



Mellanox MLNX-OS® User Manual for *IBM SX90Y3452*

Rev 1.6.6

Software Version 3.3.3706

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 2013. Mellanox Technologies. All Rights Reserved.

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

Connect-IB™, FabricIT™, Mellanox Open Ethernet™, Mellanox Virtual Modