADDRESS-MIB	RFC-4001	
SNMPV2-CONF		
SNMPV2-TC	RFC 2579	
SNMPV2-TM	RFC 3417	
SNMP-USM-AES-MIB	RFC 3826	
IANA-LANGUAGE-MIB	RFC 2591	
IANA-RTPROTO-MIB	RFC 2932	
IANAifType-MIB		
IANA-ADDRESS-FAMILY-NUMBERS-MIB		

Table 24 - Standard MIBs – Structure, Management Interface and General SNMP

MIB	Standard	Comments
SNMPv2-MIB	RFC 3418	
SNMP-FRAMEWORK-MIB	RFC 2571	
SNMP-VIEW-BASED-SM-MIB	RFC 3414	
SNMP-VIEW-BASED-ACM-MIB	RFC 3415	
SNMP-MPD-MIB	RFC 2572	

Table 24 - Standard MIBs – Structure, Management Interface and General SNMP

MIB	Standard	Comments
IP-MIB	RFC 4293	Management interface
TCP-MIB	RFC 4022	Management interface
UDP-MIB	RFC 4113	Management interface
IP-FORWARD-MIB	RFC 4292	Management interface
HOST-RESOURCES-MIB, HOST-RESOURCES-TYPE	RFC 2790	Management interface

Table 25 - Standard MIBs – Chassis and Switch

MIB	Standard	Comments
RFC1213-MIB	RFC 1213	
IF-MIB	RFC 2863	ifXTable only supported.
ENTITY-MIB	RFC 4133	
ENTITY-SENSOR-MIB	RFC 3433	Fan and temperature sensors
ENTITY-STATE-MIB	RFC 4268	Fan and temperature states
Bridge MIB	RFC 4188	dot1dTpFdbGroup and dot1dStaticGroup are not supported in this MIB, it is supported as a part of Q-Bridge-MIB. This MIB is not relevant to InfiniBand.
Q-Bridge MIB	RFC 4363	The following SNMP groups are not supported: • qBridgeVlanStatisticsGroup, • qBridgeVlanStatisticsOverflowGroup , • qBridgeVlanHCStatisticsGroup, • qBridgeLearningConstraintsGroup. The following SNMP tables are not supported: • dot1qTpFdbTable (dynamic UC MAC addresses) • dot1qTpGroupTable (dynamic MC MAC addresses) • dot1qForwardAllTable (GMRP) • dot1qForwardUnregisteredTable (GMRP) • dot1qVlanCurrentTable (GVRP) This MIB is not relevant to InfiniBand.
RSTP-MIB	RFC 4318	This MIB is not relevant to InfiniBand.
LLDP-MIB	802.1AB-2005	This MIB is not relevant to InfiniBand.

4.13.1.2 Private MIB

Table 26 - Private MIBs Supported

MIB	Comments
MELLANOX-SMI-MIB	Mellanox Private MIB main structure (no objects)
MELLANOX-PRODUCTS-MIB	List of OID – per managed system (sysObjID)
MELLANOX-IF-VPI-MIB	IfTable extensions
MELLANOX-EFM-MIB	Deprecated MIB (based on Mellanox-MIB) Traps definitions and test trap set scalar are supported.
MELLANOX-ENTITY-MIB	Enhances the standard ENTITY-MIB (contains GUID and ASIC revision).

Mellanox private MIBs can be downloaded from the [Mellanox Support](#) webpage.

4.13.1.3 Mellanox Private Traps

The following private traps are supported by MLNX-OS.

Table 27 - SNMP Traps

Trap	Action Required
asicChipDown	Reboot the system.
asicOverTempReset	Check fans and environmental temperature.
asicOverTemp	Check fans and environmental temperature.
lowPower	Add/connect power supplies.
internalBusError	N/A
procCrash	Generate SysDump and contact Mellanox support.
cpuUtilHigh	N/A
procUnexpectedExit	Generate SysDump and contact Mellanox support.
diskSpaceLow	Clean images and sysDump files using the commands “image delete” and “file debug-dump delete”.
systemHealthStatus	Refer to Health Status table.
lowPowerRecover	N/A
insufficientFans	Check Fans and environmental conditions.
insufficientFansRecover	N/A
insufficientPower	Add/connect power supplies, or change power mode using the command “power redundancy mode”.
insufficientPowerRecover	N/A

For additional information refer to MELLANOX-EFM-MIB.



For event-to-MIB mapping, please refer to [Table 20, “Supported Event Notifications and MIB Mapping,”](#) on page 209.

4.13.1.4 Configuring SNMP

➤ *To set up the SNMP:*

Step 1. Activate the SNMP server on the MLNX-OS switch (in configure mode) using the following commands:



Community strings are case sensitive.



Director switches (SX65xx systems) require SNMP timeout configuration on the agent of 60 seconds.

```
switch (config) # snmp-server enable
switch (config) # snmp-server enable notify
switch (config) # snmp-server community public ro
switch (config) # snmp-server contact "contact name"
switch (config) # snmp-server host <host IP address> traps version 2c public
switch (config) # snmp-server location "location name"
switch (config) # snmp-server user admin v3 enable
switch (config) # snmp-server user admin v3 prompt auth md5 priv des
```

4.13.1.5 Configuring an SNMPv3 User

➤ *To configure SNMP V3 user:*

Step 1. Configure the user using the command:

```
switch (config) # snmp-server user [role] v3 prompt auth <hash type> priv <privacy type>
```

where

- user role – admin
- auth type – md5 or sha
- priv type – des or aes-128

Step 2. Enter authentication password and its confirmation.

Step 3. Enter privacy password and its confirmation.

```
switch (config) # snmp-server user admin v3 prompt auth md5 priv des
Auth password: *****
Confirm: *****
Privacy password: *****
```

```
Confirm: *****
switch (config) #
```

To retrieve the system table, run the following SNMP command:

```
snmpwalk -v3 -l authPriv -a MD5 -u admin -A "<Authentication password>" -x DES -X "<privacy password>" <system ip> SNMPv2-MIB::system
```

4.13.1.6 Configuring an SNMP Notification

➤ **To set up the SNMP Notification (traps or informs):**

Step 1. Make sure SNMP and SNMP notification are enable. Run:

```
switch (config) # snmp-server enable
switch (config) # snmp-server enable notify
switch (config) #
```

Step 2. Configure SNMP host with the desired arguments (IP Address, SNMP version, authentication methods). More than one host can be configured. Each host may have different attributes. Run:

```
switch (config) # snmp-server host 10.134.47.3 traps version 3 user my-username auth sha
my-password
switch (config) #
```

Step 3. Verify the SNMP host configuration. Run:

```
switch (config) # show snmp host
Notifications enabled:      yes
Default notification community: public
Default notification port:  162

Notification sinks:

10.134.47.3
  Enabled:      yes
  Port:         162 (default)
  Notification type: SNMP v3 trap
  Username:     my-username
  Authentication type: sha
  Privacy type:  aes-128
  Authentication password: (set)
  Privacy password: (set)

switch (config) #
```

Step 4. Configure the desired event to be sent via SNMP. Run:

```
switch (config) # snmp-server notify event interface-up
switch (config) #
```



This particular event is used as an example only.

Step 5. Verify the list of traps and informs being sent to out of the system. Run:

```
switch (config) # show snmp events
Events for which traps will be sent:
asic-chip-down: ASIC (Chip) Down
cpu-util-high: CPU utilization has risen too high
disk-space-low: Filesystem free space has fallen too low
health-module-status: Health module Status
insufficient-fans: Insufficient amount of fans in system
insufficient-fans-recover: Insufficient amount of fans in system recovered
insufficient-power: Insufficient power supply
interface-down: An interface's link state has changed to down
interface-up: An interface's link state has changed to up
internal-bus-error: Internal bus (I2C) Error
liveness-failure: A process in the system was detected as hung
low-power: Low power supply
low-power-recover: Low power supply Recover
new_root: local bridge became a root bridge
paging-high: Paging activity has risen too high
power-redundancy-mismatch: Power redundancy mismatch
process-crash: A process in the system has crashed
process-exit: A process in the system unexpectedly exited
snmp-authtrap: An SNMP v3 request has failed authentication
topology_change: local bridge triggered a topology change
unexpected-shutdown: Unexpected system shutdown
switch (config) #
```



To print event notifications to the terminal (SSH or CONSOLE) refer to [Section 4.5.1, “Monitor,”](#) on page 175.

4.13.1.7 Internal Link Support

MLNX-OS supports displaying information of internal links on SX65xx systems via SNMP interface. This feature is disabled by default. When enabled, the internal link information is added to the IF tables IfXtable and IfVPItable. Additionally, new traps for internal link up/down, and internal link suboptimal speed are enabled. The user has the ability to enable one or both of the new traps.

Internal link up/down events are sent whenever there is a change in the internal link's physical state. These events are suppressed when a system internal link mismatch event occurs when the internal link's speed does not match the configured speed of the link.

4.13.2 XML API

MLNX-OS XML API is an additional option to manage the system (besides SNMP). The XML gateway provides an XML request-response protocol that can be used by end-user tools to get and set management information on the appliance. The service can be accessed over HTTP or HTTPS, and then it uses the existing web authentication mechanism. It can also be accessed over SSH, and then it uses the existing CLI authentication mechanism. XML Gateway - Management information base.

For further information please contact Mellanox support.

4.13.3 Commands

4.13.3.1 SNMP

The commands in this section are used to manage the SNMP server.

snmp-server auto-refresh

snmp-server auto-refresh {enable | interval}
no snmp-server auto-refresh enable

Configures SNMPD refresh settings.
 The no form of the command disables SNMPD refresh mechanism.

Syntax Description	enable	Enables SNMPD refresh mechanism.
	interval	Sets SNMPD refresh interval.
Default	Enabled. Interval: 60 secs	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show snmp	
Note	•	

snmp-server community

snmp-server community <community> [ro | rw]

no snmp-server community <community>

Sets a community name for either read-only or read-write SNMP requests.
The no form of the command sets the community string to default.

Syntax Description	community	Community name.
	ro	Sets the read-only community string.
	rw	Sets the read-write community string.
Default	Read-only community: "public" Read-write community: ""	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre> 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) # </pre>	
Related Commands	show snmp	
Note	- If neither the "ro" or the "rw" parameters are specified, the read-only community is set as the default community - If the read-only community is specified, only queries can be performed - If the read-write community is specified, both queries and sets can be performed	

snmp-server contact

snmp-server contact <contact name>

no snmp-server contact

Sets a value for the sysContact variable in MIB-II.

The no form of the command resets the parameter to its default value.

Syntax Description	contact name	Contact name.
Default	""	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre> 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) # </pre>	
Related Commands	show snmp	
Note		

snmp-server enable

snmp-server enable [communities | mult-communities | notify]
no snmp-server enable [communities | mult-communities | notify]

Enables SNMP-related functionality.
 The no form of the command disables the SNMP server.

Syntax Description	enable	Enables SNMP-related functionality: • SNMP engine • SNMP traps
	communities	Enables community-based authentication on this system.
	mult-communities	Enables multiple communities to be configured.
	notify	Enables sending of SNMP traps and informs from this system.
Default	SNMP is enabled by default SNMP server communities are enabled by default SNMP notifies are enabled by default SNMP server multi-communities are disabled by default	
Configuration Mode	Config	
History	3.1.0000	Initial version.
	3.2.1050	Change traps to notify.
Role	admin	
Example	<pre> 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) # </pre>	
Related Commands	show snmp	
Note	SNMP traps are only sent if there are trap sinks configured with the “snmp-server host...” command, and if these trap sinks are themselves enabled.	

snmp-server host

snmp-server host <IP address> {disable | {traps | informs} [<community> | <port> | version <snmp version>]}

no snmp-server host <IPv4 or IPv6 address> {disable | {traps| informs} [<community> | <port>]}

Configures hosts to which to send SNMP traps.

The no form of the commands removes a host from which SNMP traps should be sent.

Syntax Description	IP address	IPv4 or IPv6 address.
	disable	Temporarily disables sending of traps to this host.
	community	Specifies trap community string.
	port	Overrides default UDP port for this trap sink.
	snmp version	Specifies the SNMP version of traps to send to this host.
Default	No hosts are configured Default community is “public” Default UDP port is 162 Default SNMP version is 2c	
Configuration Mode	Config	
History	3.1.0000	Initial version.
	3.2.1050	Add inform option.
Role	admin	

Example

```
switch (config) # snmp-server host 10.10.10.10 traps version 1
switch (config) # show snmp
SNMP enabled:          yes
SNMP port:             161
System contact:
System location:

Read-only communities:
    public

Read-write communities:
    (none)

Interface listen enabled: yes
No Listen Interfaces.

Traps enabled:          yes
Default trap community: public
Default trap port:      162

Trap sinks:
    10.10.10.10
        Enabled: yes
        Type: traps version 1
        Port: 162 (default)
        Community: public (default)
switch (config) #
```

Related Commands

```
show snmp
snmp-server enable
```

Note

This setting is only meaningful if traps are enabled, though the list of hosts may still be edited if traps are disabled. Refer to “snmp-server enable” command.

snmp-server listen

snmp-server listen {enable | interface <ifName>}
no snmp-server listen {enable | interface <ifName> }

Configures SNMP server interface access restrictions.
 The no form of the command disables the listen interface restricted list for SNMP server.

Syntax Description	enable	Enables SNMP interface restrictions on access to this system.
	ifName	Adds an interface to the “listen” list for SNMP server. For example: “mgmt0”, “mgmt1”.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre> 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) # </pre>	
Related Commands	show snmp	
Note	If enabled, and if at least one of the interfaces listed is eligible to be a listen interface, then SNMP requests will only be accepted on those interfaces. Otherwise, SNMP requests are accepted on any interface.	

snmp-server location

snmp-server location <system location>

no snmp-server location

Sets a value for the sysLocation variable in MIB-II.

The no form of the command clears the contents of the sysLocation variable.

Syntax Description	system location String.
Default	""
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre> 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) # </pre>
Related Commands	show snmp
Note	

snmp-server notify

snmp-server notify {community <community> | event <event name> | port <port> | send-test}
no snmp-server notify {community | event <event name> | port}

Configures SNMP notifications (traps and informs).
 The no form of the commands negate the SNMP notifications.

Syntax Description	community	Sets the default community for traps sent to hosts which do not have a custom community string set.
	event	Specifies which events will be sent as traps.
	port	Sets the default port to which traps are sent.
	send-test	Sends a test trap.
Default	Community: public All informs and traps are enabled Port: 162	
Configuration Mode	Config	
History	3.1.0000	Initial version.
	3.2.1050	Change traps to notify.
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	<pre>show snmp show snmp events</pre>	
Note	- This setting is only meaningful if traps are enabled, though the list of hosts may still be edited if traps are disabled - Refer to Mellanox MIB file for the list of supported traps	

snmp-server port

snmp-server port <port>

no snmp-server port

Sets the UDP listening port for the SNMP agent.

The no form of the command resets the parameter to its default value.

Syntax Description	port	UDP port.
Default	161	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show snmp	
Note		

snmp-server user

```
snmp-server user {admin | <username> } v3 {[encrypted] auth <hash-type>
<password> [priv <privacy-type> [<password>]] | capability <cap> | enable
<sets> | prompt auth <hash-type> [priv <privacy-type>]}
no snmp-server user {admin | <username> } v3 {[encrypted] auth <hash-type>
<password> [priv <privacy-type> [<password>]] | capability <cap> | enable
<sets> | prompt auth <hash-type> [priv <privacy-type>]}
```

Specifies an existing username, or a new one to be added.
The no form of the command disables access via SNMP v3 for the specified user.

Syntax Description	v3	Configures SNMP v3 users.
	auth	Configures SNMP v3 security parameters, specifying passwords in plaintext on the command line (note: passwords are always stored encrypted).
	capability	Sets capability level for SET requests.
	enable	Enables SNMP v3 access for this user.
	encrypted	Configures SNMP v3 security parameters, specifying passwords in encrypted form.
	prompt	Configures SNMP v3 security parameters, specifying passwords securely in follow-up prompts, rather than on the command line.
Default	No SNMP v3 users defined	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show snmp user	
Note		

show snmp

show snmp [auto-refresh | engineID | events | host | user]

Displays SNMP-server configuration and status.

Syntax Description	auto-refresh	SNMP refreshed mechanism status.
	engineID	SNMP Engine ID.
	events	SNMP events.
	host	List of notification sinks.
	user	SNMP users.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>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) #</pre>	
Related Commands	show snmp	
Note		

show snmp auto-refresh

show snmp auto-refresh

Displays SNMPD refresh mechanism status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	<pre> 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) # </pre>
Related Commands	snmp-server auto-refresh
Note	

4.13.3.2 XML API

xml-gw enable

xml-gw enable
no xml-gw enable

Enables the XML gateway.
The no form of the command disables the XML gateway.

Syntax Description	N/A
Default	XML Gateway is enabled
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	switch (config) # xml-gw enable switch (config) # show xml-gw XML Gateway enabled: yes switch (config) #
Related Commands	show xml-gw
Note	

show xml-gw

show xml-gw

Displays the XML gateway setting.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	switch (config) # show xml-gw XML Gateway enabled: yes switch (config) #
Related Commands	xml-gw enable
Note	

4.14 Puppet Agent

Puppet is a software that allows network administrators to automate repetitive tasks. MLNX-OS includes a built-in agent for the open-source “Puppet” configuration change management system. The Puppet agent enables configuring Mellanox switches in accordance with the standard “puppet-netdev-stdlib” type library and with the “Mellanox-netdev-stdlib-mlnxos” and “Mellanox-netdev-ospf-stdlib” type libraries provided by Mellanox Technologies to the Puppet community.

For more information, please refer to the CLI commands, to the NetDev documentation at <https://github.com/puppetlabs/puppet-netdev-stdlib> and to Mellanox’s Puppet modules GitHub page at <https://github.com/Mellanox>.

4.14.1 Setting the Puppet Server

➤ *To set the puppet server:*

Step 1. Define the Puppet server (the name has to be a DNS and not IP). Run:

```
switch (config) # puppet-agent master-hostname <please_type_your_hostname_DNS_here>
switch (config) #
```

Step 2. Enable the Puppet agent. Run:

```
switch (config) # puppet-agent enable
switch (config) #
```

Step 3. (Optional) Verify there are no errors in the Puppet agent log. Run:

```
switch (config) # show puppet-agent log continuous
switch (config) #
```

4.14.2 Accepting the Switch Request

➤ *To accept the switch’s request:*

Option 1 – using Puppet cli commands:

Step 1. Ensure the certificate request. Run:

```
# puppet cert list
"switch-632476.mtr.labs.mlnx"
(F4:B4:20:3B:2B:11:76:37:14:34:D0:D1:03:ED:3D:B5)
```

Step 2. Sign the certificate request if the cert_name parameter (e.g. switch1.domain) is in the list. Run:

```
# puppet cert sign <full_domain_name>
```

Step 3. Verify the request is removed from the Puppet certification list. Run:

```
# puppet cert list
```

Option 2 – accept certificate requests in the puppet server console:

Step 1. Go to the “nodes requests” page (the button is at the top right), and wait for a certificate request for the switch and then accept it.

Figure 10: Accepting an Agent Request through the Console

Pending node requests: 1

Name	Fingerprint	Action
switch-632476.mtr.labs.mlnx	29:9F:4B:1F...	Accept Reject

4.14.3 Installing Modules on the Puppet Server

Mellanox uses netdev-stdlib types and provides a package of Mellanox providers for those types which have to be installed at the Puppet server prior to the first Puppet configuration run (before configuring resources on the Mellanox switch).

To install those modules, run the following commands in the Puppet server:

```
# puppet module install netdevops-netdev_stdlib
# puppet module install mellanox-netdev_ospf_stdlib
# puppet module install mellanox-netdev_stdlib_mlnxos
```



In case of an already installed module, please use the command “puppet module upgrade <module_name>” or “puppet module install <module_name> - -force” instead of “puppet module install <module_name>” to reinstall the modules.

For more information please refer to the Network Automation Tools document or Puppet category in the Mellanox community site at: <http://community.mellanox.com/community/support/solutions>.

4.14.4 Writing Configuration Classes

➤ To write configuration classes:

Step 1. Assigning Configuration Classes to a Node

Configuration files can be written and changed in the puppet server machine in the directory “/etc/puppetlabs/puppet/manifests/” (or “/etc/puppet/manifests” in case of an open source puppet server).

The file “/etc/puppetlabs/puppet/manifests/site.pp” is the main file for Puppet-classes-to-nodes association. To associate a configuration to a Puppet agent node, just append association lines as below:

```
Import "netdev_vlan_example"
Import "netdev_l2_vlan_example"
Import "netdev_lag_example"
node 'switch-6375dc.mtr.labs.mlnx'{

  netdev_device { $hostname: }

  include vlan_example # Asserts a class vlan_example in one of the files
  include l2_interface_example
```

```
include lag_example

}
```



If you have a puppet console, you may assign classes of configuration in the following way:

- Add the relevant classes (using the console add class button on the “nodes” page).
- Assign the classes to the relevant nodes/groups in the puppet server console (in the console node/group page -> edit -> Classes).

Step 2. Update VLAN

Manifest example (located in “/etc/puppetlabs/puppet/manifests/netdev_vlan_example.pp”).

```
class vlan_example{

    $vlans = {
        'Vlan244' => {vlan_id => 244, ensure => present},
        'Vlan245' => {vlan_id => 245, ensure => present},
    }

    create_resources( netdev_vlan, $vlans )
}
```

Step 3. Update Layer 2 Interface.

Manifest example (located in “/etc/puppetlabs/puppet/manifests/netdev_l2_interface_example.pp”)

```
class vlans_ensure_example{

    $vlans = {
        'Vlan347' => {vlan_id => 347, ensure => present},
        'Vlan348' => {vlan_id => 348, ensure => present},
        'Vlan349' => {vlan_id => 349, ensure => present},
    }

    create_resources( netdev_vlan, $vlans )
}

class l2_interface_example{

    include vlans_ensure_example #class to Ensure VLANs before assigning

    $l2_interfaces = {
        'ethernet 1/3' => {ensure => absent, vlan_tagging => disable}, #default
        'ethernet 1/4' => {ensure => present, vlan_tagging => enable,
        tagged_vlans => [Vlan348,Vlan347], untagged_vlan => Vlan349} #hybrid
    }

    create_resources( netdev_l2_interface, $l2_interfaces )
}
```

Step 4. Update LAG.

Manifest example (located in “/etc/puppetlabs/puppet/manifests/netdev_lag_example.pp”)

```
class lag_example{

    $lags = {
        'port-channel 101' => {ensure => present,
        links => ['ethernet 1/12', 'ethernet 1/13'], lacp => active},
        'port-channel 102' => {ensure => present,
        links => ['ethernet 1/6', 'ethernet 1/5'], lacp => disabled},
    }

    create_resources( netdev_lag, $lags )
}
```



You may add classes to ensure that all assigned links are with the same layer 1 and layer 2 configurations (similarly to the way we did in update l2_interface section with vlans_ensure_example class).

4.14.5 Supported Configuration Capabilities

4.14.5.1 Ethernet, Port-Channel, and InfiniBand Interface Capabilities

Table 28 - Ethernet, Port-Channel, and InfiniBand Interface Capabilities

Field	Description	Values	Example
ensure	Sets the given values or restores the interface to default	absent, present	ensure => present
speed	Sets the speed of the interface.	auto* 10m 100m 1g 10g 40g 56g	speed => 1g
admin	Disables/enables interface admin state.	up, down	admin => up
mtu	Configures the maximum transmission unit frame size for the interface.	Ethernet: 1518-9216	mtu => 1520
description	Sets the Ethernet, LAG and InfiniBand description.	Text	description => “changed_by_puppet”

4.14.5.2 VLAN Capabilities

Table 29 - VLAN Capabilities

Field	Description	Values	Example
ensure	Creates or destroys the VLAN given as a resource ID	absent, present	ensure => present
vlan_id	The VLAN ID	1-4094 (integer)	vlan_id => 245

4.14.5.3 Layer 2 Ethernet Interface Capabilities

Table 30 - L2 Ethernet and Port-Channel Interface Capabilities

Field	Description	Values	Example
ensure	Sets the given values or restores the Layer 2 interface to default.	absent, present	ensure => present
vlan_tagging	VLAN tagging mode	enable,disable	vlan_tagging => enable
tagged_vlans	List of tagged (trunked) VLANs	2-4994 (range)	tagged_vlans => [Vlan348,Vlan347]
untagged_vlan	Untag (access) VLAN	<VLAN name>	untagged_vlan => Vlan349

4.14.5.4 LAG (Port-Channel) Capabilities

Table 31 - LAG Capabilities

Field	Description	Values	Example
ensure	creates or destroys the port-channel given as a resource ID	absent, present	ensure => present
lacp	The LACP mode of the LAG	passive active on	lacp => on
links	List of ports assigned to the LAG	List of link names	links => ['ethernet 1/6','ethernet 1/5']

4.14.5.5 Layer 3 Interface Capabilities

Table 32 - L3 Interface Capabilities

Field	Description	Values	Example
ensure	Creates or destroys the interface VLAN specified in the resource ID.	present, absent	ensure => present

Table 32 - L3 Interface Capabilities

Field	Description	Values	Example
ipaddress	Sets IP address on the Layer 3 interface (requires netmask).	A valid IP address	ipaddress => '192.168.4.2'
netmask	Sets netmask for the IP address.	A valid netmask (of the form X.1X2.X3.X4), which creates a valid combination with the given IP address	netmask => '255.255.255.0'
method	Configures the method of the L3 interface (currently supports only static method).	static	method => static

4.14.5.6 OSPF Interface Capabilities

Table 33 - OSPF Interface Capabilities

Field	Description	Values	Example
ensure	Creates or destroys the OSPF interface of the associated interface of the VLAN specified in the resource ID	present, absent	ensure => present
area_id	The associated area ID	Integer representing an IP	area_id => '7200'
Type	The network type	broadcast, point_to_point	type => 'point_to_point'

4.14.5.7 OSPF Area Capabilities

Table 34 - OSPF Area Capabilities

Field	Description	Values	Example
ensure	Creates or destroys the OSPF area specified in the resource ID	present, absent	ensure => present
router_id	The OSPF area associated router ID (currently supports only default router)	default	router_id => 'default'
ospf_area_mode	The OSPF area mode	normal, stub, nssa	ospf_area_mode => 'stub'
subnets	A list of associated subnets	List of subnets	['192.168.4.0/24', '192.168.5.0/24']

4.14.5.8 Router OSPF Capabilities

Table 35 - Router OSPF Capabilities

Field	Description	Values	Example
ensure	Enables/disables the router ID specified in the resource ID	present, absent	ensure => present

4.14.5.9 Protocol LLDP, SNMP, IP Routing and Spanning Tree Capabilities

Table 36 - Protocol Enable/Disable Capabilities

Field	Description	Values	Example
ensure	Enables/disables the protocol specified in the resource ID	present, absent	ensure => present

4.14.5.10 Fetched Image Capabilities

Table 37 - Fetched Image Capabilities

Field	Description	Values	Example
ensure	Enables/disables the protocol specified in the resource ID	present, absent	ensure => present
protocol	Specifies the protocol for fetch method	http, https, ftp, tftp, scp, sftp	protocol => scp
host	The host where the file-name located	DNS/IP	host => my_DNS
user	The username for fetching the image	Username	user => my_username
password	The password for fetching the image	Password	password => my_pass
location	The location of the file name in the host file system	Directory full path	location => '/tmp'
force_delete	Remove all the images or only the ones which are not installed on any partition, before fetching	yes, no	force_delete => no

4.14.5.11 Installed Image Capabilities

Table 38 - Fetched Image Capabilities

Field	Description	Values	Example
ensure	Specifies if the image version given in as resource ID is ensured to be installed or not	present, absent	ensure => present
is_next_boot	Ensures that the installed image is the next boot partition	yes, no	is_next_boot => yes
configuration_write	Writes configurations to database.	yes, no	configuration_write => yes
force_reload	Reload if image is in other partition.	yes, no	force_reload => no

4.14.6 Supported Resources for Each Type

Table 39 - Fetched Image Capabilities

Resource Type	Puppet Type Name	Supported Resource IDS	Example
Network device	netdev_device	\$hostname	netdev_device { \$hostname: }
Layer 1 interface	netdev_interface	'ethernet <#ID>', 'port-channel <#id>', 'ib <#ID>'	netdev_interface{'ethernet 1/3': ensure => absent}
Layer 2 interface	netdev_l2_interface	'ethernet <#ID>', 'port-channel <#id>'	netdev_l2_interface{'ethernet 1/3': ensure => absent}
VLAN	netdev_vlan	VLAN name string	netdev_vlan {'Vlan244': vlan_id => 244, ensure => present }
LAG	netdev_lag	'port-channel <#id>'	netdev_lag {'port-channel 101': ensure => present }
Layer 3 interface	netdev_l3_interface	'vlan <#ID>'	netdev_l3_interface { 'vlan 4': ipaddress => '192.168.4.2', netmask => '255.255.255.0' }
OSPF interface	netdev_ospf_interface	'vlan <#ID>'	netdev_ospf_interface { 'vlan 4': ensure => present, area_id => '10' }
OSPF area	netdev_ospf_area	Valid area ID (representing an IP)	netdev_ospf_area { '10': ensure => present, ospf_area_mode=>'stub' }
OSPF router	netdev_router_ospf	Currently only supports 'default'	netdev_router_ospf { 'default': ensure => present }
Protocol	mlnx_protocol	ip_routing, lldp, snmp, spanning_tree	mlnx_protocol { 'ip_routing': ensure => present }
Fetched image	mlnx_fetched_img	The image file name	mlnx_fetched_image { 'image-PPC_M460EX-SX_3.3.4300.img': ensure => present }
Installed image	mlnx_installed_img	The image version name	mlnx_installed_img { 'SX_3.3.4300': ensure => present }

4.14.7 Troubleshooting

This section presents common issues that may prevent the switch from connecting to the puppet server.

4.14.7.1 Switch and Server Clocks are not Synchronized

This can be fixed by using NTP to synchronize the clocks at the switch (using the CLI command `ntp`) and at the server (e.g. using `ntpd`).

4.14.7.2 Outdated or Invalid SSL Certificates Either on the Switch or the Server

This can be fixed on the switch using the CLI command `puppet-agent clear-certificates` (requires `puppet-agent restart` to take effect).

On the server it can be fixed by running `puppet cert clean <switch_fqdn>` (FQDN is the Fully Qualified Domain Name which consists of a hostname and a domain suffix).

4.14.7.3 Communications Issue

Make sure it is possible to ping the puppet server hostname from the switch (using the CLI command `ping`).

If the hostname is not reachable (e.g. no DNS server) it can be statically added to the switch local hosts lookup (using the CLI command `ip host`).

Make sure that port 8140 is open (using the command `tracert {<hostname> | <ip>}/8140`).

4.14.8 Commands

puppet-agent

puppet-agent

Enters puppet agent configuration mode.

Syntax Description	N/A
Default	None
Configuration Mode	Config
History	3.3.4200
Role	admin
Example	switch (config) # puppet-agent switch (config puppet-agent) #
Related Commands	
Note	

master-hostname

master-hostname <hostname>

no master-hostname

Sets the puppet server hostname.

The no form of the command resets the parameter to its default.

Syntax Description	hostname	Puppet server hostname. Free string may be entered.
Default	puppet	
Configuration Mode	Config Puppet	
History	3.3.4200	
Role	admin	
Example	<pre>switch (config puppet-agent) # master-hostname my-puppet-server-host-name switch (config puppet-agent) #</pre>	
Related Commands		
Note		

enable

enable
no enable

Enables the puppet server on the switch.
The no form of the command disables the puppet server.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config Puppet
History	3.3.4200
Role	admin
Example	switch (config puppet-agent) # enable switch (config puppet-agent) #
Related Commands	
Note	

run-interval

run-interval <time>

Configures the time interval in which the puppet agent reports to the puppet server.

Syntax Description	time	Can be in seconds ("30" or "30s"), minutes ("30m"), hours ("6h"), days ("2d"), or years ("5y").
Default	30m	
Configuration Mode	Config Puppet	
History	3.3.4302	
Role	admin	
Example	switch (config puppet-agent) # run-interval 40m switch (config puppet-agent) #	
Related Commands	show puppet-agent	
Note		

restart

puppet-agent restart

Restarts the puppet agent.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config Puppet
History	3.3.4200
Role	admin
Example	switch (config puppet-agent) # restart switch (config puppet-agent) #
Related Commands	
Note	

show puppet-agent

show puppet-agent

Displays Puppet agent status and configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.4200
	3.3.4302 Updated output with run interval
Role	admin
Example	switch (config puppet-agent) # show puppet-agent Puppet agent is disabled Puppet master hostname: puppet Run interval: 40m switch (config puppet-agent) #
Related Commands	
Note	

show puppet-agent log

show puppet-agent log [[not] [matching | continuous] <string> | files [[not] matching] <string>]

Displays the Puppet agent's log file.

Syntax Description	continuous	Puppet agent log messages as they arrive.
	files	Displays archived Puppet agent log files.
	matching	Displays Puppet agent log that match a given string.
	not	Displays Puppet agent log that do not meet a certain string.
	string	Free string.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4200	
Role	admin	
Example	<pre>switch (config puppet-agent) # show puppet-agent log Mon Nov 04 11:52:42 +0000 2013 Puppet (notice): Starting Puppet client version 3.2.3 Mon Nov 04 11:52:44 +0000 2013 Puppet (warning): Unable to fetch my node definition, but the agent run will continue: Mon Nov 04 11:52:44 +0000 2013 Puppet (warning): Could not intern from pson: source '"<Puppet::Node:0x7f' not in PSON! Mon Nov 04 11:53:21 +0000 2013 /Netdev_vlan[Vlan104]/ensure (notice): created Mon Nov 04 11:53:22 +0000 2013 /Netdev_vlan[Vlan101]/ensure (notice): created Mon Nov 04 11:53:23 +0000 2013 /Netdev_vlan[Vlan102]/ensure (notice): created Mon Nov 04 11:53:24 +0000 2013 /Netdev_vlan[Vlan103]/ensure (notice): created Mon Nov 04 11:53:40 +0000 2013 /Netdev_l2_interface[ethernet 1/6]/untagged_vlan (notice): untagged_vlan changed 'default' to 'Vlan103' Mon Nov 04 11:53:43 +0000 2013 /Netdev_l2_interface[ethernet 1/7]/untagged_vlan (notice): untagged_vlan changed 'default' to 'Vlan103' Mon Nov 04 11:53:48 +0000 2013 /Netdev_vlan[Vlan100]/ensure (notice): created Mon Nov 04 11:53:48 +0000 2013 /Netdev_l2_interface[ethernet 1/5]/vlan_tagging (notice): vlan_tagging changed 'enable' to 'disable' Mon Nov 04 11:53:48 +0000 2013 /Netdev_l2_interface[ethernet 1/5]/tagged_vlans (notice): tagged_vlans changed '[' to '[Vlan100,Vlan101,Vlan102]' Mon Nov 04 11:53:51 +0000 2013 /Netdev_l2_interface[ethernet 1/1]/tagged_vlans (notice): tagged_vlans changed '[' to '[Vlan101,Vlan104]' Mon Nov 04 11:53:51 +0000 2013 /Netdev_l2_interface[ethernet 1/1]/untagged_vlan (notice): untagged_vlan changed 'default' to 'Vlan100' Mon Nov 04 11:53:54 +0000 2013 /Netdev_l2_interface[ethernet 1/3]/tagged_vlans (notice): tagged_vlans changed '[' to '[Vlan101,Vlan104]' Mon Nov 04 11:53:54 +0000 2013 /Netdev_l2_interface[ethernet 1/3]/untagged_vlan (notice): untagged_vlan changed 'default' to 'Vlan100' Mon Nov 04 11:53:58 +0000 2013 /Netdev_l2_interface[ethernet 1/4]/vlan_tagging (notice): vlan_tagging changed 'enable' to 'disable' Mon Nov 04 11:53:58 +0000 2013 /Netdev_l2_interface[ethernet 1/4]/tagged_vlans (notice): tagged_vlans changed '[' to '[Vlan100,Vlan101,Vlan102]' Mon Nov 04 11:54:03 +0000 2013 /Netdev_l2_interface[ethernet 1/2]/tagged_vlans (notice): tagged_vlans changed '[' to '[Vlan101,Vlan104]' Mon Nov 04 11:54:03 +0000 2013 /Netdev_l2_interface[ethernet 1/2]/untagged_vlan (notice): untagged_vlan changed 'default' to 'Vlan100' Mon Nov 04 11:54:06 +0000 2013 Puppet (notice): Finished catalog run in 47.90 seconds switch (config puppet-agent) #</pre>	
Related Commands		
Note		

5 Ethernet Switching

5.1 Interface

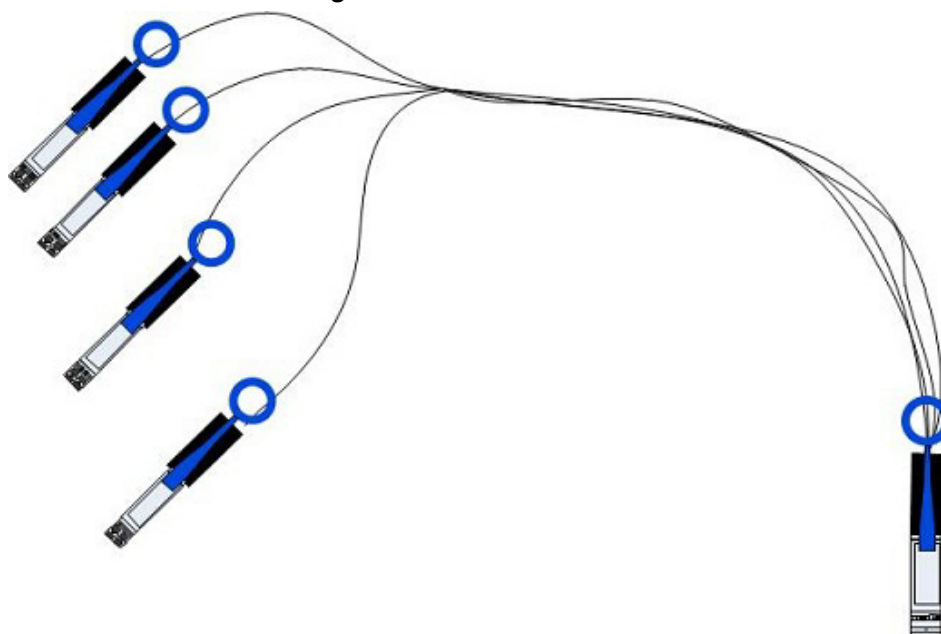
Interface Ethernet have the following physical set of configurable parameters

- Admin state – enabling or disabling the interface.
- Flow control – admin state per direction (send or receive)
- MTU (Maximum Transmission Unit) – 1518-9216 bytes
- Speed – 1/10/40/56GbE (depends on the interface type and system)
- Description – user defined string
- Module-type – the type of the module plugged in the interface

5.1.1 Break-Out Cables

The break-out cable is a unique Mellanox capability, where a single physical 40Gbps port is divided into 2x10Gbps or 4x10Gbps ports. It maximizes the flexibility of the end user to use the Mellanox switch with a combination of 10Gbps and 40Gbps interfaces according to the specific requirements of its network. Certain ports cannot be split at all and there are ports which can be split into 2 ports only. Splitting a port changes the notation of that port from x/y to x/y/z with “x/y” indicating the previous notation of the port prior to the split and “z” indicating the number of the resulting 10G port (1,2 or 1,2,3,4). Each sub-physical port is then handled as an individual port. For example: splitting port 20 into 4 will give the following new ports: 1/20/1, 1/20/2, 1/20/3, 1/20/4.

Figure 11: Break-Out Cable



A split-4 operation results in blocking a 40G port in addition to the one being split. A set of hardware restrictions determine which of the ports can be split.

Specific ports can be split by using a QSFP 1X4 breakout cable to split one 40 Gb/s port into 4 lanes (4 SFP+ connectors). These 4 lanes then go, one lane to each of the 4 SFP+ connectors. Some ports can be split into 2 10 Gb/s ports, using lanes 1 and 2 only. When a QSFP port is split into 2 10Gb/s ports then only SFP+ connectors #1 and #2 are used. Connectors #3 and #4 are left unconnected.

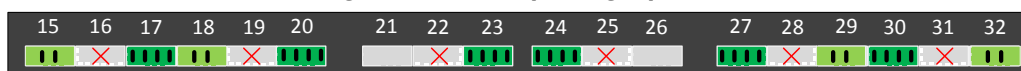


Splitting the interface deletes all configuration on that interface.

When using a port to split a data stream into 4-10Gb/s data streams (four lanes) one of the other ports on the switch will be disabled (unmapped).

- which ports can be split into 4
- which ports can be split into 2
- which ports will be unmapped due to a 1X4 split

Figure 12: Port Splitting Options



This port can be split into 4 10Gb/s SFP+

This port can be split into 2 10Gb/s SFP+

This port is unmapped by the neighboring split 4 port

The maximum number of 10 Gb/s Ethernet ports configurable with this switch is 34.

Table 40 - Port Splitting Options

Port #	Can be split to 4	Turns off port #	Can be split to 2	Port #	Can be split to 4	Turns off port #	Can be split to 2
15	—		YES	24	YES	25	—
16	—		—	25	—		—
17	YES	16	—	26	—		—
18	—		YES	27	YES	28	—
19	—		—	28			—
20	YES	19	—	29			YES
21	—		—	30	YES	31	—
22	—		—	31	—		—
23	YES	22	—	32	—		YES

To see the exact splitting options available per system, refer to each specific system's hardware user manual (Cabling chapter) located on the Mellanox website.

5.1.1.1 Changing the Module Type to a Split Mode

➤ *To split a port of an interface:*

Step 1. Shut down all the ports related to the interface. Run:

- in case of split-2, shut down the current interface only
- in case of split-4, shut down the current interface and the other interface

```
switch (config) # interface ethernet 1/19
switch (config interface ethernet 1/19) # shutdown
switch (config interface ethernet 1/19) # exit
switch (config) # interface ethernet 1/20
switch (config interface ethernet 1/20) # shutdown
```

Step 2. Split the ports as desired. Run:

```
switch (config interface ethernet 1/20) # module-type qsfp-split-4
switch (config interface ethernet 1/20) #
```

Step 3. The following warning will be displayed:
the following interfaces will be unmapped: 1/20 1/19.
Choose Yes when prompted Type 'yes' to confirm split

The <ports> field in the warning refers to the affected ports from splitting port <inf> in the applied command.



Please beware that splitting a port into 4 prevents you from accessing the splittable port, and an additional one. For example, in the procedure above, ports 19 and 20 become inaccessible.

5.1.1.2 Unsplitting a Split Port

➤ *To unsplit a split port:*

Step 1. Shut down all of the split ports. Run:

```
switch (config interface ethernet 1/20/4) # shutdown
switch (config interface ethernet 1/20/4) # exit
switch (config) # interface ethernet 1/20/3
switch (config interface ethernet 1/20/3) # shutdown
switch (config interface ethernet 1/20/3) # exit
switch (config) # interface ethernet 1/20/2
switch (config interface ethernet 1/20/2) # shutdown
switch (config interface ethernet 1/20/2) # exit
switch (config) # interface ethernet 1/20/1
switch (config interface ethernet 1/20/1) # shutdown
```

Step 2. From the first member of the split (1/20/1), change the module-type back to QSFP. Run:

```
switch (config interface ethernet 1/20/1) # module-type qsfp
```



The module-type can be changed **only** from the first member of the split and **not** from the interface that was split.

The following warning will be displayed:

The following interfaces will be unmapped: 1/20/1 1/20/2 1/20/3 1/20/4.

Step 3. Type yes when prompted Type 'yes' to confirm unsplit.

5.1.2 Transceiver Information

MLNX-OS offers the option of viewing the transceiver information of a module or cable connected to a specific interface. The information is a set of read-only parameters burned onto the EEPROM of the transceiver by the manufacture. The parameters include identifier (connector type), cable type, speed and additional inventory attributes.

➤ **To display transceiver information of a specific interface, run:**

```
switch (config) # show interfaces ethernet 1/20 transceiver
Port 1/60 state
  identifier           : QSFP+
  cable/ module type   : Passive copper, unequalized
  ethernet speed and type: 56GigE
  vendor               : Mellanox
  cable length         : 1m
  part number          : MC2207130-001
  revision             : A3
  serial number        : MT1238VS04936
switch (config) #
```



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

5.1.3 Commands

interface ethernet

interface ethernet <slot>/<port>[/<subport>]-[/<slot>/<port>[/<subport>]]

Enters the Ethernet interface or Ethernet interface range configuration mode.

Syntax Description	<slot>/<port>	Ethernet port number.
	subport	Ethernet subport number. to be used in case of split port.
Default	N/A	
Configuration Mode	Config	
History	3.1.0000	Initial version.
	3.2.1100	Added range support.
Role	admin	
Example	<pre>switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # exit switch (config) # interface ethernet 1/1-1/10 switch (config interface ethernet 1/1-1/10) #</pre>	
Related Commands	show interfaces ethernet	
Note		

flowcontrol

flowcontrol {receive | send} {off | on} [force]

Enables or disables IEEE 802.3x link-level flow control per direction for the specified interface.

Syntax Description	receive send	receive - ingresses direction send - egresses direction
	off on	on - enables IEEE 802.3x link-level flow control for the specified interface on receive or send. off - disables IEEE 802.3x link-level flow control for the specified interface on receive or send
	force	Forces command implementation.
Default	receive off, send off	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.0000	
Role	admin	
Example	switch (config interface ethernet 1/1) # flowcontrol receive off switch (config interface ethernet 1/1) #	
Related Commands	show interfaces ethernet	
Note	N/A	

mtu

mtu <frame-size>

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

Syntax Description	frame-size	This value may be 1518-9216 bytes.
Default	1522 bytes	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.0000	
Role	admin	
Example	switch (config interface ethernet 1/1) # mtu 9216 switch (config interface ethernet 1/1) #	
Related Commands	show interfaces ethernet	
Note		

shutdown

shutdown
no shutdown

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

Syntax Description	N/A
Default	The interface is enabled.
Configuration Mode	Config Interface Ethernet Config Interface Port Channel
History	3.1.0000
Role	admin
Example	switch (config interface ethernet 1/1) # shutdown switch (config interface ethernet 1/1) #
Related Commands	show interfaces ethernet
Note	

description

description <string>

no description

Sets an interface description.

The no form of the command returns the interface description to its default value.

Syntax Description	string	40 bytes
Default	""	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.1.0000	
Role	admin	
Example	switch (config interface ethernet 1/1) # description my-interface switch (config interface ethernet 1/1) #	
Related Commands	show interfaces ethernet	
Note		

speed

speed <port speed> [force]

no speed

Sets the speed of the interface.

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

Syntax Description	port speed	1000 - 1GbE 10000 - 10GbE 40000 - 40GbE auto - auto negotiates link speed
	force	force changing the speed.
Default	Depends on the port module type, see the “Notes” section below.	
Configuration Mode	Config Interface Ethernet	
History	3.1.0000	
	3.3.3500	Added auto negotiation option
Role	admin	
Example	switch (config interface ethernet 1/1) # speed 40000 switch (config interface ethernet 1/1) #	
Related Commands	show interfaces ethernet	
Note	• 56Gbps port speed requires a license (LIC-6036F-56GE) • The default speed depends on the interface capabilities, interface capable with 40Gbps will have 40Gbps speed by default • Not all interfaces support all speed options	

load-interval

load-interval <time>

no load-interval

Sets the interface counter interval.

The no form of the command resets the interval to its default value.

Syntax Description	time	In seconds.
Default	300 seconds.	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.3.0000	
Role	admin	
Example	switch (config interface ethernet 1/1) # load-interval 30 switch (config interface ethernet 1/1) #	
Related Commands	show interfaces ethernet	
Note	This interval is used for the ingress rate and egress rate counters.	

clear counters

clear counters

Clears the interface counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config Interface Ethernet Config Interface Port Channel
History	3.1.0000
Role	admin
Example	switch (config interface ethernet 1/1) # clear counters switch (config interface ethernet 1/1) #
Related Commands	show interfaces ethernet
Note	

show interfaces ethernet

show interfaces ethernet <inf> [counters [priority]]

Displays the configuration and status for the interface.

Syntax Description	inf	Interface number: <slot>/<port>.
	counters	Displays interface extended counters.
	priority	Displays interface extended counters, per priority (0-7).
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	
Example	<pre> switch (config) # show interfaces ethernet 1/1 Eth1/1 Admin state: Enabled Operational state: Up Description: N/A Mac address: 00:02:c9:71:ed:2d MTU: 1500 bytes(Maximum packet size 1522 bytes) Flow-control: receive off send off Actual speed: 40 Gbps Width reduction mode: Not supported Switchport mode: access Last clearing of "show interface" counters 00:20:39 60 seconds Ingress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec 60 seconds Egress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec Rx 0 packets 0 unicast packets 0 multicast packets 0 broadcast packets 0 bytes 0 error packets 0 discard packets Tx 63 packets 0 unicast packets 63 multicast packets 0 broadcast packets 4032 bytes 0 discard packets switch (config) # </pre>	
Related Commands		
Note		

show interfaces ethernet [<inf>] capabilities

show interfaces ethernet [<inf>] capabilities

Displays the interface capabilities.

Syntax Description	inf	shows only one interface capabilities. Interface number: <slot>/<port>.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # show interfaces ethernet 1/1 capabilities Eth1/1 Speed : 10000,40000 FlowControl : Send, Receive switch (config) #</pre>	
Related Commands		
Note		

show interfaces ethernet [<inf>] description

show interfaces ethernet [<inf>] description

Displays the admin status and protocol status for the specified interface.

Syntax Description	inf	Interface number: <slot>/<port>.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # show interfaces ethernet 0/1 description Interface Status Protocol ----- - Ethernet 1/1 Enables up switch (config) #</pre>	
Related Commands		
Note		

show interfaces ethernet [<inf>] status

show interfaces ethernet [<inf>] status

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

Syntax Description	infInterface number: <slot>/<port>.			
Default	N/A			
Configuration Mode	Any Command Mode			
History	3.1.0000			
Role	admin			
Example	switch (config) # show interfaces ethernet status			
	Port	Operational state	Speed	Negotiation
	Eth1/1	Up	40 Gbps	No-Negotiation
	Eth1/2	Up	10 Gbps	No-Negotiation
	Eth1/3	Up	40 Gbps	No-Negotiation
	...			
	switch (config) #			
Related Commands				
Note				

show interfaces ethernet [*<inf>*] transceiver**show interfaces ethernet [<inf>] transceiver**

Displays the transceiver info.

Syntax Description	inf interface number: <slot>/<port>
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0000
Role	admin
Example	<pre>switch (config) # show interfaces ethernet 1/1 transceiver Port 1/1 state identifier : QSFP+ cable/ module type : Optical cable/ module ethernet speed and type: 40GBASE - SR4 vendor : Mellanox cable_length : 50 m part number : MC2210411-SR4 revision : A1 serial number : TT1151-00006 switch (config) #</pre>
Related Commands	
Note	

module-type

module-type <type> [force]

Splits or un-splits the interface, as desired.

Syntax Description	type	qsfp - Port runs at 40000/56000Mbps. qsfp-split-2 - Port is split and runs at 2X10000Mbps. qsfp-split-4 - Port is split and runs at 4X10000Mbps.
	force	force the split operation without asking for user confirmation.
Default	interface module type is qsfp (if the interface supports 40Gbps speed)	
Configuration Mode	Config Interface Ethernet	
History	3.1.1400	
Role	admin	
Example	<pre>switch (config interface ethernet 1/4) # module-type qsfp-split-4 the following interfaces will be unmapped: 1/4 1/1 Type 'yes' to confirm split: yes switch (config interface ethernet 1/4) #</pre>	
Related Commands	<pre>switchport mode switchport [trunk hybrid] allowed-vlan show vlan</pre>	
Note	- The affected interfaces should be disabled prior to the operation - in order to un-split the interface - used the command with “qsfp”, the speed is set to 40Gbps “module-type qsfp”. - This command is applicable only on 40Gbps Ethernet ports	

5.2 Link Aggregation Group (LAG)

Link Aggregation protocol describes a network operation in which several same speed links are combined into a single logical entity with the accumulated bandwidth of the originating ports. LAG groups exchange Lag Aggregation Control Protocol (LACP) packets in order to align the functionality between both endpoints of the LAG. To equally send traffic on all LAG links, the switch uses a hash function which can use a set of attributes as key to the hash function.

As many as 16 physical ports can be aggregated on a single LAG.

5.2.1 Configuring Static Link Aggregation Group (LAG)

➤ *To configure a static LAG:*

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Create a port-channel entity. Run:

```
switch (config) # interface port-channel 1
switch (config interface port-channel 1) #
```

Step 4. Change back to config mode.

```
switch (config interface port-channel 1) # exit
switch (config) #
```

Step 5. Add a physical port to the port-channel. Run:

```
switch (config interface ethernet 1/4) # channel-group 1 mode on
switch (config interface ethernet 1/4) #
```



If the physical port is operationally up, this port becomes an active member of the aggregation. Consequently, it becomes able to convey traffic.

5.2.2 Configuring Link Aggregation Control Protocol (LACP)

➤ *To configure LACP:*

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Create a port-channel entity. Run:

```
switch (config) # interface port-channel 1
switch (config interface port-channel 1) #
```

Step 4. Change back to config mode. Run:

```
switch (config interface port-channel 1) # exit
switch (config) #
```

Step 5. Enable LACP in the switch. Run:

```
switch (config) # lacp
switch (config) #
```

Step 6. Add a physical port to the port-channel. Run:

```
switch (config interface ethernet 1/4) # channel-group 1 mode active/passive
switch (config interface ethernet 1/4) #
```

5.2.3 Commands

interface port-channel

interface port-channel <1-4096>[-<2-4096>]
no interface port-channel <1-4096>[-<2-4096>]

Creates a port channel and enters the port-channel configuration mode. There is an option to create a range of port-channel interfaces.
 The no form of the command deletes the port-channels, or range of port-channels.

Syntax Description	1-4096 / 2-4096	Port channel number.
Default	Port channels are not created by default.	
Configuration Mode	Config	
History	3.1.1400	Initial version.
	3.2.1100	Added range support.
Role	admin	
Example	<pre>switch (config)# interface port-channel 1 switch (config interface port-channel 1) # exit switch (config)# interface port-channel 1-10 switch (config interface port-channel 1-10) #</pre>	
Related Commands		
Note		

lACP

lACP
no lACP

Enables LACP in the switch.
The no form of the command disables LACP in the switch.

Syntax Description	N/A
Default	LACP is disabled.
Configuration Mode	Config
History	3.1.1400
Role	admin
Example	switch (config)# lACP switch (config)#
Related Commands	
Note	

lacp system-priority

lacp system-priority <1-65535>

no lacp system-priority

Configures the LACP system priority.

The no form of the command sets the LACP system-priority to default.

Syntax Description	1-65535	LACP system-priority.
Default	32768	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	
Example	<pre>switch (config)# lacp system-priority 1 switch (config)# show lacp interfaces port-channel Port-channel Module Admin Status is enabled Port-channel System Identifier is 00:02:c9:5c:61:70 LACP System Priority: 3 switch (config)#</pre>	
Related Commands		
Note		

lacp (interface)

lacp {rate fast | port-priority <1-65535>}

no lacp {rate fast | port-priority}

Configures the LACP interface parameters.

The no form of the command sets the LACP interface configuration to default.

Syntax Description	rate fast	Sets LACP PDUs on the port to be in fast (1 second) or slow rate. (30 seconds).														
	1-65535	LACP port-priority.														
Default	rate - slow (30 seconds) port-priority 32768															
Configuration Mode	Config															
History	3.1.1400															
Role	admin															
Example	<pre>switch (config)# lacp rate fast switch (config)# show lacp interfaces ethernet 1/7 Port : 1/7 ----- Port State = Down Channel Group : 1 Pseudo port-channel = Po1 LACP port-priority = 32768 LACP Rate = Slow LACP Activity : Passive LACP Timeout : Short Aggregation State : Aggregation, Defaulted,</pre> <table><thead><tr><th>Port</th><th>State</th><th>LACP Port Priority</th><th>Admin Key</th><th>Oper Key</th><th>Port Number</th><th>Port State</th></tr></thead><tbody><tr><td>1/7</td><td>Down</td><td>128</td><td>1</td><td>1</td><td>0x7</td><td>0x0</td></tr></tbody></table> <pre>switch (config)#</pre>		Port	State	LACP Port Priority	Admin Key	Oper Key	Port Number	Port State	1/7	Down	128	1	1	0x7	0x0
Port	State	LACP Port Priority	Admin Key	Oper Key	Port Number	Port State										
1/7	Down	128	1	1	0x7	0x0										
Related Commands																
Note	Configuring LACP rate (fast or slow) will configure the peer port to send (fast or slow), it does not make any affect on the local port LACP rate.															

port-channel load-balance

port-channel load-balance <method>
no port-channel load-balance <method>

Configures the port-channel load balancing distribution function method.
 The no form of the command sets the distribution function method to default.

Syntax Description	method	Possible load balance methods: • destination-ip • destination-mac • destination-port • source-destination-ip • source-destination-mac • source-destination-port • source-ip • source-mac • source-port
Default	source-destination-mac	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	
Example	<pre>switch (config)# port-channel load-balance ethernet destination-ip source-port source-mac switch (config)# show interfaces port-channel load-balance destination-ip,source-mac,source-port switch (config)#</pre>	
Related Commands		
Note	Several load balance methods can be configured (refer to the example)	

channel-group

channel-group <1-4096> [mode {on | active | passive}]

no channel-group

Assigns and configures a physical interface to a port channel.

The no form of the command removes a physical interface from the port-channel.

Syntax Description	1-4096	The port channel number.
	mode on	Static assignment the port to LAG. LACP will not be enabled on this port.
	mode active/passive	Dynamic assignment of the port to LAG. LACP will be enabled in either passive or active mode.
Default	N/A	
Configuration Mode	Config Interface Ethernet	
History	3.1.1400	
Role	admin	
Example	switch (config interface 1/7)# channel-group 1 mode active switch (config interface 1/7)# show interfaces port-channel summary Flags: D- Down P - Up in port-channel (members) I - Individual H - Hot-standby (LACP only) s - Suspended r - Module-removed U - Up (port-channel)	

	Group Port-Channel	Type Member Ports

	1 Po1(D)	LACP Eth1/7(D)
	switch (config interface 1/7)#	
Related Commands	show interfaces port-channel summary show interfaces port-channel compatibility-parameters show lacp interfaces ethernet	
Note	- Setting the mode to active/passive is possible only in LACP is enabled. - The first port in the LAG decide if the LAG will be static (“on”) or LACP (“active” , “pasive”). - All the ports in the LAG must have the same configuration, determines by the first port added to the LAG. The port with a different configuration will be rejected, for the list of dependencies refer to ‘show interfaces port-channel compatibility-parameters’	

show lacp system-identifier

show lacp system-identifier

Displays the system identifier of LACP.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin
Example	switch (config)# show lacp system-identifier 00:02:c9:5c:61:70 switch (config)#
Related Commands	show lacp interface port-channel
Note	

show lacp counters

show lacp counters

Displays the LACP PDUs counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin
Example	<pre>switch (config)# show lacp counters LACPDUs Marker Marker Response Port Sent Recv Sent Recv LACPDUs Sent Recv Sent Recv Sent Recv Illegal Unknown ----- Port-channel: 1 ----- 1/7 0 0 0 0 0 0 0 0</pre> switch (config) # switch (config)#
Related Commands	
Note	

show lacp interface ethernet

show lacp interface ethernet <inf>

Displays the LACP interface configuration and status.

Syntax Description	inf	Interface number, for example “1/1”.																			
Default	N/A																				
Configuration Mode	Any Command Mode																				
History	3.1.1400																				
Role	admin																				
Example	<pre>switch (config) # show lacp interfaces ethernet 1/4 Port : 1/4 ----- Port State = Down Channel Group : 1 Pseudo port-channel = Po1 LACP port-priority = 128 LACP Rate = Slow LACP Activity : Passive LACP Timeout : Short Aggregation State : Aggregation, Defaulted,</pre> <table><tr><th>Port</th><th>State</th><th>LACP Port Priority</th><th>Admin Key</th><th>Oper Key</th><th>Port Number</th><th>Port State</th></tr><tr><td>1/4</td><td>Down</td><td>128</td><td>1</td><td>1</td><td>0x4</td><td>0x0</td></tr></table> <pre>switch (config) #</pre>							Port	State	LACP Port Priority	Admin Key	Oper Key	Port Number	Port State	1/4	Down	128	1	1	0x4	0x0
Port	State	LACP Port Priority	Admin Key	Oper Key	Port Number	Port State															
1/4	Down	128	1	1	0x4	0x0															
Related Commands																					
Note																					

show lacp interface neighbor

show lacp interface neighbor

Displays the LACP interface neighbor status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin
Example	<pre> switch (config) # show lacp interfaces neighbor Flags: A - Device is in Active mode P - Device is in Passive mode Channel group 1 neighbors Port 1/4 ----- Partner System ID : 00:00:00:00:00:00 Flags : A LACP Partner Port Priority : 0 LACP Partner Oper Key : 0 LACP Partner Port State : 0x0 Port State Flags Decode ----- Activity : Active Aggregation State : Aggregation, Sync, Collecting, Distributing, Expired, Defaulted, switch (config) # </pre>
Related Commands	
Note	

show lacp interfaces port-channel

show lacp interfaces port-channel

Displays the LACP global parameters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin
Example	<pre>switch (config) # show lacp interfaces port-channel Port-channel Module Admin Status is enabled Port-channel System Identifier is 00:01:02:03:04:05 LACP System Priority: 32768 switch (config) #</pre>
Related Commands	
Note	

show interfaces port-channel

show interfaces port-channel {compatibility-parameters | load-balance | summary}

Displays port-channel parameters.

Syntax Description	compatibility-parameters	Displays the parameters that must be the same among the member ports of the port-channel interface.
	load-balance	Displays the type of load-balancing in use for port-channels.
	summary	Displays a summary of the port-channel interfaces.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4000	
Role	admin	
Example	<pre> switch (config) # show interfaces port-channel compatibility-parameters * Port-mode * Speed * MTU * Flow Control * Access VLAN * Allowed VLAN list * Flowcontrol & PFC * Channel-group mode * CoS parameters Static configuration on the port should be removed: * ACL port binding * Static mrouter * Static mac address switch (config) #show interfaces port-channel load-balance source-destination-mac switch (config) #show interfaces port-channel summary Flags: D- Down P - Up in port-channel (members) I - Individual H - Hot-standby (LACP only) s - Suspended r - Module-removed U - Up (port-channel) ----- Group Port- Type Member Ports Channel ----- switch (config) # </pre>	
Related Commands		
Note		

5.3 VLANs

A Virtual Local Area Network (VLAN) is an L2 segment of the network which defines a broadcast domain and is identified by a tag added to all Ethernet frames running within the domain. This tag is called a VLAN ID (VID) and can take a value of 1-4094.

Each port can have a switch mode of either:

- Access – Access port is a port connected to a host. It can accept only untagged frames, and assigns them a default configured VLAN (Port VLAN ID). On egress, traffic sent from the access port is untagged.
- Access-dcb – This mode is Mellanox specific that receives ingress untagged traffic but sends egress priority tag (VLAN ID = 0)
- Hybrid – Hybrid port is a port connected to either switches or hosts. It can receive both tagged and untagged frames and assigns untagged frames a default configured VLAN (Port VLAN ID). It receives tagged frames with VLANs of which the port is a member (these VLANs' names are allowed). On egress, traffic of allowed VLANs sent from the Hybrid port is sent tagged, while traffic sent with PVID is untagged.
- Trunk – Trunk port is a port connecting 2 switches. It accepts only tagged frames with VLANs of which the port is a member. On egress, traffic sent from the Trunk port is tagged. By default, a Trunk port is, automatically, a member on all current VLANs.

5.3.1 Configuring Access Mode and Assigning Port VLAN ID (PVID)

➤ *To configure Access mode and assign PVID to interfaces:*

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Create a VLAN. Run:

```
switch (config) # vlan 6
switch (config vlan 6) #
```

Step 4. Change back to config mode. Run:

```
switch (config vlan 6) # exit
switch (config) #
```

Step 5. Enter the interface context. Run:

```
switch (config) # interface ethernet 1/36
switch (config interface ethernet 1/36) #
```

Step 6. From within the interface context, configure the interface mode to Access. Run:

```
switch (config interface ethernet 1/36) # switchport mode access
switch (config interface ethernet 1/36) #
```

Step 7. From within the interface context, configure the Access VLAN membership. Run:

```
switch (config interface ethernet 1/36) # switchport access vlan 6
switch (config interface ethernet 1/36) #
```

Step 8. Change back to config mode. Run:

```
switch (config interface ethernet 1/36) # exit
switch (config) #
```

5.3.2 Configuring Hybrid Mode and Assigning Port VLAN ID (PVID)

➤ *To configure Hybrid mode and assign PVID to interfaces:*

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Create a VLAN. Run:

```
switch (config) # vlan 6
switch (config vlan 6) #
```

Step 4. Change back to config mode. Run:

```
switch (config vlan 6) # exit
switch (config) #
```

Step 5. Enter the interface context. Run:

```
switch (config) # interface ethernet 1/36
switch (config interface ethernet 1/36) #
```

Step 6. From within the interface context, configure the interface mode to Access. Run:

```
switch (config interface ethernet 1/36) # switchport mode hybrid
switch (config interface ethernet 1/36) #
```

Step 7. From within the interface context, configure the Access VLAN membership. Run:

```
switch (config interface ethernet 1/36) # switchport hybrid vlan 6
switch (config interface ethernet 1/36) #
```

Step 8. Change to config mode again. Run:

```
switch (config interface ethernet 1/36) # exit
switch (config) #
```

5.3.3 Configuring Trunk Mode VLAN Membership

➤ *To configure Trunk mode VLAN membership:*

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Create a VLAN. Run:

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

Step 4. Change back to config mode. Run:

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

Step 5. Enter the interface context. Run:

```
switch [standalone: master] (config) # interface ethernet 1/35
switch [standalone: master] (config interface ethernet 1/35) #
```

Step 6. From within the interface context, configure the interface mode to Trunk. Run:

```
switch [standalone: master] (config interface ethernet 1/35) # switchport mode trunk
switch [standalone: master] (config interface ethernet 1/35) #
```

5.3.4 Configuring Hybrid Mode VLAN Membership

➤ *To configure Hybrid mode VLAN membership:*

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Create a VLAN. Run:

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

Step 4. Change back to config mode. Run:

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

Step 5. Enter the interface context. Run:

```
switch (config) # interface ethernet 1/35
switch (config interface ethernet 1/35) #
```

Step 6. From within the interface context, configure the interface mode to Hybrid. Run:

```
switch (config interface ethernet 1/35) # switchport mode hybrid
switch (config interface ethernet 1/35) #
```

Step 7. From within the interface context, configure the allowed VLAN membership. Run:

```
switch (config interface ethernet 1/35) # switchport hybrid allowed-vlan add 10
switch (config interface ethernet 1/35) #
```

Step 8. Change to config mode again. Run:

```
switch (config interface ethernet 1/35) # exit
switch (config) #
```

5.3.5 Commands

vlan

vlan {<vlan-id> | <vlan-range>}
no vlan {<vlan-id> | <vlan-range>}

Creates a VLAN or range of VLANs, and enters a VLAN context.
 The no form of the command deletes the VLAN or VLAN range.

Syntax Description	vlan-id	1-4094.
	vlan-range	Any range of VLANs.
Default	VLAN 1 is enabled by default.	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	
Example	<pre>switch (config) # vlan 10 switch (config vlan 10) # show vlan</pre>	
	<pre>VLAN Name Ports ---- - 1 default Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2 ... 10 switch (config vlan 10) #</pre>	
Related Commands	<pre>show vlan switchport mode switchport [trunk hybrid] allowed-vlan</pre>	
Note	Interfaces are not added automatically to VLAN unless configured with trunk or hybrid mode with “all” option turned on.	

name

name <vlan-name>

no name

Adds VLAN name.

The no form of the command deletes the VLAN name.

Syntax Description	vlan-name	40-character long string.																								
Default	No name available.																									
Configuration Mode	Config VLAN																									
History	3.1.1400																									
Role	admin																									
Example	<pre>switch (config) # vlan 10 switch (config vlan 10) # name my-vlan-name switch (config vlan 10) # show vlan</pre> <table> <thead> <tr> <th>VLAN</th><th>Name</th><th>Ports</th></tr> </thead> <tbody> <tr> <td>1</td><td>default</td><td>Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2, Eth1/5,</td></tr> <tr> <td>15,</td><td></td><td>Eth1/6, Eth1/7, Eth1/8, Eth1/9, Eth1/10, Eth1/11, Eth1/12, Eth1/13, Eth1/14, Eth1/15,</td></tr> <tr> <td>20,</td><td></td><td>Eth1/16, Eth1/17, Eth1/18, Eth1/19, Eth1/20,</td></tr> <tr> <td>25,</td><td></td><td>Eth1/21, Eth1/22, Eth1/23, Eth1/24, Eth1/25,</td></tr> <tr> <td>30,</td><td></td><td>Eth1/26, Eth1/27, Eth1/28, Eth1/29, Eth1/30,</td></tr> <tr> <td>35,</td><td></td><td>Eth1/31, Eth1/32, Eth1/33, Eth1/34, Eth1/35,</td></tr> <tr> <td>10</td><td>my-vlan-name</td><td>Eth1/36, Po34, Po4096</td></tr> </tbody> </table>		VLAN	Name	Ports	1	default	Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2, Eth1/5,	15,		Eth1/6, Eth1/7, Eth1/8, Eth1/9, Eth1/10, Eth1/11, Eth1/12, Eth1/13, Eth1/14, Eth1/15,	20,		Eth1/16, Eth1/17, Eth1/18, Eth1/19, Eth1/20,	25,		Eth1/21, Eth1/22, Eth1/23, Eth1/24, Eth1/25,	30,		Eth1/26, Eth1/27, Eth1/28, Eth1/29, Eth1/30,	35,		Eth1/31, Eth1/32, Eth1/33, Eth1/34, Eth1/35,	10	my-vlan-name	Eth1/36, Po34, Po4096
VLAN	Name	Ports																								
1	default	Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2, Eth1/5,																								
15,		Eth1/6, Eth1/7, Eth1/8, Eth1/9, Eth1/10, Eth1/11, Eth1/12, Eth1/13, Eth1/14, Eth1/15,																								
20,		Eth1/16, Eth1/17, Eth1/18, Eth1/19, Eth1/20,																								
25,		Eth1/21, Eth1/22, Eth1/23, Eth1/24, Eth1/25,																								
30,		Eth1/26, Eth1/27, Eth1/28, Eth1/29, Eth1/30,																								
35,		Eth1/31, Eth1/32, Eth1/33, Eth1/34, Eth1/35,																								
10	my-vlan-name	Eth1/36, Po34, Po4096																								
Related Commands	<pre>show vlan switchport mode switchport [trunk hybrid] allowed-vlan</pre>																									
Note	Name can not be added to a range of VLANs.																									

show vlan

show vlan [id <vlan-id>]

Displays the VLAN table.

Syntax Description	vlan-id	1-4094.									
Default	N/A										
Configuration Mode	Any Command Mode										
History	3.1.1400										
Role	admin										
Example	<pre>switch (config vlan 10) # show vlan</pre> <table> <thead> <tr> <th>VLAN</th><th>Name</th><th>Ports</th></tr> </thead> <tbody> <tr> <td>1</td><td>default</td><td>Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2 ...</td></tr> <tr> <td>10</td><td>my-vlan-name</td><td></td></tr> </tbody> </table>		VLAN	Name	Ports	1	default	Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2 ...	10	my-vlan-name	
VLAN	Name	Ports									
1	default	Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2 ...									
10	my-vlan-name										
Related Commands	<pre>show vlan switchport mode switchport [trunk hybrid] allowed-vlan vlan</pre>										
Note											

switchport mode

switchport mode {access | trunk | hybrid | access-dcb}

no switchport mode

Sets the switch port mode.

The no form of the command sets the switch port mode to access.

Syntax Description	access	Un-tagged port. 802.1q tagged traffic will be filtered. egress traffic is un-tagged.																																								
	trunk	802.1q tagged port, un-tagged traffic will be filtered.																																								
	hybrid	Both 802.1q tagged and un-tagged traffic is allowed on the port.																																								
	access-dcb	Un-tagged port, egress traffic is priority tagged.																																								
Default	access.																																									
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel																																									
History	3.1.1400																																									
	3.3.4500	Added MLAG port-channel configuration mode																																								
Role	admin																																									
Example	<pre>switch (config) # interface ethernet 1/7 switch (config interface ethernet 1/7) # switchport mode access switch (config interface ethernet 1/7) # show interfaces switchport</pre> <table><thead><tr><th>Interface</th><th>Mode</th><th>Access vlan</th><th>Allowed vlans</th></tr></thead><tbody><tr><td>Eth1/2</td><td>access</td><td>1</td><td></td></tr><tr><td>Eth1/3</td><td>access</td><td>1</td><td></td></tr><tr><td>Eth1/4/1</td><td>access</td><td>1</td><td></td></tr><tr><td>Eth1/4/2</td><td>access</td><td>1</td><td></td></tr><tr><td>Eth1/5</td><td>access</td><td>1</td><td></td></tr><tr><td>Eth1/6</td><td>access</td><td>1</td><td></td></tr><tr><td>....</td><td></td><td></td><td></td></tr><tr><td>Po34</td><td>access</td><td>1</td><td></td></tr><tr><td>Po4096</td><td>access</td><td>1</td><td></td></tr></tbody></table> <pre>switch (config interface ethernet 1/7) #</pre>		Interface	Mode	Access vlan	Allowed vlans	Eth1/2	access	1		Eth1/3	access	1		Eth1/4/1	access	1		Eth1/4/2	access	1		Eth1/5	access	1		Eth1/6	access	1						Po34	access	1		Po4096	access	1	
Interface	Mode	Access vlan	Allowed vlans																																							
Eth1/2	access	1																																								
Eth1/3	access	1																																								
Eth1/4/1	access	1																																								
Eth1/4/2	access	1																																								
Eth1/5	access	1																																								
Eth1/6	access	1																																								
....																																										
Po34	access	1																																								
Po4096	access	1																																								
Related Commands	show vlan show interfaces switchport switchport access vlan switchport [trunk hybrid] allowed-vlan vlan																																									
Note																																										

switchport access

switchport access vlan <vlan-id>

no switchport access vlan

Sets the port access VLAN.

The no form of the command sets the port access VLAN to 1.

Syntax Description	vlan-id	1-4094.																																								
Default	1																																									
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel																																									
History	3.1.1400	Initial version																																								
	3.2.0500	Format change (removed hybrid and access-dcb options). Previous command format was: “switchport {hybrid access-dcb access} vlan <vlan-id>”																																								
	3.3.4500	Added MLAG port-channel configuration mode																																								
Role	admin																																									
Example	<pre>switch (config) # interface ethernet 1/7 switch (config interface ethernet 1/7) # switchport access vlan 10 switch (config interface ethernet 1/7) # show interfaces switchport</pre> <table><thead><tr><th>Interface</th><th>Mode</th><th>Access vlan</th><th>Allowed vlans</th></tr></thead><tbody><tr><td>Eth1/2</td><td>access</td><td>1</td><td></td></tr><tr><td>Eth1/3</td><td>access</td><td>1</td><td></td></tr><tr><td>Eth1/4/1</td><td>access</td><td>1</td><td></td></tr><tr><td>Eth1/4/2</td><td>access</td><td>1</td><td></td></tr><tr><td>Eth1/5</td><td>access</td><td>1</td><td></td></tr><tr><td>Eth1/6</td><td>access</td><td>1</td><td></td></tr><tr><td>Eth1/7</td><td>access</td><td>10</td><td></td></tr><tr><td>....</td><td></td><td></td><td></td></tr><tr><td>Po4096</td><td>access</td><td>1</td><td></td></tr></tbody></table> <pre>switch (config interface ethernet 1/7) #</pre>		Interface	Mode	Access vlan	Allowed vlans	Eth1/2	access	1		Eth1/3	access	1		Eth1/4/1	access	1		Eth1/4/2	access	1		Eth1/5	access	1		Eth1/6	access	1		Eth1/7	access	10						Po4096	access	1	
Interface	Mode	Access vlan	Allowed vlans																																							
Eth1/2	access	1																																								
Eth1/3	access	1																																								
Eth1/4/1	access	1																																								
Eth1/4/2	access	1																																								
Eth1/5	access	1																																								
Eth1/6	access	1																																								
Eth1/7	access	10																																								
....																																										
Po4096	access	1																																								
Related Commands	show vlan show interfaces switchport switchport mode switchport [trunk hybrid] allowed-vlan vlan																																									
Note	This command is not applicable for interfaces with port mode trunk. only one option (“access”, “access-dcb” or “hybrid”) is applicable to configure on the port, depends on the switchport mode of the port.																																									

switchport {hybrid, trunk} allowed-vlan

switchport {hybrid, trunk} allowed-vlan {<vlan> | add <vlan> | remove <vlan> all | except <vlan> | none}

Sets the port allowed VLANs.

Syntax Description	vlan	VLAN ID (1-4094) or VLAN range.
	add	Add VLAN or range of VLANs.
	remove	Remove VLANs or range of VLANs.
	all	Add all VLANs in available in the VLAN table. New vlans that will be added to the vlan table will be added automatically.
	except	Add all VLANs expect this VLAN or VLAN range.
	none	Remove all VLANs.
Default	N/A	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
History	3.1.1400	
Role	admin	
Example	<pre> switch (config) # interface ethernet 1/7 switch (config interface ethernet 1/7) # switchport hybrid allowed-vlan all switch (config interface ethernet 1/7) #show interfaces switchport Interface Mode Access vlan Allowed vlans ----- ----- ----- ----- Eth1/2 access 1 Eth1/3 access 1 Eth1/4/1 access 1 Eth1/4/2 access 1 Eth1/5 access 1 Eth1/6 access 1 Eth1/7 hybrid 1 1, 10 Po34 access 1 Po4096 access 1 switch (config interface ethernet 1/7) # </pre>	
Related Commands	<pre> show vlan show interfaces switchport switchport access vlan switchport mode vlan </pre>	
Note	This command is not applicable for interfaces with port mode access or access-dcb.	

show interface switchport

show interface switchport

Displays all interface switch port configurations.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin
Example	<pre>switch (config) #show interfaces switchport Interface Mode Access vlan Allowed vlans ----- ----- ----- ----- Eth1/2 access 1 Eth1/3 access 1 Eth1/4/1 access 1 Eth1/4/2 access 1 Eth1/5 access 1 Eth1/6 access 1 Eth1/7 hybrid 1 1, 10 Po34 access 1 Po4096 access 1 switch (config)#</pre>
Related Commands	<pre>show vlan switchport access vlan switchport mode vlan</pre>
Note	

5.4 MAC Address Table

5.4.1 Configuring Unicast Static MAC Address

You can configure static MAC addresses for unicast traffic. This feature improves security and reduces unknown unicast flooding.

➤ *To configure Unicast Static MAC address:*

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Run the command `mac-address-table static unicast <destination mac address> vlan <vlan identifier(1-4094)> interface ethernet <slot>/ <port>`.

```
switch (config) # mac-address-table static unicast 00:11:22:33:44:55 vlan 1 interface  
ethernet 0/1
```

5.4.2 Commands

mac-address-table aging-time

mac-address-table aging-time <age>

no mac-address-table aging-time

Sets the maximum age of a dynamically learnt entry in the MAC address table.
The no form of the command resets the aging time of the MAC address table to its default.

Syntax Description	age	10-1000000 seconds.
Default	300	
Configuration Mode	Config	
History	3.1.0600	
Role	admin	
Example	<pre>switch (config) # mac-address-table aging-time 50 switch (config) # show mac-address-table aging-time Mac Address Aging Time: 50 switch (config) #</pre>	
Related Commands	<pre>show mac-address-table show mac-address-table aging time</pre>	
Note		

mac-address-table static

mac-address-table static <mac address> **vlan** <vlan> **interface** <if-type> <if-number>

no mac-address-table static <mac address> **vlan** <vlan> **interface** <if-type> <if-number>

Configures a static MAC address in the forwarding database.

The no form of the command deletes a configured static MAC address from the forwarding database.

Syntax Description	mac address	Destination MAC address.	
	vlan	VLAN ID or VLAN range.	
	if-type	Ethernet or port-channel interface type.	
	if-number	The interface number (i.e. 1/1, 3).	
Default	No static MAC addresses available in default.		
Configuration Mode	Config		
History	3.1.0600		
Role	admin		
Example	<pre>switch (config) # mac-address-table static aa:aa:aa:aa:aa:aa vlan 1 interface ethernet 1/7 switch (config) # show mac-address-table Switch ethernet-default Vlan Mac Address Type Interface ---- - 1 aa:aa:aa:aa:aa:aa static Eth1/7 Number of unicast: 1 Number of multicast: 0 switch (config) #</pre>		
Related Commands	<pre>show mac-address-table mac-address-table aging time</pre>		
Note	The no form of the command will not clear a dynamic MAC address. Dynamic MAC addresses are cleared using the “clear mac-address-table dynamic” command.		

clear mac-address-table dynamic

clear mac-address-table dynamic

Clear the dynamic entries in the MAC address table.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0600
Role	admin
Example	switch (config) # clear mac-address-table dynamic switch (config) #
Related Commands	mac-address-table aging-time mac-address-table static show mac-address-table
Note	This command does not clear the MAC addresses learned on the mgmt0 port. Static entries are deleted using the “no mac-address-table static” command.

show mac-address-table

show mac-address-table [**address** <mac-address> | **interface ethernet** <if-number> | **vlan** [<vlan> | **range** <range>] | **unicast** | **multicast**]

Displays the static and dynamic unicast and multicast MAC addresses for the switch. Various of filter options available.

Syntax Description	mac-address	Filter the table to a specific MAC address.
	if-number	Filter the table to a specific interface.
	vlan	Filter the table to a specific VLAN number (1-4094).
	range	Filter the table to a range of VLANs.
	unicast	Filter the table to a unicast addresses only.
	multicast	Filter the table to a multicast addresses only.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0600	
	3.3.4500	Updated Example
Role	admin	
Example	switch (config) # show mac-address-table	
	<pre>Switch ethernet-default Vlan Mac Address Type Interface ---- - 1 00:00:00:00:00:01 Static Po5 1 00:00:3D:5C:FE:16 Dynamic Eth1/1 1 00:00:3D:5D:FE:1B Dynamic Eth1/2 Number of unicast: 2 Number of multicast: 0 switch (config) #</pre>	
Related Commands	mac-address-table static clear mac-address-table	
Note		

show mac-address-table aging-time

show mac-address-table aging-time

Displays the MAC address table aging time.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.0600
Role	admin
Example	<pre>switch (config) # mac-address-table aging-time 300 switch (config) # show mac-address-table aging-time</pre> Mac Address Aging Time: 300 <pre>switch (config) #</pre>
Related Commands	<pre>mac-address-table aging-time mac-address-table static clear mac-address-table</pre>
Note	MAC addresses learned on the mgmt0 is not shown by this command.

5.5 Spanning Tree

The operation of Rapid Spanning Tree Protocol (RSTP) provides for rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN. The RSTP component avoids this delay by calculating an alternate root port, and immediately switching over to the alternate port if the root port becomes unavailable. Thus, using RSTP, the switch immediately brings the alternate port to forwarding state, without the delays caused by the listening and learning states. The RSTP component conforms to IEEE standard 802.1D 2004.

RSTP enhancements is a set of functions added to increase the volume of RSTP in Mellanox switches. It adds a set of capabilities related to the behavior of ports in different segments of the network. For example: the required behavior of a port connected to a non-switch entity, such as host, is to converge quickly, while the required behavior of a port connected to a switch entity is to converge based on the RSTP parameters.

Additionally, it adds security issues on a port and switch basis, allowing the operator to determine the state and role of a port or the entire switch should an abnormal event occur. For example: If a port is configured to be root-guard, the operator will not allow it to become a root-port under any circumstances, regardless of any BPDU that will have been received on the port.

5.5.1 Port Priority and Cost

When two ports on a switch are part of a loop, the STP port priority and port path cost configuration determine which port on the switch is put in the forwarding state and which port is put in the blocking state.

To configure port priority use the following command:

```
switch (config interface ethernet <inf>)# spanning-tree port-priority <0-240>
```

To configure port path cost use the following command:

```
switch (config interface ethernet <inf>)# spanning-tree cost <1-2000000000>
```

5.5.2 Port Type

Port type has the following configuration options:

- **edge** – is not assumed to be converged by the RSTP learning/forwarding mechanism. It converges to forwarding quickly.



It is recommended to configure the port type for all ports connected to hosts as edge ports.

- **normal** – is assumed to be connected to a switch, thus it tries to be converged by the RSTP learning/forwarding. However, if it does not receive any BPDUs, it is operationally moved to be edge.
- **network** – is assumed to be connected to a switch. If it does not receive any BPDUs, it is moved to discarding state.

Each of these configuration options is mutually exclusive.

Port type is configured using the command `spanning-tree port type`. It may be applied globally on the switch (Config) level, which configures all switch interfaces. Another option is to configure ports individually by entering the interface's configuration mode.

- Global configuration:

```
switch (config)# spanning-tree port type {edge , normal , network} default
```

- Interface configuration:

```
switch (config interface ethernet <inf>)# spanning-tree port type {edge , normal, network}
```

5.5.3 BPDU Filter

Using BPDU filter prevents the CPU from sending/receiving BPDUs on specific ports.

BPDU filtering is configured per interface. When configured, the port does not send any BPDUs and drops all BPDUs that it receives. To configure BPDU filter, use the following command:

```
switch (config interface ethernet <inf>)# spanning-tree bpdupfilter {enable , disable}
```



Configuring BPDU filtering on a port connected to a switch can cause bridging loops because the port filters any BPDU it receives and goes to forwarding state.

5.5.4 Loop Guard

Loop guard is a feature that prevents loops in the network.

When a blocking port in a redundant topology transitions to the forwarding state (accidentally), an STP loop occurs. This happens when BPDUs are no longer received by one of the ports in a physically redundant topology.

Loop guard is useful in switched networks where devices are connected point-to-point. A designated bridge cannot disappear unless it sends an inferior BPDU or brings the link down on a point-to-point connection.



The loop guard configuration is only allowed on “network” port type.

If loop guard is enabled and the port does not receive BPDUs, the port is put into an inconsistent state (blocking) until the port starts to receive BPDUs again. A port in the inconsistent state does not transmit BPDUs. If BPDUs are received again, loop guard alters its inconsistent state condition. STP converges to a stable topology without the failed link or bridge after loop guard isolates the failure.

Disabling loop guard moves all loop-inconsistent ports to listening state.

To configure loop guard use the following command:

```
switch (config interface ethernet <inf>)# spanning-tree guard loop
```

5.5.5 Root Guard

Configuring root guard on a port prevents that port from becoming a root port. A port put in root-inconsistent (blocked) state if an STP convergence is triggered by a BPDU that makes that port a root port. The port is unblocked after the port stops sending BPDUs.

To configure loop guard use the following command:

```
switch (config interface ethernet <inf>)# spanning-tree guard root
```

5.5.6 MSTP

Spanning Tree Protocol (STP) is a mandatory protocol to run on L2 Ethernet networks to eliminate network loops and the resulting broadcast storm caused by these loops. Multiple STP (MSTP) enables the virtualization of the L2 domain into several VLANs, each governed by a separate instance of a spanning tree which results in a network with higher utilization of physical links while still keeping the loop free topology on a logical level.

Up to 64 MSTP instances can be defined in the switch. Up to 64 VLANs can be mapped to a single MSTP instance. MSTP instance 0 (the default instance) may have all possible VLANs (1-4094) mapped to it.

For MSTP network design over Mellanox L2 VMS, please refer to [Mellanox Virtual Modular Switch Reference Guide](#).

5.5.7 Commands

spanning-tree

spanning-tree
no spanning-tree

Globally enables the spanning tree feature.
The no form disables the spanning tree feature.

Syntax Description	N/A
Default	Spanning tree is enabled.
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	switch (config) # no spanning-tree switch (config) #
Related Commands	show spanning-tree
Note	

spanning-tree (timers)

spanning-tree [forward-time <time in secs> | hello-time <time in secs> | max-age <time in secs>]

no spanning-tree [forward-time | hello-time | max-age]

Sets the spanning tree timers.

The no form of the command sets the timer to default.

Syntax Description	forward-time	Controls how fast a port changes its spanning tree state from Blocking state to Forwarding state. Parameter range: 4-30 seconds.
	hello-time	Determines how often the switch broadcasts its hello message to other switches when it is the root of the spanning tree. Parameter range: 1-2 seconds.
	max-age	Sets the maximum age allowed for the Spanning Tree Protocol information learnt from the network on any port before it is discarded. Parameter range: 6-40 seconds.
Default	forward-time: 15 seconds hello-time: 2 seconds max-age: 20 seconds	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	switch (config) # spanning-tree forward-time switch (config) #	
Related Commands	show spanning-tree	
Note	The following formula applies on the spanning tree timers: $2 * (\text{ForwardTime} - 1) \geq \text{MaxAgeTime} \geq 2 * (\text{Hello Time} + 1)$	

spanning-tree port type (default global)

spanning-tree port type <port-type> default
no spanning-tree port type default

Configures all switch interfaces as edge/network/normal ports. These ports can be connected to any type of device.

The no form of the command disables the spanning tree operation.

Syntax Description	port-type	• Edge - Assumes all ports are connected to hosts/servers. • Network - Assumes all ports are connected to switches and bridges. • Normal - the port type (Edge or Network) determines according to the spanning tree operational mode.
Default	Normal	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # spanning-tree port type edge default switch (config) #</pre>	
Related Commands	show spanning-tree	
Note		

spanning-tree priority

spanning-tree priority <bridge-priority>

no spanning-tree priority

Sets the spanning tree bridge priority.

The no form of the command sets the bridge priority to default.

Syntax Description	bridge-priority	Sets the bridge priority for the spanning tree. Its value must be in steps of 4096, starting from 0. Only the following values are applicable: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.
Default	32786	
Configuration Mode	Config	
History	3.1.0000	
Role	admin	
Example	switch (config) # spanning-tree priority 4096 switch (config) #	
Related Commands	show spanning-tree	
Note		

spanning-tree port-priority

spanning-tree port-priority <priority>

no spanning-tree port-priority

Configures the spanning-tree interface priority.

The no form of the command returns configuration to its default.

Syntax Description	priority	Spanning tree interface priority. The possible values are: 0, 16, 32,48, 64, 80, 96, 112, 128,144, 160, 176, 192, 208, 224, 240.
Default	128	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
History	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	
Example	switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # spanning-tree port-priority 16 switch (config interface ethernet 1/1) #	
Related Commands	show spanning-tree	
Note		

spanning-tree cost

spanning-tree cost <port cost>

no spanning-tree cost

Configures the interface cost of the spanning tree.

The no form of the command returns configuration to its default.

Syntax Description	port cost	Sets the spanning tree cost of an interface. Value range is 0-2000000000.
Default	The default cost is derived from the speed. 1Gbps 20000 10Gbps 2000 40Gbps 500 56Gbps 357	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
History	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	
Example	switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # spanning-tree cost 1000 switch (config interface ethernet 1/1) #	
Related Commands	show spanning-tree	
Note	- LAG default cost is calculated by dividing the port speed by the number of active links in UP state. For example: if there were 4 links in the LAG out of which only two are in UP state, assuming the port speed is 10Gbps, the LAG cost will be $2000/2 = 1000$. - When configuring the cost for a LAG, the cost will be fixed to this configuration, no matter what the number of active links (UIP state) in the LAG is - Unstable network may cause the LAG cost to change dynamically assuming the cost parameter is not configured for anything else other than default	

spanning-tree port type

spanning-tree port type <port type>

no spanning-tree port type

Configures spanning-tree port type

The no form of the command returns configuration to default.

Syntax Description	port type	Sets the spanning-tree port type. The port type parameter has four options: • Default (globally defined) • Edge • Normal • Network In case there is no change of this parameter, the configuration will be taken from the global default port type.
Default	Globally defined by the command “spanning-tree port type <port-type> default”	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
History	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	
Example	<pre>switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # spanning-tree port type edge switch (config interface ethernet 1/1) #</pre>	
Related Commands	show spanning-tree	
Note		

spanning-tree guard

spanning-tree guard {loop | root}
no spanning-tree guard {loop | root}

Configures spanning-tree guard.
 The no form of the command returns configuration to default.

Syntax Description	loop	Enables loop-guard on the interface. If the loop-guard is enabled, upon a situation where the interface fails to receive BPDUs the switch will not egress data traffic on this interface.
	root	Enables root-guard on the interface. If root-guard is enabled on the interface, the interface will never be selected as root port.
Default	loop-guard and loop-guard are disabled.	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
History	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	
Example	switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # spanning-tree guard root switch (config interface ethernet 1/1) #	
Related Commands	show spanning-tree	
Note		

spanning-tree bpdudfilter

spanning tree bpdudfilter {disable | enable}

no spanning tree bpdudfilter

Configures spanning-tree BPDU filter on the interface. The interface will ignore any BPDU that it receives and will not send PDBUs, The STP state on the port will move to the forwarding state.

The no form of the command returns the configuration to default.

Syntax Description	disable	Disables the BPDU filter on this port.
	enable	Enables the BPDU filter on this port.
Default	BPDU filter is disabled.	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
History	3.1.0000	
Role	admin	
Example	switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # spanning-tree bpdudfilter enable switch (config interface ethernet 1/1) #	
Related Commands	show spanning-tree	
Note	This command can be used when the switch is connected to hosts.	

clear spanning-tree counters

clear spanning-tree counters

Clears the spanning-tree counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.1.0000
Role	admin
Example	switch (config) # clear panning-tree counters switch (config) #
Related Commands	show spanning tree
Note	

show spanning-tree

show spanning-tree [detail | interface <type> <number>]

Displays spanning tree information.

Syntax Description	detail	Displays detailed spanning-tree configuration and statistics.
	interface <type> <number>	Displays the running state for a specific interface. Options for “type”: ethernet or port-channel. Options for “number”: <slot/port> or <number>.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config) # show spanning-tree Switch ethernet-default Spanning tree protocol is enabled rstp Spanning tree force version:2 Root ID Priority 32768 Address 00:02:c9:5c:61:70 This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32768 Address 00:02:c9:5c:61:70 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Interface Role Sts Cost Prio Type ---- - switch (config) #</pre>	
Related Commands	<pre>clear spanning-tree counters spanning-tree</pre>	
Note		

spanning-tree mst max-hops

spanning-tree mst max-hops <max-hops>

no spanning-tree mst max-hops

Specifies the max hop value inserts into BPDUs that sent out as the root bridge.
The no form of the command sets the parameter to its default value.

Syntax Description	max-hops	Max hop value. The range is 6-40.
Default	20	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	switch (config)# spanning-tree mst max-hops 20 switch (config)#	
Related Commands		
Note	The max hop setting determines the number of bridges in an MST region that a BPDU can traverse before it is discarded.	

spanning-tree mst priority

spanning-tree mst <mst-instance> priority <priority>

no spanning-tree mst <mst-instance> priority

Configures the specified instance's priority number.

The no form of the command sets the parameter to its default value.

Syntax Description	mst-instance	MST instance. Range is 1-64.
	priority	MST instance port priority. Possible values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
Default	32768	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	switch (config)# spanning-tree mst 1 priority 32768 switch (config)#	
Related Commands		
Note	The bridge priority is the four most significant digits of the bridge ID, which is used by spanning tree algorithms to select the root bridge and choose among redundant links. Bridge ID numbers range from 0-65535 (16 bits); bridges with smaller bridge IDs are elected over other bridges.	

spanning-tree mst vlan

spanning-tree mst <mst-instance> vlan <vlan-range>
no spanning-tree mst <mst-instance> vlan <vlan-range>

Maps a VLAN or a range of VLANs into an MSTP instance.
 The no form of the command unmaps a VLAN or a range of VLANs from MSTP instances.

Syntax Description	mst-instance	MST instance. Range is 1-64.
	vlan <vlan-range>	A single VLAN or a a range of VLANs. The format is <vlan> or <from-vlan>-<to-vlan>.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	switch (config)# spanning-tree mst 1 vlan 10-20 switch (config)#	
Related Commands		
Note		

spanning-tree mst revision

spanning-tree mst revision <number>

no spanning-tree mst revision

Configures the MSTP revision number.

The no form of the command sets the parameter to its default value.

Syntax Description	number	The MST revision number. Range is 0-65535.
Default	0	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	<pre>switch (config)# spanning-tree mst revision 1 switch (config)#</pre>	
Related Commands		
Note	The revision number is one of three parameters, along with the MST name and VLAN-to-instance map, that identify the switch's MST region.	

spanning-tree mst name

spanning-tree mst name <name>

no spanning-tree mst name

Configures the MSTP name.

The no form of the command sets the parameter to its default value.

Syntax Description	name	MST name: Up to 32 characters.
Default	N/A	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	<pre>switch (config)# spanning-tree mst name my-mst switch (config)#</pre>	
Related Commands		
Note	The name is one of three parameters, along with the MST revision number and VLAN-to-instance map, that identifies the switch's MST region.	

spanning-tree mst root

spanning-tree mst <mst-instance> root <role>

no spanning-tree mst <mst-instance> root

Changes the bridge priority for the specified MST instance to the following values:

- Primary – 8192
- Secondary – 16384

The no form of the command sets the parameter to its default value.

Syntax Description	mst-instance	MSTP instance. Possible range is 1-64.
	role	Values: “primary” or “secondary”.
Default	primary	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	switch (config)# spanning-tree mst name my-mst switch (config)#	
Related Commands		
Note	The root command is a way to automate a system configuration while ‘playing’ with the priority field. The priority field granularity may be too explicit for some users in case you wish to have 2 levels of priority (primary and secondary). So by default all the switches get the same priority and while using the root option you can get the role of master and backup by setting the priority field to a predefined value.	

spanning-tree mode

spanning-tree mode {rst | mst}

no spanning-tree mode

Changes the spanning tree mode.

The no form of the command sets the parameter to its default value.

Syntax Description	mst	Multiple spanning tree.
	rst	Rapid spanning tree.
Default	rst	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	switch (config)# spanning-tree mode mst switch (config)#	
Related Commands		
Note		

spanning-tree mst port-priority

spanning-tree mst {mst-instance} port-priority <priority>
no spanning-tree mode

Changes the spanning tree mode.
 The no form of the command sets the parameter to its default value.

Syntax Description	mst-instance	MST instance. Range is 1-64.
	priority	MST instance port priority. Valid values are: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 and 240.
Default	rst	
Configuration Mode	Config Interface Port Channel	
History	3.3.4150	
Role	admin	
Example	<pre>switch (config interface ethernet 1/1)# spanning-tree mst 1 port- priority 32768 switch (config interface port-channel 1)# spanning-tree mst 1 port- priority 32768 switch (config)#</pre>	
Related Commands		
Note		

spanning-tree mst cost

spanning-tree mst {mst-instance} cost <cost-value>
no spanning-tree mode

Configures the cost per MSTP instance.
 The no form of the command sets the parameter to its default value.

Syntax Description	mst-instance	MST instance. Range is 1-64.
	cost-value	MST instance port cost. Range is 0-2000000000.
Default	2000 for 10Gb/s, 500 for 40Gb/s, 20000 for 1Gb/s, 357 for 56Gb/s	
Configuration Mode	Config Interface Port Channel	
History	3.3.4150	
Role	admin	
Example	switch (config interface ethernet 1/1)# spanning-tree mst 1 cost 4000 switch (config interface port-channel 1)# spanning-tree mst 1 cost 4000 switch (config)#	
Related Commands		
Note		

show spanning-tree

show spanning-tree [**detail** | **interface** {**ethernet** <slot>/<port> | **port-channel** <port-channel>} | **mst** [<instance> **interface** {**ethernet** <slot>/<port> | **port-channel** <port-channel>} | **details** | **interface** {**ethernet** <slot>/<port> | **port-channel** <port-channel>}} | **root**]

Displays spanning-tree information for a switch.

Syntax Description	detail	Displays detailed spanning-tree information on a switch.
	interface {ethernet <slot>/<port> port-channel <port-channel>}	Displays running state for the specified interface.
	mst [<instance> interface {ethernet <slot>/<port> port-channel <port-channel>} details interface {ethernet <slot>/<port> port-channel <port-channel>}	Displays basic multi-spanning-tree information of a specific switch or a specific interface.
	root	Displays root multi-spanning-tree information of a specific switch.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4150	
Role	admin	
Example	<pre>switch (config) # show spanning-tree root Instance Priority MAC addr Root Cost Hello Time Max Age FWD Dly Root Port ----- MST0 32768 00:02:c9:71:ed:40 500 2 20 15 Eth1/20 MST1 32768 00:02:c9:71:f0:c0 0 2 20 15 - MST2 0 00:02:c9:71:f0:c0 0 2 20 15 - MST3 32768 00:02:c9:71:f0:c0 0 2 20 15 - switch (config) #</pre>	
Related Commands		
Note		

5.6 OpenFlow

MLNX-OS supports OpenFlow 1.0. OpenFlow is a network protocol that facilitates direct communication between network systems via Ethernet. Software Defined Networks (SDN) allows a centralist management of network equipment. OpenFlow allows the SDN controller to manage SDN equipment. The OpenFlow protocol allows communication between the OpenFlow controller and OpenFlow agent.

OpenFlow is useful to manage switches and allow applications running on the OpenFlow controller to have access to the switch's datapath and provide functionality such as flow steering, security enhancement, traffic monitoring and more.

The OpenFlow controller communicates with the OpenFlow switch over secured channel using OpenFlow protocol.

An OpenFlow switch contains a flow table which contains flows inserted by the OpenFlow controller. And the OpenFlow switch performs packet lookup and forwarding according to those rules.

Mellanox OpenFlow switch implementation is based on the hybrid model, allowing the coexistence of an OpenFlow pipeline and a normal pipeline. In this model, a packet is forwarded according to OpenFlow configuration, if such configuration is matched with the packet parameters. Otherwise, the packet is handled by the normal (regular forwarding/routing) pipeline.

The OpenFlow specification defines:

“OpenFlow-hybrid switches support both OpenFlow operation and normal Ethernet switching operation, i.e. traditional L2 Ethernet switching, VLAN isolation, L3 routing (IPv4 routing, IPv6 routing...), ACL and QoS processing. Those switches must provide a classification mechanism outside of OpenFlow that routes traffic to either the OpenFlow pipeline or the normal pipeline. For example, a switch may use the VLAN tag or input port of the packet to decide whether to process the packet using one pipeline or the other, or it may direct all packets to the OpenFlow pipeline.”

Utilizing the built-in capabilities of the hybrid switch/router is the main benefit of the hybrid mode. It increases network performance and efficiency – faster processing of new flows as well as lower load on the controllers. The hybrid switch processes non-OpenFlow data through its local management plane and achieve better efficiency and use of resources, compared to the pure OpenFlow switch.

5.6.1 Flow Table

The flow table contains flows which are used to perform packet lookup, modification and forwarding. Each flow has a 12 tuple key. The key is used in order to classify a packet into a certain flow. The key contains the flowing fields: ingress port, source MAC, destination MAC, EtherType, VLAN ID, PCP, source IP, destination IP, IP protocol, IP ToS bits, TCP/UDP source port and TCP/UDP destination port.

The flow key can have a specific value for each field or wildcard which signals to the switch to ignore this part of the key.

Each packet passes through the flow table once a match is found; the switch performs the actions configured to the specific flow by the OpenFlow controller.

Upkeeping a flow table enables the switch to forward incoming traffic with a simple lookup on its flow table entries. OpenFlow switches perform a check for matching entries on, or ignore using a wildcard, specific fields of the ingress traffic. If the entry exists, the switch performs the action associated with that flow entry. Packets without a flow entry match are forwarded according to the normal pipeline (hybrid switch).

Every flow entry contains one of the following parameters:

1. Header fields for matching purposes with each entry containing a specific value or a wildcard which could match all entries.
2. Matching packet counters which are useful for statistical purposes, in order to keep track of the number of packets.
3. Actions which specify the manner in which to handle the packets of a flow which can be any of the following:
 - a. Forwarding the packet
 - b. Dropping the packet
 - c. Forwarding the packet to the OpenFlow controller
 - d. Modifying the VLAN, VLAN priority (PCP), and/or stripping the VLAN header



The flow table supports up to 1000 flows.

5.6.2 Configuring OpenFlow

➤ *To run OpenFlow on a switch:*

Step 1. Unlock the OpenFlow CLI commands. Run:

```
switch (config) # protocol openflow
```

Step 2. Configure interfaces to be managed by OpenFlow. Run:

```
switch (config) # interface ethernet 1/1-1/4 openflow mode hybrid
```

Step 3. Configure the OpenFlow controller IP and TCP port. Run:

```
switch (config) # openflow controller-ip 10.209.0.205 tcp-port 6633
```

Step 4. (Optional) Verify the OpenFlow configuration. Run:

```
switch (config) # show openflow
OpenFlow version: OF VERSION 1.0
Table size: 1000, 0 in use
Active controller ip: 10.209.0.205 port: 6633
Connection status: HANDSHAKE_COMPLETE (CONNECTED)
Forward-to-controller: ospf lldp arp-unicast arp-broadcast (all)
Enabled ports: Eth1/1      Eth1/2      Eth1/3      Eth1/4
switch (config) #
```



To be able to configure the switch using the controller, you should see the following line in the output:

Connection status must be: HANDSHAKE_COMPLETE (CONNECTED).

5.6.3 Commands

protocol openflow

protocol openflow
no protocol openflow

Unhides the OpenFlow commands.
 The no form of the command hides the OpenFlow commands.

Syntax Description	N/A
Default	no protocol openflow
Configuration Mode	Config
History	3.3.4200
Role	admin
Example	switch (config) # protocol openflow switch (config) #
Related Commands	
Note	

openflow description

openflow description <string>

Sets the OpenFlow description.

Syntax Description	string	Free string.
Default	N/A	
Configuration Mode	Config	
History	3.3.4302	
Role	admin	
Example	<pre> switch (config) # openflow description OF-switch-104 switch (config) # show openflow detail OpenFlow version: OF VERSION 1.0 Table size: 1000, 0 in use Active controller ip: 10.209.1.39 port: 6633 Connection status: HANDSHAKE_COMPLETE (CONNECTED) Forward-to-controller: ospf lldp arp-unicast arp-broadcast (all) Enabled ports: Eth1/10 Eth1/11 Eth1/13 Eth1/19 Echo period: 10 sec Keep alive period: 30 sec Messages in (last session): 86290 Messages out (last session): 47984 Disconnect count: 0 Openflow description: OF-switch-104 Datapath ID: 00:00:00:02:c9:a8:e3:50 Not supporting buffering Not supporting emergency flows Not supporting port statistics Not supporting IP reassemble Supporting spanning tree Not supporting queue statistics switch (config) # </pre>	
Related Commands		
Note		

openflow mode hybrid

openflow mode hybrid
no openflow mode

Enables OpenFlow on the port.
The no form of the command returns the port to its default state.

Syntax Description	N/A
Default	no openflow mode
Configuration Mode	Config Interface Ethernet
History	3.3.4200
Role	admin
Example	switch (config interface ethernet 1/1)# openflow mode hybrid switch (config interface ethernet 1/1)#
Related Commands	
Note	

controller-ip

controller-ip <ip-address> [tcp-port <port-number>]

no controller-ip <ip-address> tcp-port

Sets the OpenFlow controller's IP & TCP port.

The no form of the command sets the parameter to its default.

Syntax Description	ip-address	The IPv4 address of the OpenFlow controller.
	tcp-port <port-number>	Sets the TCP port number of the OpenFlow controller.
Default	0.0.0.0; TCP port 6633	
Configuration Mode	Config OpenFlow	
History	3.3.4200	
Role	admin	
Example	<pre>switch (config openflow) # controller-ip 10.10.10.10 tcp-port 6633 switch (config openflow) #</pre>	
Related Commands		
Note		

datapath-id

datapath-id <value>

no datapath-id

Sets a specific identifier for the switch with which the controller is communicating. The no form of the command resets the parameter to its default value.

Syntax Description	value	The most significant 16 bits of the agent data-path ID. Range is 0x0000-0xFFFF in hexa.
Default	0x0000	
Configuration Mode	Config OpenFlow	
History	3.3.4200	
Role	admin	
Example	<pre>switch (config openflow) # datapath-id 0x1234 switch (config openflow) #</pre>	
Related Commands		
Note		

forward-to-controller

forward-to-controller {[ospf] [lldp] [arp-unicast] [arp-broadcast] all | none}

Forwards the selected traffic types to the controller from all the ports on which OpenFlow enabled.

Syntax Description	ospf	Forwards OSPF traffic to the controller.
	lldp	Forwards LLDP traffic to the controller.
	arp-unicast	Forwards ARP-unicast traffic to the controller.
	arp-broadcast	Forwards ARP-broadcast traffic to the controller.
	all	Forwards all traffic types to the controller.
	none	Forwards no traffic to the controller.
Default	None	
Configuration Mode	Config OpenFlow	
History	3.3.4200	
Role	admin	
Example	<pre>switch (config openflow) # forward-to-controller all switch (config openflow) #</pre>	
Related Commands		
Note		

show openflow

show openflow [detail | tables | flows <id>]

Displays general information about the OpenFlow protocol configuration.

Syntax Description	detail	Displays detailed information about the OpenFlow protocol.
	tables	Displays information about the OpenFlow tables (size, type, etc.).
	flows <id>	Displays specific flows inside the OpenFlow tables. ID may be a range (e.g. 1-10).
	statistics	Displays OpenFlow statistics.
Default	None	
Configuration Mode	Any Command Mode	
History	3.3.4200	
	3.3.4302	Removed flow-id parameter Added “flows” and “statistics” parameters
Role	admin	
Example	<pre>switch (config openflow) # show openflow flows 2 Flow id: 2 priority: 1 hard timeout: infinite idle timeout: 0 sec match: ingress interface: Eth1/18 source Ethernet address: 11:22:33:44:55:66 destination Ethernet address: 77:88:aa:bb:cc:fe Ethernet type: 0x800 VLAN ID: 308 PCP: 4 SIP: 1.1.1.1 DIP: 2.2.2.2 Dport: 1790 Protocol: 86 TOS: 120 actions: output controller statistics: 0 packets, 0 bytes switch (config openflow) #</pre>	
Related Commands		
Note		

5.7 IGMP Snooping



Only IGMP Snooping v1 and v2 are supported.

The Internet Group Multicast Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. The host joins a multicast-group by sending a join request message towards the network router, and responds to queries sent from the network router by dispatching a join report.

A given port can be either manually configured to be a router-port or it can be dynamically manifested when having received a query, hence, the network router is connected to this port. All IGMP Snooping Control packets received from hosts (joins/leaves) are forwarded to the router-port, and the router-port will update its multicast-group data-base accordingly. Each dynamically learnt multicast group will be added to all of the router-ports on the switch.

As many as 5K multicast groups can be created on the switch.

5.7.1 Configuring IGMP Snooping

You can configure IGMP snooping to establish multicast group memberships.

➤ **To configure IGMP snooping:**

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Enable IGMP snooping globally. Run:

```
switch (config) # ip igmp snooping
switch (config) #
```

Step 4. Enable IGMP snooping on a VLAN. Run:

```
switch (config) # vlan 2
switch (config vlan 2) # ip igmp snooping
```

5.7.2 Defining a Multicast Router Port on a VLAN

You can define a Multicast Router (MRouter) port on a VLAN in one of the following methods:

➤ **To change the Interface Switchport to Trunk:**

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Enable IGMP snooping globally. Run:

```
switch (config) # ip igmp snooping
switch (config) #
```

- Step 4.** Change the interface switchport mode of the port (the interface is member of VLAN 1 by default). Run:

```
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) # switchport mode trunk
```

- Step 5.** Change back to config mode. Run:

```
switch (config interface ethernet 1/1) # exit
switch (config) #
```

- Step 6.** Define the MRouter port on the VLAN. Run:

```
switch (config) # vlan 2
switch (config vlan 2) # ip igmp mrouter interface ethernet 1/1
switch (config vlan 2) #
```

➤ **To change the Interface Switchport to Hybrid:**

- Step 1.** Log in as admin.

- Step 2.** Enter config mode. Run:

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

- Step 3.** Enable IGMP snooping globally. Run:

```
switch (config) # ip igmp snooping
switch (config) #
```

- Step 4.** Create a VLAN. Run:

```
switch (config) # vlan 200
switch (config vlan 200) #
```

- Step 5.** Change back to config mode. Run:

```
switch (config vlan 200) # exit
switch (config) #
```

- Step 6.** Change the interface switchport mode of the port (the interface is member of VLAN 1 by default). Run:

```
switch (config) # interface ethernet 1/36
switch (config interface ethernet 1/36) # switchport mode hybrid
```

- Step 7.** Attach the VLAN to the port's interface. Run:

```
switch (config interface ethernet 1/36) # switchport mode hybrid allowed-vlan 200
switch (config interface ethernet 1/36) #
```

- Step 8.** Change to config mode again. Run:

```
switch (config interface ethernet 1/36) # exit
switch (config) #
```

- Step 9.** Define the MRouter port on the VLAN. Run:

```
switch (config) # vlan 200
switch (config vlan 200) # ip igmp mrouter interface ethernet 1/36
switch (config vlan 200) #
```

5.7.3 IGMP Snooping Querier

IGMP Snooping Querier compliments the IGMP snooping functionality. IGMP Snooping Querier is used to support IGMP snooping in a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed. When IGMP Snooping Querier is enabled, IGMP queries are sent out periodically by the switch through all ports in the VLAN and to which hosts wishing to receive IP multicast traffic respond with IGMP report messages. IGMP Snooping Querier must be used in conjunction with IGMP snooping as IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

➤ **To configure IGMP Snooping Querier**

Step 1. Enable the IGMP snooping on the switch. Run:

```
switch (config) # ip igmp snooping
```

Step 2. Enable the IGMP snooping querier on a specific VLAN. Run:

```
switch (config) # interface vlan 10  
switch (config vlan 10)# ip igmp snooping querier
```

Step 3. Set the query interval time. Run:

```
switch (config vlan 10)# igmp snooping querier query-interval 25
```

Step 4. (Optional) Verify the IGMP snooping querier configuration. Run:

```
switch (config vlan 10)# show ip igmp snooping querier  
VLAN 10  IGMP Querier Present  query-interval: 125  address: 1.1.1.2  version: 2  
switch (config vlan 10)#
```

5.7.4 Commands

ip igmp snooping (admin)

ip igmp snooping
no ip igmp snooping

Enables IGMP snooping globally or per VLAN.
 The no form of the command disables IGMP snooping globally or per VLAN.

Syntax Description	N/A
Default	IGMP snooping is disabled, globally and per VLAN.
Configuration Mode	Config Config VLAN
History	3.1.1400
Role	admin
Example	<pre>switch (config) # ip igmp snooping switch (config) # vlan 10 switch (config vlan 10) # ip igmp snooping switch (config vlan 10) # exit switch (config) # show ip igmp snooping</pre> IGMP snooping global configuration: <pre>IGMP snooping globally enabled IGMP snooping operationally enabled Proxy-reporting globally disabled Last member query interval is 1 seconds Mrouter timeout is 125 seconds Port purge timeout is 260 seconds Report suppression interval is 5 seconds</pre> <pre>switch (config vlan 10) # show ip igmp snooping vlan 10</pre> Vlan 10 configuration parameters: <pre>IGMP snooping is enabled IGMP version is V2 Snooping switch is acting as Non-Querier mrouter static port list: none mrouter dynamic port list: none switch (config vlan 10) # vlan 10 switch (config vlan 10) #</pre>
Related Commands	show ip igmp snooping
Note	IGMP snooping has global admin state, and per VLAN admin state. Both states need to be enabled in order to enable the IGMP snooping on a specific VLAN.

ip igmp snooping (config)

ip igmp snooping {last-member-query-interval <1-25> | proxy reporting mrouter-timeout <60-600> | port-purge-timeout <130-1225> | report-suppression-interval <1-25>}

no ip igmp snooping {last-member-query-interval | proxy reporting | mrouter-timeout | report-suppression-interval}

Configures IGMP global parameters.

The no form of the command resets the IGMP global parameters to default.

Syntax Description	last-member-query-interval <1-25>	Sets the time period (in seconds) with which the general queries are sent by the IGMP querier. After timeout expiration the port will be removed from the multicast group.
	proxy reporting	Enables proxy reporting
	mrouter-timeout <60-600>	Sets the IGMP snooping router port purge time-out after which the port gets deleted if no IGMP router control packets are received. The default value is 125 seconds.
	port-purge-timeout <130-1225>	Sets the IGMP snooping port purge time interval after which the port gets deleted if no IGMP reports are received.
	report-suppression-interval <1-25>	Sets the IGMP snooping report-suppression time interval for which the IGMPv2 report messages for the same group will not get forwarded onto the router ports. The default value is 5 seconds.
Default	last-member-query-interval – 1 second proxy reporting is disabled mrouter-timeout – 125 port-purge-timeout – 260 seconds report-suppression-interval – 5 seconds	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	

Example

```
switch (config) # ip igmp snooping report-suppression-interval 3
switch (config) # show ip igmp snooping
```

IGMP snooping global configuration:

```
IGMP snooping globally enabled
IGMP snooping operationally enabled
Proxy-reporting globally disabled
Last member query interval is 1 seconds
Mrouter timeout is 125 seconds
Port purge timeout is 260 seconds
Report suppression interval is 3 seconds
```

```
switch (config) #
```

Related Commands

```
ip igmp snooping (admin)
show ip igmp snooping
```

Note

ip igmp snooping fast-leave

ip igmp snooping fast-leave
no ip igmp snooping fast-leave

Enables fast leave processing on a specific interface.
 The no form of the command disables fast leave processing on a specific interface.

Syntax Description	N/A
Default	Normal-leave is enabled.
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel
History	3.1.1400 3.3.4500 Added MLAG port-channel configuration mode
Role	admin
Example	<pre> switch (config interface ethernet 1/1) # ip igmp snooping fast-leave switch (config interface ethernet 1/1) # show ip igmp snooping inter- faces interface leave-mode ----- Eth1/1 Fast Eth1/2 Normal Eth1/3 Normal ... switch (config interface ethernet 1/1) # </pre>
Related Commands	show ip igmp snooping interfaces
Note	

ip igmp snooping static-group

ip igmp snooping static-group <IP address> interface <type> <number>
no ip igmp snooping static-group <IP address> interface <type> <number>

Creates a static multicast group and attaches a port to a specified group.
 The no form of the command deletes the interface from the multicast group.

Syntax Description	Ip address	Multicast IP address <224.x.x.x - 239.255.255.255>	
	interface <type> <number>	Attach the group to a specific interface. type - ethernet or port-channel	
Default	No static groups are configured.		
Configuration Mode	Config VLAN		
History	3.1.1400		
Role	admin		
Example	<pre>switch (config)# vlan 1 switch (config vlan 1) # ip igmp snooping static-group 230.0.0.1 interface ethernet 1/1 switch (config vlan 1) # show ip igmp snooping groups Vlan ID Group St/Dyn Ports ----- 1 230.0.0.1 St Eth1/1 Total Num of Dynamic Group Addresses 0 Total Num of Static Group Addresses 1 switch (config vlan 1) #</pre>		
Related Commands	show ip igmp snooping groups		
Note	If the deleted interface is the last port, it deletes the entire multicast group.		

ip igmp snooping mrouter

ip igmp snooping mrouter interface <type> <number>
no ip igmp snooping mrouter interface <type> <number>

Creates a static multicast router port on a specific VLAN, on a specific interface.
 The no form of the command removes the static multicast router port from a specific VLAN.

Syntax Description	interface <type> <number> Attaches the group to a specific interface. type - ethernet or port-channel.
Default	No static mrouter are configured.
Configuration Mode	Config VLAN
History	3.1.1400
Role	admin
Example	<pre>switch (config)# vlan 1 switch (config vlan 1) # ip igmp snooping mrouter interface ethernet 1/1 switch (config vlan 1) # show ip igmp snooping mrouter Vlan Ports ----- 1 Eth1/1(static) switch (config vlan 1) #</pre>
Related Commands	show ip igmp snooping mrouter
Note	The multicast router port can be created only if IGMP snooping is enabled both globally and on the VLAN.

ip igmp snooping unregistered multicast

ip igmp snooping unregistered multicast <options>

no ip igmp snooping unregistered multicast

Sets the behavior of the snooping switch for unregistered multicast traffic.
The no form of the command sets it default.

Syntax Description	options • flood • forward-to-mrouter-ports
Default	flood
Configuration Mode	Config
History	3.2.0500
Role	admin
Example	<pre>switch (config) # ip igmp snooping unregistered multicast flood switch (config) # show ip igmp snooping</pre> IGMP snooping global configuration: <pre>IGMP snooping globally enabled IGMP snooping operationally enabled Proxy-reporting globally disabled Last member query interval is 1 seconds Mrouter timeout is 125 seconds Port purge timeout is 260 seconds Report suppression interval is 5 seconds IGMP snooping unregistered multicast: flood switch (config) #</pre>
Related Commands	show ip igmp snooping
Note	

ip igmp snooping querier

ip igmp snooping querier
no ip igmp snooping querier

Enables the IGMP Snooping Querier on a VLAN.
 The no form of the command disables the IGMP Snooping Querier on a VLAN.

Syntax Description	N/A
Default	Disable
Configuration Mode	Config VLAN
History	3.3.4200
Role	admin
Example	switch (config vlan 1)# ip igmp snooping querier switch (config vlan 1)#
Related Commands	igmp snooping querier query-interval show ip igmp snooping querier
Note	

igmp snooping querier query-interval

igmp snooping querier query-interval <time>

no igmp snooping querier query-interval

Configures the query interval.

The no form of the command rests the parameter to its default.

Syntax Description	time	Time interval between queries (in seconds).
Default	125 seconds	
Configuration Mode	Config VLAN	
History	3.3.4200	
Role	admin	
Example	switch (config vlan 1)# igmp snooping querier query-interval 20 switch (config vlan 1)#	
Related Commands	igmp snooping querier query-interval show ip igmp snooping querier	
Note		

show ip igmp snooping

show ip igmp snooping

Displays IGMP snooping information for all VLANs or a specific VLAN.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin
Example	<pre>switch (config) # show ip igmp snooping IGMP snooping global configuration: IGMP snooping globally enabled IGMP snooping operationally enabled Proxy-reporting globally disabled Last member query interval is 1 seconds Mrouter timeout is 125 seconds Port purge timeout is 260 seconds Report suppression interval is 3 seconds IGMP snooping unregistered multicast: flood switch (config) #</pre>
Related Commands	
Note	

show ip igmp snooping groups

show ip igmp snooping groups

Displays per VLAN the list of multicast groups attached (static or dynamic allocated) per port.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin
Example	<pre>switch (config) # show ip igmp snooping groups Vlan ID Group St/Dyn Ports ----- 1 230.0.0.1 St Eth1/1 Total Num of Dynamic Group Addresses 0 Total Num of Static Group Addresses 1 switch (config) #</pre>
Related Commands	
Note	

show ip igmp snooping vlan

show ip igmp snooping vlan {<vlan/vlan-range> | all}

Displays IGMP configuration per VLAN or VLAN range.

Syntax Description	vlan/vlan range	Displays IGMP VLAN configuration per specific VLAN or VLAN range.
	all	Display IGMP VLAN configuration on all VLAN.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
Role	admin	
Example	<pre>switch (config) # show ip igmp vlan 1 Vlan 1 configuration parameters: IGMP snooping is enabled IGMP version is V2 Snooping switch is acting as Non-Querier mrouter static port list: Eth1/1 mrouter dynamic port list: none switch (config) #</pre>	
Related Commands		
Note		

show ip igmp snooping mrouter

show ip igmp snooping mrouter

Displays IGMP snooping multicast router information.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin
Example	<pre>switch (config) # show ip igmp snooping mrouter Vlan Ports ----- 1 Eth1/1(static) switch (config) #</pre>
Related Commands	
Note	

show ip igmp snooping interfaces

show ip igmp snooping interfaces

Displays IGMP snooping interface information.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin
Example	<pre> switch (config) # show ip igmp snooping interfaces interface leave-mode ----- 1/1 Normal 1/2 Normal 1/3 Normal 1/4 Fast ... switch (config) # </pre>
Related Commands	
Note	

show ip igmp snooping statistics

show ip igmp snooping statistics

Displays IGMP snooping statistical counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.1.1400
Role	admin
Example	<pre>switch (config) # show ip igmp snooping statistics Snooping Statistics for VLAN 1 General queries received : 0 Group specific queries received : 0 V1/V2 reports received : 0 V1/V2 reports transmitted : 0 Leave messages received : 0 Group specific queries transmitted: 0 Leave messages transmitted: 0 Unsuccessful joins received count Per Vlan: 0 Active/Successful joins received count Per Vlan: 0 Active Groups count: 0 Packets dropped: 0 switch (config) #</pre>
Related Commands	
Note	

show ip igmp snooping querier

show ip igmp snooping querier [vlan <num>]

Displays running IGMP snooping querier configuration on the VLANs.

Syntax Description	vlan <num>	Displays the IGMP snooping querier configuration running on the specified VLAN.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.4200	
Role	admin	
Example	switch (config) # show ip igmp snooping querier vlan 10 Vlan 1 IGMP Querier Present query-interval: 20 address: 1.1.1.2 version: 2 switch (config) #	
Related Commands		
Note		

5.8 Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 LAN. The protocol is formally defined in IEEE 802.1AB.

5.8.1 Configuring LLDP

➤ *To configure the LLDP on the switch:*

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Enable LLDP globally on the switch. Run:

```
switch (config) # lldp
switch (config) #
```

Step 4. Enable LLDP per interface. Run:

```
switch (config interface ethernet 1/1) # lldp receive
switch (config interface ethernet 1/1) # lldp transmit
```

Step 5. Show LLDP local information. Run:

```
switch (config) # show lldp local

LLDP is Enabled

Local global configuration
Chassis sub type: macAddress (4)
Chassis id: 00:11:22:33:44:55
System Name: "switch-111111"
System Description: my-system-description
Supported capabilities: B
Supported capabilities enabled: B
```

Step 6. Show LLDP remote information. Run:

```
switch (config)# show lldp interfaces ethernet 1/1 remote

Ethernet 1/1
Remote Index: 1
Remote chassis id: 00:11:22:33:44:55 ; chassis id subtype: mac
Remote port-id: ethernet 1/2; port id subtype: local
Remote port description: ethernet 1/2
Remote system name: remote-system
Remote system description: remote-system-description
Remote system capabilities supported: B ; B
```

5.8.2 DCBX

Data Center Bridging (DCB) is an enabler for running the Ethernet network with lossless connectivity using priority-based flow control and enhanced transmission selection. DCBx (exchange)

compliments the DCB implementation by offering a dynamic protocol that communicates DCB attributes between peering endpoint.

5.8.3 Commands

lldp

lldp
no lldp

Enables LLDP globally.
The no form of the command disables the LLDP.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.2.0300
Role	admin
Example	switch (config)# lldp switch (config)#
Related Commands	show lldp local
Note	

lldp reinit

lldp reinit <seconds>
no lldp reinit

Sets the delay in seconds from enabling the LLDP on the port until re-initialization will be attempted.

The no form of the command sets the parameter to default.

Syntax Description	seconds	1-10
Default	2	
Configuration Mode	Config	
History	3.2.0300	
Role	admin	
Example	switch (config)# lldp reinit 10 switch (config)#	
Related Commands	show lldp timers	
Note		

lldp timer

lldp timer <seconds>
no lldp timer

Sets the LLDP interval at which LLDP frames are transmitted. (lldpMessageTxInterval)

The no form of the command sets the parameter to default.

Syntax Description	seconds	5-32768
Default	30	
Configuration Mode	Config	
History	3.2.0300	
Role	admin	
Example	switch (config)# lldp timer 10 switch (config)#	
Related Commands	show lldp timers	
Note		

lldp tx-delay

lldp tx-delay <seconds>

no lldp tx-delay

Indicates the delay in seconds between successive LLDP frame transmissions
The no form of the command sets the parameter to default.

Syntax Description	seconds	1-8192
Default	2	
Configuration Mode	Config	
History	3.2.0300	
Role	admin	
Example	switch (config)# lldp tx-delay 10 switch (config)#	
Related Commands	show lldp timers	
Note	The recommended value for the tx-delay is set by the following formula: $1 \leq \text{lldp tx-delay} \leq (0.25 * \text{lldp timer})$	

lldp tx-hold-multiplier

lldp tx-hold-multiplier <seconds>

no lldp tx-hold-multiplier

The time-to-live value expressed as a multiple of the lldpMessageTxInterval object. The no form of the command sets the parameter to default.

Syntax Description	seconds	1-8192
Default	2	
Configuration Mode	Config	
History	3.2.0300	
Role	admin	
Example	switch (config)# lldp tx-hold-multiplier 10 switch (config)#	
Related Commands	show lldp timers	
Note	The actual time-to-live value used in LLDP frames, can be expressed by the following formula: $TTL = \min(65535, (lldpMessageTxInterval * lldpMessageTxHoldMultiplier))$ For example, if the value of lldpMessageTxInterval is '30', and the value of lldpMessageTxHoldMultiplier is '4', then the value '120' is encoded in the TTL field in the LLDP header.	

lldp {receive | transmit}

lldp {receive | transmit}
no lldp {receive | transmit}

Enables LLDP to be received or transmitted on this port.
 The no form of the command disables the LLDP to be received or transmitted on this port.

Syntax Description	N/A
Default	Enabled for receive and Transmit.
Configuration Mode	Config Interface Ethernet
History	3.2.0300
Role	admin
Example	switch (config interface ethernet 1/1)# lldp receive switch (config interface ethernet 1/1)# lldp transmit switch (config interface ethernet 1/1)#
Related Commands	show lldp interface
Note	The LLDP is disabled by default (globally)

lldp tlv-select

lldp tlv-select {[dcbx] [dcbx-cee] [port-description] [sys-name] [sys-description] [sys-capabilities] [management-address] [none] all}

Sets the LLDP basic TLVs to be transmitted on this port.

Syntax Description	dcbx	Enables LLDP-DCBX TLVs.
	dcbx-cee	Enables LLDP-DCBX CEE TLVs.
	port-description	LLDP port description TLV.
	sys-name	LLDP system name TLV.
	sys-description	LLDP system description TLV.
	sys-capabilities	LLDP system capabilities TLV.
	management-address	LLDP management address TLV.
	all	all above TLVs.
	none	None of the above TLVs.
Default	all	
Configuration Mode	Config Interface Ethernet	
History	3.2.0300	Initial revision
	3.3.0000	Added “none” parameter
	3.3.4302	Added “dcbx” parameter
	3.3.4402	Added “dcbx-cee” parameter
Role	admin	
Example	<pre>switch (config interface ethernet 1/1)# lldp tlv-select port-description sys-name switch (config interface ethernet 1/1)#</pre>	
Related Commands	show lldp interface	
Note		

dcb application-priority

dcb application-priority <selector> <protocol> <priority>

Adds an application to the application priority table.

Syntax Description	selector	Protocol field in hexa notation (e.g. '0x8906' for FCoE, '0x8914' for FIP).
	protocol	Has 4 options: 1. ethertype 2. tcp-sctp 3. udp-dccp 4. tcp-sctp-udp-dccp
	priority	Range: 0-7.
Default	No applications are available. The table is empty.	
Configuration Mode	Config	
History	3.3.4200	
Role	admin	
Example	switch (config-if)# dcb application-priority ethertype 3 0x8906 switch (config-if)#	
Related Commands	show lldp interface	
Note		

show lldp local

show lldp local

Shows LLDP local information.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0300
Role	admin
Example	<pre>switch (config)# show lldp local LLDP is Enabled Local global configuration Chassis sub type: macAddress (4) Chassis id: 0002C9030046AF00 System Name: my-switch System Description: SX1036 Supported capabilities: B,R Supported capabilities enabled: B switch (config)#</pre>
Related Commands	
Note	

show lldp interface

show lldp interface [ethernet <inf>]

Shows LLDP local interface table information.

Syntax Description	infInterface number (e.g. 1/1).				
Default	N/A				
Configuration Mode	Any Command Mode				
History	3.2.0300	First release			
	3.3.4200	Updated example			
	3.3.4402	Updated example			
Role	admin				
Example	switch (config)# show lldp interface ethernet 1/1				
	TLV flags:				
	PD: port-description, SN: sys-name, SD: sys-description, SC: sys-capabilities, MA: management-address, ETS-C: ETS-Configuration, ETS-R: ETS-Recommendation, AP: Application Priority, PFC: Priority Flow Control, CEE: Converged Enhanced Ethernet DCBX version				
	Interface	Receive	Transmit	Notification	TLVs
	eth1/1	Enable	Enable	Enable	PD, SN, SD, SC, MA, PFC, CEE
eth1/2	Disable	Disable	Enable	PD, SN, SD, MA, AP	
eth1/3	Enable	Disable	Disable	PD, SD, SC, ETS-R, AP, PFC	
...					
	switch (config)#				
Related Commands					
Note					

show lldp interfaces ethernet <inf> remote

show lldp interfaces ethernet <inf> remote

Shows LLDP remote interface table information.

Syntax Description	inf	Local interface number (e.g. 1/1).
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.2.0300	First release.
	3.3.4200	Updated output.
Role	admin	

Example

```

switch (config)# show lldp interfaces ethernet <number> Ethernet <port-number> // example "Ethernet 1/1"
Latest LLDPDU received on <date> // e.g. date: "Thu Feb 14 12:08:29 2013" - new field
Remote Index:
Remote chassis id: <byte array> ; chassis id subtype: <sub-type>
Remote port-id: <byte array> ; port id subtype: <sub-type>
Remote port description: <byte array>
Remote system name: <byte array>
Remote system description: < byte array>
Remote system capabilities supported: <enum parsed as defined in the MIB> ; enable <enum parsed as defined in the
MIB>
Management Table //theoretically remote can send more then one management address (Future) RemoteIndex Subtype Address
ifSubtype ifId OID
1 ipv4(1) 10.10.10.10 ifIndex(2) 1(mgmt0) <Oid>
1 ipv4(1) 10.10.10.11 ifIndex(3) 2(mgmt1) <Oid>
Unknown TLVs Table //(Future) Type Info
-----
<integer> <byte-array>
<integer> <byte-array>
Organizationally-Defined Information Table // (Future) OUI subtype Index DefInfo
-----
<byte-array> <integer> <integer> <byte-array>
<byte-array> <integer> <integer> <byte-array>
Remote PFC configuration // new section Willing: {enabled, disabled}
MACsec: {enabled, disabled}
Number of supported traffic classes: 4 // range is 1-8
PFC enabled on priorities: 5 7 // it could be "0 1 2 3 4 5 6 7" or " 1 3 7" or "None"
WARNING: peer PFC configuration does not match the local PFC configuration // This warning should appear only if the
local and remote PFC configuration don't match!
Remote ETS configuration // new section Willing: {enabled, disabled}
CBS: {enabled, disabled}
Number of supported traffic classes: 3 // range is 1-8
WARNING: peer ETS configuration does not match the local ETS configuration // This warning should appear only if the
local and remote ETS configuration don't match!
Priority assignment table: Priority TC
-----
0
0
1
0
2
1
3
1
4
2
5
2
6
3
7
3
Traffic class bandwidth table // (No need to have the recommended TC - ETS-Recommended TLV)
TC Bandwidth TSA
-----
Page 43 of 354
0 25% tsaStrictPriority(0) // we are expecting either 0 or 2 as answers.

```

Related Commands**Note**

show lldp timers

show lldp timers

Shows LLDP timers configuration

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0300
Role	admin
Example	<pre>switch (config)# show lldp timers msg-tx-interval:30 tx-delay:2 tx-hold:4 tx-reinit-delay:2 switch (config)#</pre>
Related Commands	
Note	

show lldp statistics global

show lldp statistics global

Shows LLDP global statistics

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0300
Role	admin
Example	<pre>switch (config)# show lldp timers Remote Table Last Change Time : 10300 Remote Table Inserts : 5 Remote Table Deletes : 0 Remote Table Drops : 0 Remote Table Ageouts : 0 switch (config)#</pre>
Related Commands	
Note	

show lldp statistics [interface ethernet <inf>]

show lldp statistics [interface ethernet <inf>]

Shows LLDP interface statistics

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.2.0300
Role	admin
Example	<pre>switch (config)# show lldp statistics ethernet 1/1 Interface Frames In In TLVs TLVs Ageout Out Discarded Errors Total Discarded Unrecognize Frames ----- Eth 1/1 0 0 10 0 0 0 0 switch (config)#</pre>
Related Commands	
Note	

show dcb application-priority

show dcb application-priority

Displays application priority admin table.

Syntax Description	N/A												
Default	N/A												
Configuration Mode	Any Command Mode												
History	3.3.4200												
Role	admin												
Example	<pre>switch (config)# show dcb application-priority</pre> Application priority configuration <table><thead><tr><th>Selector</th><th>Protocol</th><th>Priority</th></tr><tr><th colspan="3">-----</th></tr></thead><tbody><tr><td>Ethertype</td><td>0x8906</td><td>3</td></tr><tr><td>Ethertype</td><td>0x8914</td><td>3</td></tr></tbody></table> <pre>switch (config)#</pre>	Selector	Protocol	Priority	-----			Ethertype	0x8906	3	Ethertype	0x8914	3
Selector	Protocol	Priority											

Ethertype	0x8906	3											
Ethertype	0x8914	3											
Related Commands													
Note													

5.9 Quality of Service (QoS)

5.9.1 Priority Flow Control and Link Level Flow Control

Priority Flow Control (PFC) provides an enhancement to the existing pause mechanism in Ethernet. The current Ethernet pause option stops all traffic on a link. PFC creates eight separate virtual links on the physical link and allows any of these links to be paused and restarted independently, enabling the network to create a no-drop class of service for an individual virtual link. PFC has 8 possible priorities (3 bits in VLAN header). Each priority can be mapped to one of 4 possible queues in the ingress.

The PFC software offers the following features:

- Provides per-priority enabling or disabling of flow control
- Transmits PFC-PAUSE frames when the receive threshold for a particular traffic class is reached
- Provides the management capability for an administrator to configure the flow control properties on each port of the switch
- Keeps flow control disabled for all priorities on all ports by default
- Allows an administrator to enable or disable flow control per port and per priority level
- Supports flow control only on physical ports, not on logical interfaces such as tunnels or interfaces defined by sharing a physical port in multiple virtual switch contexts
- Uses the configured threshold values to set up the queue buffer spaces accordingly in the datapath
- Provides hardware abstraction layer callouts for the following:
 - Enabling or disabling of flow control on each port for each priority
 - Configuring the queue depth for each priority on each port
- Provides trace logs for execution upon error conditions and for any event notifications from the hardware or datapath. These trace logs are a useful aid in troubleshooting.
- Allows the administrator to configure the minimum and maximum threshold values for flow control. These configurations are applied globally on all ports and priorities.

Priority Based Flow Control (PFC) provides an enhancement to the existing pause flow control mechanism as described in 802.1X.

➤ **To enable PFC globally:**

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Enable PFC globally on the switch. Run:

```
switch (config) # dcb priority-flow-control enable
This action might cause traffic loss while shutting down a port with priority-flow-control mode on
Type 'yes' to confirm  enable pfc globally: yes
```

➤ **To enable PFC per priority:**

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Enable PFC globally on the switch. Run:

```
switch (config) # dcb priority-flow-control enable
# dcb priority-flow-control enable
This action might cause traffic loss while shutting down a port with priority-flow-control mode on
Type 'yes' to confirm enable pfc globally: yes
switch (config) #
```

Step 4. Choose the desirable priority you want to enable using the command `dcb priority-flow-control priority <pri[0..7]> enable`.

```
switch (config) # dcb priority-flow-control priority 5 enable
```

➤ **To enable PFC per interface:**

Step 1. Log in as admin.

Step 2. Change to config mode. Run:

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

Step 3. Enable PFC globally on the switch. Run:

```
switch (config) # dcb priority-flow-control enable
```

Step 4. Choose the desirable priority you want to enable using the command `dcb priority-flow-control priority <pri[0..7]> enable`

```
switch (config) # dcb priority-flow-control 5 enable
```

Step 5. Change to Interface mode. Run:

```
switch (config) #
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) #
```

Step 6. Enable PFC for the specific interface:

```
switch (config interface ethernet 1/1) # dcb priority-flow-control mode on
```

5.9.2 Enhanced Transmission Selection (ETS)

Enhanced Transmission Selection (ETS) provides a common management framework for assignment of bandwidth to traffic classes, for weighted round robin (WRR) scheduling. If a traffic class does not use all the bandwidth allocated to it, other traffic classes can use that available bandwidth. This allows optimal utilization of the network capacity while prioritizing and providing the necessary resources.

The ETS feature has the following attributes:

- ETS global admin:
 - Enable (default) – scheduling mode is WRR according to the configured bandwidth-per-traffic class
 - Disable – scheduling mode is Strict Priority (SP)

- Bandwidth percentage for each traffic class: By default each traffic class gets an equal share

The default mapping of priority to traffic classes (per interface) is as follows:

- Priority 0,1 mapped to TC 0
- Priority 2,3 mapped to TC 1
- Priority 4,5 mapped to TC 2
- Priority 6,7 mapped to TC 3



TC0 and TC3 are lossy TCs, while TC1 and TC2 can be lossless as well as lossy. It is possible but not recommended to map PFC enabled priorities (lossless traffic) to those TC0 or TC3.

ETS is enabled by default (scheduling is WRR).

➤ **To set the scheduling mode to Strict Priority:**

Step 1. Run the command `dcb ets disable`.

```
switch (config) # no dcb ets enable
```

➤ **To configure the WRR bandwidth percentage:**

Step 1. Make sure ETS feature is enabled. Run:

```
switch (config) # dcb ets enable
```

Step 2. Choose the WRR bandwidth rate and distribution.

By default the WRR distribution function is equal 25% per TC. Changing the WRR bandwidth rate will cause a change in the distribution function, for example if you wish to schedule more traffic on TC-0, TC-1, TC-2 while reducing the amount of traffic sent on TC-3, run the command `dcb ets tc bandwidth`.

```
switch (config) # dcb ets tc bandwidth 30 30 30 10
# show dcb ets
```

ETS enabled

TC	Bandwidth
0	30%
1	30%
2	30%
3	10%

Number of Traffic Class: 4
switch (config) #



Traffic class priorities are <0-3>, where 0 is the lowest and 3 is the highest.



The sum of all traffic class bandwidth value (in percentage) should be 100, otherwise the command fails.

Step 3. Run the command `show dcb ets` to verify the configuration.

```
switch (config) # show dcb ets
ETS enabled
```

TC	Bandwidth
0	30%
1	30%
2	10%
3	30%

```
Number of Traffic Class: 4
switch (config) #
```

5.9.3 Commands

5.9.3.1 Enhanced Transmission Selection (ETS)

dcb ets enable

dcb ets enable
no dcb ets enable

Sets the switch egress scheduling mode to be weighted round robin.
 The no form of the command sets the switch egress scheduling mode to be strict priority.

Syntax Description	N/A										
Default	ETS is enabled.										
Configuration Mode	Config										
History	3.1.0000										
Role	admin										
Example	<pre>switch (config)# dcb ets enable switch (config)# show dcb ets</pre> ETS enabled <table> <thead> <tr> <th>TC</th><th>Bandwidth</th></tr> </thead> <tbody> <tr><td>0</td><td>25%</td></tr> <tr><td>1</td><td>25%</td></tr> <tr><td>2</td><td>25%</td></tr> <tr><td>3</td><td>25%</td></tr> </tbody> </table> Number of Traffic Class: 4 <pre>switch (config) #</pre>	TC	Bandwidth	0	25%	1	25%	2	25%	3	25%
TC	Bandwidth										
0	25%										
1	25%										
2	25%										
3	25%										
Related Commands	show dcb ets										
Note											

dcb ets tc bandwidth

dcb ets tc bandwidth <tc-0> <tc-1> <tc-2> <tc-3>
no dcb ets tc bandwidth

Configures the bandwidth limit of the traffic class.
 The no form of the command sets the bandwidths per traffic class back to its default.

Syntax Description	tc-i 0-100.										
Default	25% per traffic class.										
Configuration Mode	Config										
History	3.1.0000										
Role	admin										
Example	<pre>switch (config)# dcb ets tc bandwidth 20 20 30 30 switch (config) # show dcb ets</pre> ETS enabled <table> <thead> <tr> <th>TC</th><th>Bandwidth</th></tr> </thead> <tbody> <tr><td>0</td><td>20%</td></tr> <tr><td>1</td><td>20%</td></tr> <tr><td>2</td><td>30%</td></tr> <tr><td>3</td><td>30%</td></tr> </tbody> </table> Number of Traffic Class: 4 <pre>switch (config) #</pre>	TC	Bandwidth	0	20%	1	20%	2	30%	3	30%
TC	Bandwidth										
0	20%										
1	20%										
2	30%										
3	30%										
Related Commands	show dcb ets										
Note	The sum of all traffic class bandwidth must be equal to 100.										

vlan map-priority

vlan map priority <priority> traffic-class <tc>
no vlan map priority <priority>

Maps an VLAN user priority to a traffic class.
 The no form of the command sets the mapping back to default.

Syntax Description	N/A
Default	Priority 0,1 mapped to tc 0. Priority 2,3 mapped to tc 1. Priority 4,5 mapped to tc 2. Priority 6,7 mapped to tc 3.
Configuration Mode	Config Interface Ethernet
History	3.1.0000
Role	admin
Example	switch (config interface ethernet 1/1) # vlan map-priority 1 traffic-class 2 switch (config interface ethernet 1/1) #
Related Commands	show dcb ets interface
Note	

show dcb ets

show dcb ets

Displays ETS configuration and operational data.

Syntax Description

Default	ETS is enabled.
----------------	-----------------

Configuration Mode	Any Command Mode
---------------------------	------------------

History	3.1.0000
----------------	----------

Role	admin
-------------	-------

Example	switch (config)# show dcb ets
----------------	-------------------------------

ETS enabled

TC	Bandwidth
0	25%
1	25%
2	25%
3	25%

Number of Traffic Class: 4

switch (config) #

Related Commands

Note

show dcb ets interface

show dcb ets interface <type> <number>

Displays ETS configuration and operational data, per interface.

Syntax Description	type	ethernet or port-channel
	number	interface number, i.e. 1/1
Default	ETS is enabled.	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	

Example

```
switch (config)# show dcb ets interface ethernet 1/1
```

```
ETS Port Mode           :ON MODE
ETS Oper State          :INIT STATE
ETS State Machine Type  :Assymmetric
```

```
-----
ETS Local Port Info
```

```
-----
TC bandwidth table
```

```
-----
TC          Bandwidth      RecomBandwidth
-----
0           25%            25%
1           25%            25%
2           25%            25%
3           25%            25%
```

```
priority assignment table
```

```
-----
Priority      TC
```

```
-----
0             0
1             0
2             1
3             1
4             2
5             2
6             3
7             3
```

```
Number of Traffic Class: 4
```

```
Willing Status: Disable
```

```
-----
ETS Admin Port Info
```

```
-----
TC          Bandwidth      RecomBandwidth
-----
0           30%            30%
1           30%            30%
2           30%            30%
3           10%            10%
```

```
-----
ETS Remote Port Info
```

```
-----
No Remote Entry is Present
```

```
-----
switch (config) #
```

Related Commands**Note**

5.9.3.2 Priority Flow Control (PFC)

dcb priority-flow-control enable

dcb priority-flow-control enable
no dcb priority-flow-control enable

Enables PFC globally on the switch.
 The no form of the command globally disables PFC on the switch.

Syntax Description	N/A
Default	PFC is disabled.
Configuration Mode	Config
History	3.1.0000 Initial revision
	3.3.0000 Output update
Role	admin
Example	<pre>switch (config)# dcb priority-flow-control enable This action might cause traffic loss while shutting down a port with priority-flow-control mode on Type 'yes' to confirm enable pfc globally: yes switch (config)# show dcb priority-flow-control PFC enabled Priority Enabled List : Priority Disabled List :0 1 2 3 4 5 6 7 TC Lossless --- - 0 N 1 Y 2 Y 3 N Interface PFC admin PFC oper ----- 1/1 Disabled Disabled 1/2 Disabled Disabled 1/3 Disabled Disabled 1/4 Disabled Disabled ... switch (config) #</pre>
Related Commands	show dcb priority-flow-control
Note	This command asks the user to approve traffic loss because there might be interfaces with dcb mode on, that will be shutdown.

dcb priority-flow-control priority

dcb priority-flow-control priority <prio> enable
no dcb priority-flow-control priority <prio> enable

Enables PFC per priority on the switch.
 The no form of the command disables PFC per priority on the switch.

Syntax Description	prio	0-7.																																	
Default	PFC is disabled for all priorities.																																		
Configuration Mode	Config																																		
History	3.1.0000																																		
Role	admin																																		
Example	<pre>switch (config)# dcb priority-flow-control priority 0 enable switch (config)# show dcb priority-flow-control</pre> PFC enabled Priority Enabled List : 0 Priority Disabled List : 1 2 3 4 5 6 7 <table><tr><td>TC</td><td>Lossless</td></tr><tr><td>---</td><td>-----</td></tr><tr><td>0</td><td>N</td></tr><tr><td>1</td><td>Y</td></tr><tr><td>2</td><td>Y</td></tr><tr><td>3</td><td>N</td></tr></table> <table><tr><td>Interface</td><td>PFC admin</td><td>PFC oper</td></tr><tr><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>1/1</td><td>Disabled</td><td>Disabled</td></tr><tr><td>1/2</td><td>Disabled</td><td>Disabled</td></tr><tr><td>1/3</td><td>Disabled</td><td>Disabled</td></tr><tr><td>1/4</td><td>Disabled</td><td>Disabled</td></tr><tr><td>...</td><td></td><td></td></tr></table> <pre>switch (config) #</pre>		TC	Lossless	---	-----	0	N	1	Y	2	Y	3	N	Interface	PFC admin	PFC oper	-----	-----	-----	1/1	Disabled	Disabled	1/2	Disabled	Disabled	1/3	Disabled	Disabled	1/4	Disabled	Disabled	...		
TC	Lossless																																		
---	-----																																		
0	N																																		
1	Y																																		
2	Y																																		
3	N																																		
Interface	PFC admin	PFC oper																																	
-----	-----	-----																																	
1/1	Disabled	Disabled																																	
1/2	Disabled	Disabled																																	
1/3	Disabled	Disabled																																	
1/4	Disabled	Disabled																																	
...																																			
Related Commands	show dcb priority-flow-control																																		
Note																																			

dcb priority-flow-control mode on

dcb priority-flow-control mode on [force]

no dcb priority-flow-control mode

Enables PFC per interface.

The no form of the command disables PFC per interface.

Syntax Description	force	Force command implementation.
Default	PFC is disabled for all interfaces.	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
History	3.1.0000 3.3.4500 Added MLAG port-channel configuration mode	
Role	admin	
Example	<pre> switch (config interface ethernet 1/1) # dcb priority-flow-control mode on switch (config interface ethernet 1/1) # show dcb priority-flow-control PFC enabled Priority Enabled List : 0 Priority Disabled List : 1 2 3 4 5 6 7 TC Lossless --- - 0 N 1 Y 2 Y 3 N Interface PFC admin PFC oper ----- 1/1 On Enabled 1/2 Disabled Disabled 1/3 Disabled Disabled 1/4 Disabled Disabled ... switch (config) # </pre>	
Related Commands	show dcb priority-flow-control	
Note		

show dcb priority-flow-control

show dcb priority-flow-control [interface <type> <inf>] [detail]

Displays DCB priority flow control configuration and status.

Syntax Description	type	• ethernet • port-channel
	inf	The interface number.
	detail	Adds details information to the show output.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
Role	admin	
Example	<pre>switch (config interface ethernet 1/1) # show dcb priority-flow-control PFC enabled Priority Enabled List : 0 Priority Disabled List : 1 2 3 4 5 6 7 TC Lossless --- - 0 N 1 Y 2 Y 3 N Interface PFC admin PFC oper ----- 1/1 On Enabled 1/2 Disabled Disabled 1/3 Disabled Disabled 1/4 Disabled Disabled ... switch (config) #</pre>	
Related Commands		
Note		

5.10 Access Control List

An Access Control List (ACL) is a list of permissions attached to an object, to filter or match switches packets. When the pattern is matched at the hardware lookup engine, a specified action (e.g. permit/deny) is applied. The rule fields represent flow characteristics such as source and destination addresses, protocol and VLAN ID.

ACL support currently allows actions of *permit* or *deny* rules, and supports only ingress direction. ACL search pattern can be taken from either L2 or L3 fields, e.g L2/L3 source and destination addresses, protocol, VLAN ID and priority or TCP port.

5.10.1 Configuring Access Control List

Access Control List (ACL) is configured by the user and is applied to a port once the ACL search engine matches search criteria with a received packet.

➤ **To configure ACL:**

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

Step 3. Create a MAC / IPv4 ACL (access-list) entity.

```
switch (config) mac access-list mac-acl
switch (config mac access-list mac-acl) #
```

Step 4. Add a MAC / IP rules to the appropriate access-list.

```
switch (config mac access-list mac-acl) seq-number 10 deny 0a:0a:0a:0a:0a:0a mask
ff:ff:ff:ff:ff:ff any vlan 6 cos 2 protocol 80
switch (config mac access-list mac-acl) #
```

Step 5. Bind the created access-list to an interface (slot/port or port-channel).

```
switch (config)
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) # mac port access-group mac-acl
```

5.10.2 ACL Actions

An ACL action is a set of actions can be activated in case the packet hits the ACL rule.

➤ **To modify the VLAN tag of the egress traffic as part of the ACL “permit” rule:**

Step 1. Create access-list action profile:

- a. Create an action access-list profile using the command `access-list action <action-profile-name>`
- b. Add rule to map a VLAN using the command `vlan-map <vlan-id>` within the action profile configuration mode

Step 2. Create an access-list and bind the action rule:

- a. Create an access-list profile using the command `ipv4/mac access-list`
- b. Add access list rule using the command `deny/permit (action <action profile name>)`

Step 3. Bind the access-list to an interface using the command `ipv4/mac port access-group`

Create an action profile and add vlan mapping action:

```
switch (config)#access-list action my-action
switch (config access-list action my-action) # vlan-map 20
switch (config access-list action my-action) #exit
```

Create an access list and bind rules:

```
switch (config)# mac access-list my-list
switch (config mac access-list my-list)# permit any any action my-action
switch (config mac access-list my-list)# exit
```

Bind an access-list to a port:

```
Switch (config)# interface ethernet 1/1
Switch (config interface ethernet 1/1)# mac port access-group my-list
```

5.10.3 Commands

ipv4/mac access-list

```
{ipv4 | mac} access-list <acl-name>
no {ipv4 | mac} access-list <acl-name>
```

Creates a MAC or IPv4 ACL and enter the ACL configuration mode.
The no form of the command deletes the ACL.

Syntax Description	ipv4 mac	IPv4 or MAC – access list.
	acl-name	User defined string for the ACL.
Default	No ACL available by default.	
Configuration Mode	Config	
History	3.1.1400	
Role	admin	
Example	<pre>switch (config)# mac access-list my-mac-list switch (config mac access-list my-mac-list)#</pre>	
Related Commands	ipv4/port access-group	
Note		

ipv4/mac port access-group

{ipv4 | mac} port access-list <acl-name>
no {ipv4 | mac} port access-list <acl-name>

Binds an ACL to the interface.
 The no form of the command unbinds the ACL from the interface.

Syntax Description	ipv4 mac	IPv4 or MAC – access list.
	acl-name	ACL name.
Default	No ACL is bind by default.	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
History	3.1.1400	
	3.3.4500	Added MLAG port-channel configuration mode
Role	admin	
Example	switch (config interface ethernet 1/1) # mac port access-group my-list switch (config interface ethernet 1/1) #	
Related Commands	ipv4/mac access-list	
Note	The access control list should be defined prior to the binding action.	

deny/permit (MAC ACL rule)

[seq-number <sequence-number>] {deny|permit} {any | <source-mac> [mask <mac>]} {any | <destination-mac> [mask <mac>]} [protocol <protocol>] [cos <cos-value>] [vlan <vlan-id> | vlan-mask <vlan-mask>] [action <action-id>] no <sequence-number>

Creates a rule for MAC ACL.

The no form of the command deletes a rule from the MAC ACL.

Syntax Description	sequence-number	Optional parameter to set a specific sequence number for the rule. The range is:1-500.
	deny permit	Determines the type of the rule, denies or permits action.
	{any <source-mac> [mask <mac>]}	Sets source MAC and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the source MAC.
	{any <destination-mac> [mask <mac>]}	Sets destination MAC and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the destination MAC.
	protocol	Sets the Ethertype field value from the MAC address. Possible range is: 0x0000-0xffff.
	cos-value	Sets the COS (priority bits) field, possible range is: 0-7.
	vlan-id	Sets the VLAN ID field, possible range is 0-4095.
	vlan-mask <vlan-mask>	Sets VLAN group. Range: 0x0000-0x0FFF.
	action	Action name (free string).
Default	No rule is added by default to access control list. Default sequence number is in multiple of 10.	
Configuration Mode	Config MAC ACL	
History	3.1.1400	
	3.3.4500	Added vlan-mask parameter
Role	admin	
Example	<pre>switch (config mac access-list my-list) # seq-number 10 deny 0a:0a:0a:0a:0a:0a mask ff:ff:ff:ff:ff:ff any vlan 6 cos 2 protocol 80 switch (config mac access-list my-list) #</pre>	
Related Commands	ipv4/mac access-list ipv4/mac port access-group	
Note		

deny/permit (IPv4 ACL rule)

```
[seq-number <sequence-number>] {permit | deny} ip {<source-ip> [mask <ip>] |
[any]} {<dest-ip> [mask <ip>] | [any]} [action <action-id>]
no <sequence-number>
```

Creates a rule for IPv4 ACL.

The no form of the command deletes a rule from the IPv4 ACL.

Syntax Description	sequence-number	Optional parameter to set a specific sequence number for the rule. The range is:1-500.
	deny permit	Determines the type of the rule, deny or permit action. Valid mask values fall in the range 0-255.
	{any <source-ip> [mask <ip>]}	Sets source IP and optionally sets a mask for that IP address. The “any” option causes the rule to not check the source IP. Valid mask values fall in the range 0-255.
	{any <destination-ip> [mask <ip>]}	Sets destination IP and optionally sets a mask for that MAC. The “any” option causes the rule to not check the destination MAC.
Default	No rule is added by default to access control list. Default sequence number is in multiple of 10.	
Configuration Mode	Config IPv4 ACL	
History	3.1.1400	First version
	3.3.4302	Updated syntax description of mask <ip> parameter
Role	admin	
Example	switch (config ipv4 access-list my-list) # seq-number 51 deny ip 1.1.1.1 mask 123.12.13.53 45.45.45.0 mask 123.132.21.123 switch (config ipv4 access-list my-list) #	
Related Commands	ipv4/mac access-list ipv4/mac port access-group	
Note		

deny/permit (IPv4 TCP/UDP ACL rule)

```
[seq-number <sequence-number>] {permit | deny} {tcp | udp} {<source-ip>
[mask <ip>] | [any]} {<dest-ip> [mask <ip>] | [any]} [eq-source <port-number>]
[eq-destination <port-number>] [action <action-id>]
no <sequence-number>
```

Creates a rule for IPv4 UDP/TCP ACL.

The no form of the command deletes a rule from the ACL.

Syntax Description	sequence-number	Optional parameter to set a specific sequence number for the rule. The range is:1-500.
	deny permit	Determines the type of the rule, deny or permit action.
	tcp udp	UDP or TCP rule transport type.
	{any <source-ip> [mask <ip>]}	Sets source IP and optionally sets a mask for that IP address. The “any” option will cause the rule not to check the source IP.
	{any <destination-ip> [mask <ip>]}	Sets destination IP and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the destination MAC.
	[eq-source <port-number>]	TCP/UDP source port number. Range is 0-65535.
	[eq-destination <port-number>]	TCP/UDP destination port number. Range is 0-65535.
Default	No rule is added by default to access control list. Default sequence number is in multiple of 10.	
Configuration Mode	Config IPv4 ACL	
History	3.1.1400	
Role	admin	
Example	switch (config ipv4 access-list my-list) # seq-number 10 deny tcp any any eq-source 1200 switch (config ipv4 access-list my-list) #	
Related Commands	ipv4/mac access-list ipv4/mac port access-group	
Note		

access-list action

access-list action <action-profile-name>

no access-list action <action-profile-name>

Creates access-list action profile and entering the action profile configuration mode.
The no form of the command deletes the action profile.

Syntax Description	action-profile-name	given name for the profile.
Default	N/A	
Configuration Mode	Config	
History	3.2.0230	
Role	admin	
Example	<pre>switch (config)# access-list action my-action switch (config access-list action my-action)# show access-list action my-action Access-list Action my-action Mapped_Vlan_ID Mapped_port Counter_set Policer_ID ===== N/A N/A N/A N/A switch (config access-list action my-action)#</pre>	
Related Commands		
Note		

vlan-map

vlan-map <vlan-id>

no vlan-map

Adds action to map a new VLAN to the packet (in the ingress port or VLAN).
The no form of the command removes the action to map a new VLAN.

Syntax Description	vlan-id	0-4095.
Default	N/A	
Configuration Mode	Config	
History	3.2.0230	
Role	admin	
Example	<pre>switch (config access-list action my-action)# vlan-map 10 switch (config access-list action my-action)# show access-list action my-action Access-list Action my-action Mapped_Vlan_ID Mapped_port Counter_set Policer_ID ===== 10 N/A N/A N/A switch (config access-list action my-action)#</pre>	
Related Commands		
Note		

show access-list action

show access-list action {<action-profile-name> | summary}

Displays the access-list action profiles summary.

Syntax Description	action-profile-name	Filter the table according to the action profile name.
	summary	Display summary of the action list.
Default	N/A	
Configuration Mode	Config	
History	3.2.0230	
Role	admin	
Example	<pre> switch (config access-list action my-action)# show access-list action my-action Access-list Action my-action Mapped_Vlan_ID Mapped_port Counter_set Policer_ID ===== 10 N/A N/A N/A switch (config access-list action my-action)# </pre>	
Related Commands		
Note		

show mac/ipv4 access-lists

show [mac | ipv4 |] access-lists <access-list-name>

Displays the list of rules for the MAC/IPv4 ACL.

Syntax Description	ipv4 mac	IPv4 or MAC - access list.
	access-list-name	ACL name.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
History	3.3.4500	Updated output
Role	admin	
Example	<pre>switch (config mac access-list my-list) # show mac access-lists my-list mac access-list my-list seq-number p/d smac dmac protocol cos vlan vlan-mask action ===== 10 deny any any 0800 3 3 0x0FFF none 20 deny any any 80 2 6 0x0000 none 30 deny any any any any any 0x0ACB none 40 deny any any any any any N/A none switch (config mac access-list my-list) #</pre>	
Related Commands	deny/permit (MAC ACL rule) deny/permit (IPv4 ACL rule) deny/permit (IPv4 TCP/UDP ACL rule) ipv4/mac access-list ipv4/mac port access-group	
Note		

show mac/ipv4 access-lists summary

show [mac |ipv4 |] access-lists summary

Displays the summary of number of rules per ACL, and the interfaces attached.

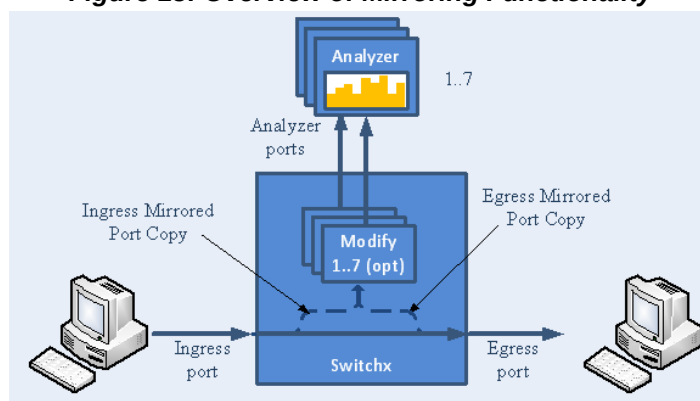
Syntax Description	ipv4 mac	IPv4 or MAC - Access list
	access-list-name	ACL name
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.1400	
Role	admin	
Example	<pre>switch (config) # show mac access-lists summary mac access-list my-list Total ACES Configured: 2 Configured on interfaces: Ethernet 1/1 Ethernet 1/2 switch (config) #</pre>	
Related Commands	<pre>deny/permit (MAC ACL rule) deny/permit (IPv4 ACL rule) deny/permit (IPv4 TCP/UDP ACL rule) ipv4/mac access-list ipv4/mac port access-group</pre>	
Note		

5.11 Port Mirroring

Port mirroring enables data plane monitoring functionality which allows the user to send an entire traffic stream for testing. Port mirroring sends a copy of packets of a port's traffic stream, called "mirrored port", into an analyzer port. Port mirroring is used for network monitoring. It can be used for intrusion detection, security breaches, latency analysis, capacity and performance matters, and protocol analysis.

Figure 13 provides an overview of the mirroring functionality.

Figure 13: Overview of Mirroring Functionality

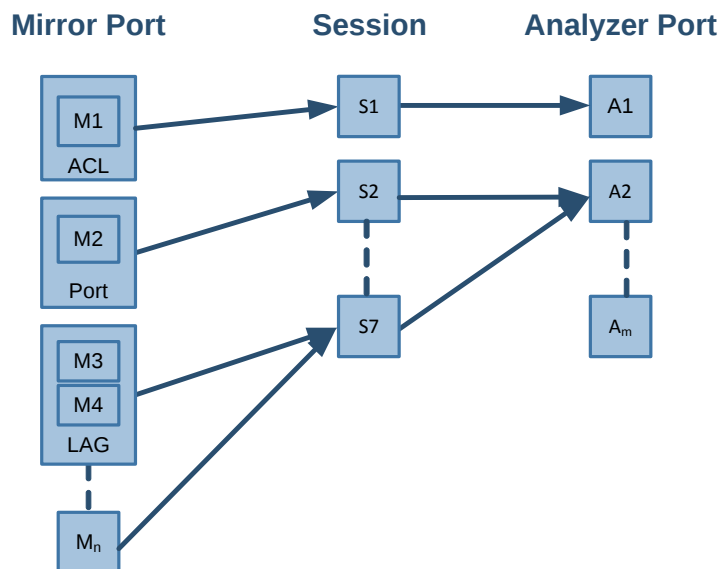


There is no limitation on the number of mirroring sources and more than a single source can be mapped to a single analyzer destination.

5.11.1 Mirroring Sessions

Port mirroring is performed by configuring mirroring sessions. A session is an association of a mirror port (or more) and an analyzer port.

Figure 14: Mirror to Analyzer Mapping



A mirroring session is a monitoring configuration mode that has the following parameters:

Table 41 - Mirroring Parameters

Parameter	Description	Access
Source interface(s)	List of source interfaces to be mirrored.	RW
Destination interface	A single analyzer port through which all mirrored traffic egress.	RW
Header format	The format and encapsulation of the mirrored traffic when sent to analyzer.	RW
Truncation	Enabling truncation segments each mirrored packet to 64 bytes.	RW
Congestion control	Controls the behavior of the source port when destination port is congested.	RW
Admin state	Administrative state of the monitoring session.	RW

5.11.1.1 Source Interface

The source interface (mirror port) refers to the interface from which the traffic is monitored. Port mirroring does not affect the switching of the original traffic. The traffic is simply duplicated and sent to the analyzer port. Traffic in any direction (either ingress, egress or both) can be mirrored.

There is no limitation on the number of the source interfaces mapped to a mirroring session.



Ingress and egress traffic flows of a specific source interface can be mapped to two different sessions.

LAG

The source interface can be a physical interface or a LAG.

Port mirroring can be configured on a LAG interface but not on a LAG member. When a port is added to a mirrored LAG it inherits the LAG's mirror configuration. However, if port mirroring configuration is set on a port, that configuration must be removed prior to adding the port to a LAG interface.

When a port is removed from a LAG, the mirror property is switched off for that port.

Control Protocols

All control protocols captured on the mirror port are forwarded to the analyzer port in addition to their normal treatment. For example LACP, STP, and LLDP are forwarded to the analyzer port in addition to their normal treatment by the CPU.

Exceptions to the behavior above are the packets that are being handled by the MAC layer, such as pause frames.

5.11.1.2 Destination Interface

The destination interface is an analyzer port is one to which mirrored traffic is sent. The mirrored packets, are duplicated, optionally modified and sent to the analyzer port. The SwitchX® platform supports up to 7 analyzer ports where any mirror port can be mapped to any analyzer port and more than a single mirror port can be mapped to a single analyzer port.

Packets can be forwarded to any destination using the command `destination interface`.
The analyzer port supports status and statistics as any other port.

LAG

The destination interface cannot be a member of LAG when the header format is local.

Control Protocols

The destination interface may also operate in part as a standard port, receiving and sending out non-mirrored traffic. When the header format is configured as a local port, ingress control protocol packets that are received by the local analyzer port get discarded.

Advanced MTU Considerations

The analyzer port, like its counterparts, is subject to MTU configuration. It does not send packets longer than configured.

When the analyzer port sends encapsulated traffic, the analyzer traffic has additional headers and therefore longer frame. The MTU must be configured to support the additional length, otherwise, the packet is truncated to the configured MTU.

The system on the receiving end of the analyzer port must be set to handle the egress traffic. If it is not, it might discard it and indicate this in its statistics (packet too long).

5.11.1.3 Header Format

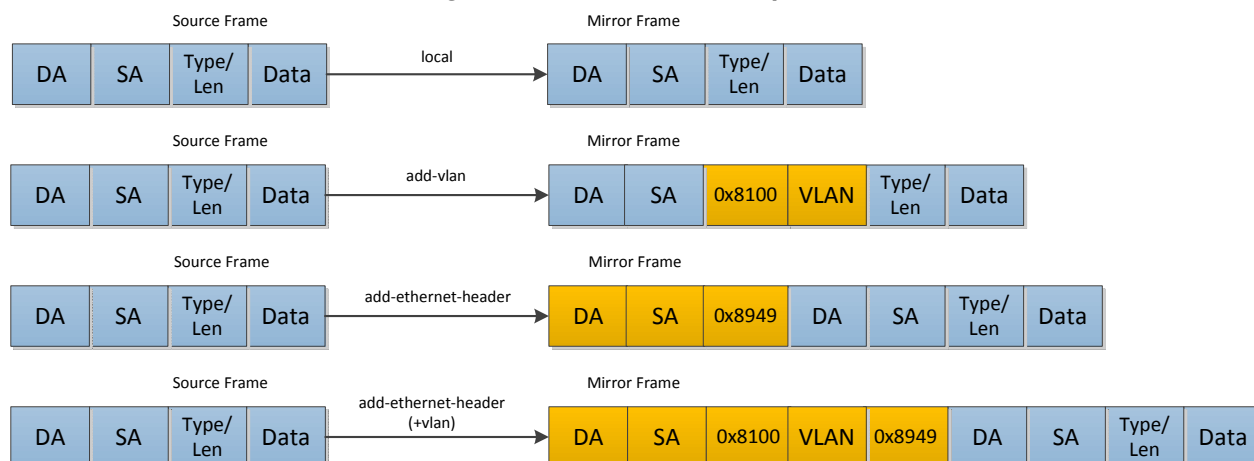
Ingress traffic from the source interface can be manipulated in several ways depending on the network layout using the command `header -format`.

If the analyzer system is directly connected to the destination interface, then the only parameters that can be configured on the port are the MTU, speed and port based flow control. Priority flow control is not supported in this case. However, if the analyzer system is indirectly connected to the destination interface, there are two options for switching the mirrored data to the analyzer system:

- A VLAN tag may be added to the Ethernet header of the mirrored traffic
- An Ethernet header can be added with include a new destination address and VLAN tag



It must be taken into account that adding headers increases packet size.

Figure 15: Header Format Options

5.11.1.4 Congestion Control

The destination ports might receive pause frames that lead to congestion in the switch port. In addition, too much traffic directed to the analyzer port (for example 40GbE mirror port is directed into 10G analyzer port) might also lead to congestion.

In case of congestion:

- When best effort mode is enabled on the analyzer port, SwitchX drops excessive traffic headed to the analyzer port using tail drop mechanism, however, the regular data (mirrored data heading to its original port) does not suffer from a delay or drops due to the analyzer port congestion.
- When the best effort mode on the analyzer port is disabled, the SwitchX does not drop the excessive traffic. This might lead to buffer exhaustion and data path packet loss.

The default behavior in congestion situations is to drop any excessive frames that may clog the system.



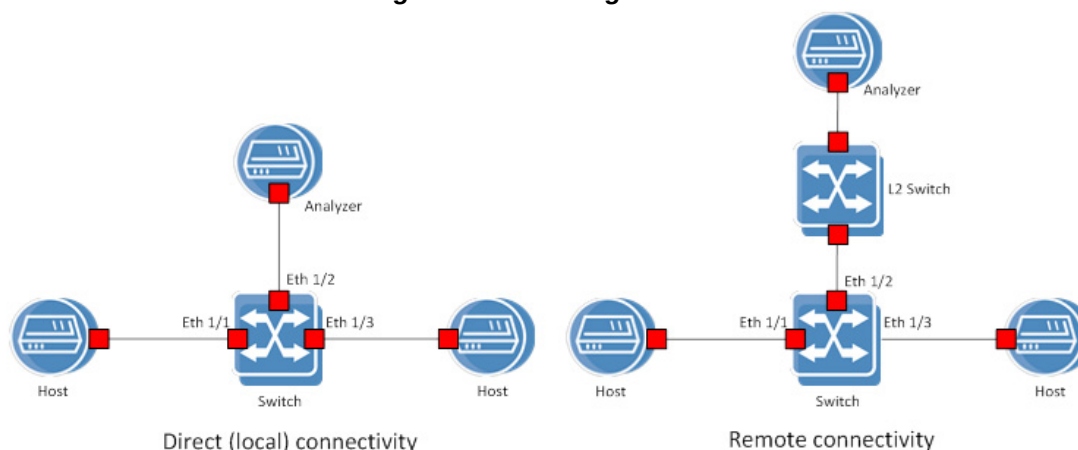
ETS, PFC and FC configurations do not apply to the destination port.

5.11.1.5 Truncation

When enabled, the system can truncate the mirrored packets into smaller 64-byte packets (default) which is enough to capture the packets' L2 and L3 headers.

5.11.2 Configuring Mirroring Sessions

Figure 16 presents two network scenarios with direct and remote connectivity to the analyzer equipment. Direct connectivity is when the analyzer is connected to the analyzer port of the switch. In this case there is no need for adding an L2 header to the mirrored traffic. Remote connectivity is when the analyzer is indirectly connected to the analyzer port of the switch. In this situation, adding an L2 header may be necessary depending on the network's setup.

Figure 16: Mirroring Session

➤ **To configure a mirroring session:**

Step 1. Create a session. Run:

```
switch (config) # monitor session 1
```



This command enters a monitor session configuration mode. Upon first implementation the command also creates the session.

Step 2. Add source interface(s). Run:

```
switch (config monitor session 1) # add source interface ethernet 1/1 direction both
```

Step 3. Add destination interface. Run:

```
switch (config monitor session 1) # destination interface ethernet 1/2
```

Step 4. (Optional) Set header format. Run:

```
switch (config monitor session 1) # header-format add-ethernet-header destination-mac  
00:0d:ec:f1:a9:c8 add-vlan 10 priority 5 traffic-class 2
```



For remote connectivity use the header formats add-vlan or add-ethernet-header. For local connectivity, use local.

Step 5. (Optional) Truncate the mirrored traffic to 64-byte packets. Run:

```
switch (config monitor session 1) # truncate
```

Step 6. (Optional) Set congestion control. Run:

```
switch (config monitor session 1) # congestion pause-excessive-frames
```



The default for this command is to drop excessive frames. The pause-excessive-frames option uses flow control to regulate the traffic from the source interfaces.



If the option `pause-excessive-frame` is selected, make sure that flow control is enabled on **all** source interfaces on the ingress direction of the monitoring session using the command `flowcontrol` in the interface configuration mode.

Step 7. Enable the session. Run:

```
switch (config monitor session 1) # no shutdown
```

5.11.3 Verifying Mirroring Sessions

➤ **To verify the attributes of a specific mirroring session:**

```
switch (config) # show monitor session 1
Admin: Enable
Status: Up
Truncate: Enable
Destination interface: eth1/2
Congestion type: pause-excessive-frames
Header format: add-ethernet-header
                - traffic class 2
                - vlan 10
                - priority 5
                - destination-mac 00:0d:ec:f1:a9:c8

Source interfaces
Interface  direction
-----
eth1/1    both
```

➤ **To verify the attributes of running mirroring sessions:**

```
switch (config) # show monitor session summary
```

Session	Admin	Status	Mode	Destination	Source
1	Enable	Up	add-eth	eth1/2	eth1/1(b)
2	Disable	Down	add-vlan	eth1/2	eth1/8(i), po1(e)
3	Enable	Up	add-eth	eth1/5	eth1/18(e)
7	Disable	Down	local		

5.11.4 Commands

5.11.4.1 Config

monitor session

monitor session <session-id>
no monitor session <session-id>

Creates session and enters monitor session configuration mode upon using this command for the first time.
The no form of the command deletes the session.

Syntax Description	session-id	The monitor session ID. The range is 1-7.
Default	N/A	
Configuration Mode	Config	
History	3.3.3500	
Role	admin	
Example	switch (config)# monitor session 1 switch (config monitor session 1)#	
Related Commands		
Note		

5.11.4.2 Config Monitor Session

destination interface

destination interface <type> <number> [force]
no destination interface

Sets the egress interface number.
 The no form of the command deletes the destination interface.

Syntax Description	interface <type> <number>	Sets the interface type and number (e.g. ethernet 1/2)
	force	The user does not need to shutdown the port prior the operation.
Default	no destination interface	
Configuration Mode	Config Monitor Session	
History	3.3.3500	Initial version
	3.3.4100	Added force argument
Role	admin	
Example	switch (config monitor session 1) # destination interface ethernet 1/2 switch (config monitor session 1)#	
Related Commands		
Note		

shutdown

shutdown
no shutdown

Disables the session.
 The no form of the command enables the session.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config Monitor Session
History	3.3.3500
Role	admin
Example	switch (config monitor session 1) # no shutdown switch (config monitor session 1)#
Related Commands	
Note	

add source interface

add source interface <type> <number> **direction** <d-type>

no source interface <type> <number>

Adds a source interface to the mirrored session.

The no form of the command deletes the source interface.

Syntax Description	interface <type> <number>	Configures interface as “ethernet” or “port-channel”.
	direction <d-type>	Configures the direction of the mirrored traffic. The options are as follows: • egress – sets the egress traffic to be monitored • ingress – sets the ingress traffic to be monitored • both – sets egress and ingress traffic to be monitored
Default	N/A	
Configuration Mode	Config Monitor Session	
History	3.3.3500	
Role	admin	
Example	<pre>switch (config monitor session 1) # add source interface ethernet 1/1 direction both switch (config monitor session 1)#</pre>	
Related Commands		
Note	If mirroring is configured in one direction (e.g. ingress) on an interface and then is configured in the other direction (e.g. egress), then the ultimate setting is “both”.	

header-format

header-format {local [traffic-class <tc>] | add-vlan <vlan-id> [priority <prio>]
[traffic-class <tc>] | add-ethernet-header destination-mac <mac-address> [add-
vlan <vlan-id> [priority <prio>]] [traffic-class <tc>]}
no header-format

Sets the header format of the mirrored traffic.

The no form of the command resets the parameter values back to default.

Syntax Description	local	The mirrored header of the frame is not changed.
	traffic-class <tc>	Changes the egress traffic class of the frame. Range is 0-3.
	add-vlan <vlan-id>	An 802.1q VLAN tag is added to the frame.
	priority <prio>	The priority to be added to the Ethernet header. Range is 0-7.
	add-ethernet-header	Adds an Ethernet header to the mirrored frame.
	destination-mac	The destination MAC address of the added Ethernet frame.
Default	no-change vlan 1 priority 0 traffic-class 0	
Configuration Mode	Config Monitor Session	
History	3.3.3500	
Role	admin	
Example	switch (config monitor session 1) # header-format add-ethernet-header destination-mac 00:0d:ec:f1:a9:c8 add-vlan 10 priority 5 traffic-class 2 switch (config monitor session 1)#	
Related Commands		
Note	If add-ethernet-header is used, the source MAC address is the one attached to the switch.	

truncate

truncate
no truncate

Truncates the mirrored frames to 64-byte packets.
The no form of the command disables truncation.

Syntax Description	N/A
Default	no truncate
Configuration Mode	Config Monitor Session
History	3.3.3500
Role	admin
Example	<pre>switch (config monitor session 1) # truncate switch (config monitor session 1)#</pre>
Related Commands	
Note	This command applies for all sessions on the same analyzer port.

congestion

congestion [drop-excessive-frames | pause-excessive-frames]
no congestion

Sets the system's behavior when congested
 The no form of the command disables truncation.

Syntax Description	drop-excessive-frames	Drops excessive frames.
	pause-excessive-frames	Pauses excessive frames.
Default	drop-excessive-frames	
Configuration Mode	Config Monitor Session	
History	3.3.3500	
	3.3.4000	Added Syntax Description.
Role	admin	
Example	<pre>switch (config monitor session 1) # congestion pause-excessive-frames switch (config monitor session 1)#</pre>	
Related Commands		
Note	This command applies for all sessions on the same analyzer port.	

5.11.4.3 Show

show monitor session

show monitor session <session-id>

Displays monitor session configuration and status.

Syntax Description	session-id	The monitor session ID. Range is 1-7.
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.3.3500	
Role	admin	
Example	<pre>switch (config) # show monitor session 1 Admin: Enable Status: Up Truncate: Enable Destination interface: eth1/2 Congestion type: pause-excessive-frames Header format: add-ethernet-header - traffic class 2 - vlan 10 - priority 5 - destination-mac 00:0d:ec:f1:a9:c8 Source interfaces Interface direction ----- eth1/1 both switch (config) #</pre>	
Related Commands		
Note		

show monitor session summary

show monitor session summary

Displays monitor session configuration and status summary.

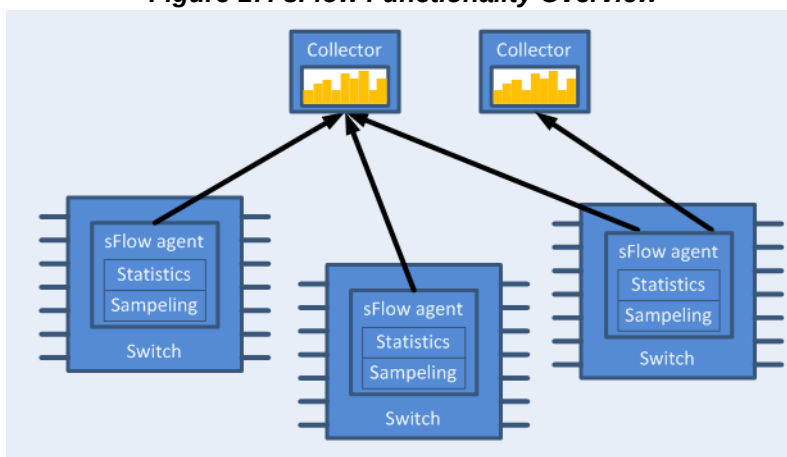
Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.3500
Role	admin
Example	<pre>switch (config) # show monitor session summary Session Admin Status Mode Destination Source 1 Enable Up add-eth eth1/2 eth1/1(b) 2 Disable Down add-vlan eth1/2 eth1/8(i), po1(e) 3 Enable Up add-eth eth1/5 eth1/18(e) 7 Disable Down local switch (config) #</pre>
Related Commands	
Note	

5.12 sFlow

sFlow (ver. 5) is a procedure for statistical monitoring of traffic in networks. MLNX-OS supports an sFlow sampling mechanism (agent), which includes collecting traffic samples and data from counters. The sFlow datagrams are then sent to a central collector.

The sampling mechanism must ensure that any packet going into the system has an equal chance of being sampled, irrespective of the flow to which it belongs. The sampling mechanism provides the collector with periodical information on the amount (and load) of traffic per interface by loading the counter samples into sFlow datagrams.

The sFlow packets are encapsulated and sent in UDP over IP. The UDP port number that is used is the standard 6343 by default.

Figure 17: sFlow Functionality Overview

5.12.1 Flow Samples

The sFlow agent samples the data path packet based.

Truncation and sampling rate are the two parameters that influence the flow samples. In case of congestion the flow samples can be truncated to a predefined size before it is being assigned to the CPU. The truncation can be set to any value between 64 to 256 bytes with the default being 128 bytes. Furthermore, the sampling rate may also be adjust as required.

5.12.2 Statistical Samples

The sFlow agent samples interface counters time based. Polling interval is configurable to any value between 5-3600 seconds with the default being 20 seconds.

The following statistics are gathered by the CPU:

Table 42 - List of Statistical Counters

Counter	Description
Total packets	The number of packets that pass through sFlow-enabled ports.
Number of flow samples	The number of packets that are captured by the sampling mechanism.
Number of statistic samples	The number of statistical samples.
Number of discarded samples	The number of samples that were discarded.
Number of datagrams	The number of datagrams that were sent to the collector.

5.12.3 sFlow Datagrams

The sFlow datagrams contain flow samples and statistical samples.

The sFlow mechanism uses IP protocol, therefore if the packet length is more than the interface MTU, it becomes fragmented by the IP stack. The MTU may also be set manually to anything in the range of 200-9216 bytes. The default is 1400 bytes.

5.12.4 Sampled Interfaces

sFlow must be enabled on physical or LAG interfaces that require sampling. When adding a port to a LAG, sFlow must be disabled on the port. If a port with enabled sFlow is configured to be added to a LAG, the configuration is rejected. Removing a port from a LAG disables sFlow on the port regardless of the LAG's sFlow status.

5.12.5 Configuring sFlow

➤ *To configure the sFlow agent:*

Step 1. Unlock the sFlow commands. Run:

```
switch (config) # protocol sflow
```

Step 2. Enable sFlow on the system. Run:

```
switch (config) # sflow enable
```

Step 3. Enter sFlow configuration mode. Run:

```
switch (config) # sflow
switch (config sflow) #
```

Step 4. Set the central collector's IP. Run:

```
switch (config sflow) # collector-ip 10.10.10.10
```

Step 5. Set the agent-ip used in the sFlow header. Run:

```
switch (config sflow) # agent-ip 20.20.20.20
```

Step 6. (Optional) Set the sampling rate of the mechanism. Run:

```
switch (config sflow) # sampling-rate 16000
```



This means that one every 16000 packet gets collected for sampling.

Step 7. (Optional) Set the maximum size of the data path sample. Run:

```
switch (config sflow) # max-sample-size 156
```

Step 8. (Optional) Set the frequency in which counters are polled. Run:

```
switch (config sflow) # counter-poll-interval 19
```

Step 9. (Optional) Set the maximum size of the datagrams sent to the central collector. Run:

```
switch (config sflow) # max-datagram-size 1500
```

Step 10. Enable the sFlow agent on the desired interfaces. Run:

```
switch (config interface ethernet 1/1) # sflow enable
switch (config interface port-channel 1) # sflow enable
```

5.12.6 Verifying sFlow

➤ *To verify the attributes of the sFlow agent:*

```
switch (config)# show sflow

sflow protocol enabled
sflow enabled
sampling-rate 16000
max-sampled-size 156
counter-poll-interval 19
max-datagram-size 1500
collector-ip 10.10.10.10
collector-port 6343
agent-ip 20.20.20.20

Interfaces
Ethernet: eth1/1
Port-channel: po1

Statistics:
Total Packets: 2000
Number of flow samples: 1200
Number of samples discarded: 0
Number of statistic samples: 800
Number of datagrams: 300
```

5.12.7 Commands

5.12.7.1 Config

protocol sflow

protocol sflow
no protocol sflow

Unhides the sFlow commands.
The no form of the command deletes sFlow configuration and hides the sFlow commands.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.3500
Role	admin
Example	switch (config) # protocol sflow switch (config) #
Related Commands	
Note	

sflow enable (global)

sflow enable
no sflow enable

Enables sFlow in the system.
The no form of the command disables sFlow without deleting the configuration.

Syntax Description	N/A
Default	Disabled
Configuration Mode	Config
History	3.3.3500
Role	admin
Example	switch (config) # sflow enable switch (config) #
Related Commands	
Note	

sflow

sflow

Enters sFlow configuration mode.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.3.3500
Role	admin
Example	switch (config) # sflow switch (config sflow) #
Related Commands	
Note	

5.12.7.2 Config sFlow

sampling-rate

sampling-rate <rate>
no sampling-rate

Sets sFlow sampling ratio.
The no form of the command resets this parameter to its default value.

Syntax Description	rate	Sets the number of packets passed before selecting one for sampling. The range is 4000-16777215. Zero disables sampling.
Default	16000	
Configuration Mode	Config sFlow	
History	3.3.3500	
Role	admin	
Example	switch (config sflow) # sampling-rate 16111 switch (config sflow) #	
Related Commands		
Note		

max-sample-size

max-sample-size <packet-size>
no max-sample-size

Sets the maximum size of sampled packets by sFlow.
 The no form of the command resets the parameter to its default value.

Syntax Description	packet-size	The sampled packet size. The range is 64-256 bytes.
Default	128 bytes	
Configuration Mode	Config sFlow	
History	3.3.3500	
Role	admin	
Example	switch (config sflow) # max-sample-size 165 switch (config sflow) #	
Related Commands		
Note	Sampled payload beyond the configured size is discarded.	

counter-poll-interval

counter-poll-interval <seconds>

no counter-poll-interval

Sets the sFlow statistics polling interval.

The no form of the command resets the parameter to its default value.

Syntax Description	seconds	The sFlow statistics polling interval in seconds. Range is 5-3600 seconds. Zero disables the statistic polling.
Default	20 seconds	
Configuration Mode	Config sFlow	
History	3.3.3500	
Role	admin	
Example	switch (config sflow) # counter-poll-interval 30 switch (config sflow) #	
Related Commands		
Note		

max-datagram-size

max-datagram-size <packet-size>
no max-datagram-size

Sets the maximum sFlow packet size to be sent to the collector.
 The no form of the command resets the parameter to its default value.

Syntax Description	packet-size	The packet size of the packet being sent to the collector. The range is 200-9216 bytes.
Default	1400 bytes	
Configuration Mode	Config sFlow	
History	3.3.3500	
Role	admin	
Example	switch (config sflow) # max-datagram-size 9216 switch (config sflow) #	
Related Commands		
Note	This packet contains the data sample as well as the statistical counter data.	

collector-ip

collector-ip <ip-address> [udp-port <udp-port-number>]
no collector-ip [<ip-address> udp-port]

Sets the collector's IP.

The no form of the command resets the parameters to their default values.

Syntax Description	ip-address	The collector IP address.
	udp-port <udp-port-number>	Sets the collector UDP port number.
Default	ip-address: 0.0.0.0 udp-port-number: 6343	
Configuration Mode	Config sFlow	
History	3.3.3500	
Role	admin	
Example	switch (config sflow) # collector-ip 10.10.10.10 switch (config sflow) #	
Related Commands		
Note		

agent-ip

agent-ip {<ip-address> | **interface** {<if-name> | **vlan** <id> | **loopback** <number>}}

no agent-ip

Sets the IP address associated with this agent.

The no form of the command resets the parameters to their default values.

Syntax Description	loopback <number>	Loopback interface. The range is 1-32.
	if-name	Interface name (e.g. mgmt0, mgmt1).
	vlan <id>	Interface VLAN. Range is 1-4094
	ip-address	The sFlow agent's IP address (i.e. the source IP of the packet).
Default	ip-address: 0.0.0.0	
Configuration Mode	Config sFlow	
History	3.3.3500	
Role	admin	
Example	<pre>switch (config sflow) # agent-ip 20.20.20.20 switch (config sflow) #</pre>	
Related Commands		
Note	The IP address here is used in the sFlow header.	

clear counters

clear counters

Clears sFlow counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Config sFlow
History	3.3.3500
Role	admin
Example	switch (config sflow) # clear counters switch (config sflow) #
Related Commands	
Note	

sflow enable (interface)

sflow enable
no sflow enable

Enables sFlow on this interface.
 The no form of the command disables sFlow on the interface.

Syntax Description	N/A
Default	disable no view-port-channel member
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel
History	3.3.3500 3.3.4500 Added MLAG port-channel configuration mode
Role	admin
Example	switch(config interface ethernet 1/1)# sflow enable ... switch(config interface port-channel 1)# sflow enable
Related Commands	
Note	

5.12.7.3 Show

show sflow

show sflow

Displays sFlow configuration and counters.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any Command Mode
History	3.3.3500
Role	admin
Example	<pre>switch (config)# show sflow sflow protocol enabled sflow enabled sampling-rate 16000 max-sampled-size 156 counter-poll-interval 19 max-datagram-size 1500 collector-ip 10.10.10.10 collector-port 6343 agent-ip 20.20.20.20 Interfaces Ethernet: eth1/1 Port-channel: po1 Statistics: Total Packets: 2000 Number of flow samples: 1200 Number of samples discarded: 0 Number of statistic samples: 800 Number of datagrams: 300</pre>
Related Commands	
Note	

Appendix A: Strict Security Mode

A.1 Overview

Strict mode is a security state of a system complying with the NIST SP 800-131A standard. Because of compatibility issues, strict mode is not the default state of the system and it should be manually set. Strict mode is based on NIST SP 800-131A document which defines cryptographically “acceptable” technologies. This document explains how to configure possible cryptographic vulnerabilities in the system to use secure technologies.



Some protocols, however, cannot be operated in a manner that complies with the 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
<password2>
```

- **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.

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 secure 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 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:

- 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 HTTPS strict mode, run:**

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

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

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

- **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 difference 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)
root	Root User	admin	No password required for login
xmladmin	XML Admin User	admin	No password required for login
xmluser	XML Monitor User	monitor	No password required for login

When moving to strict mode, each switch username must be recreated manually using the 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)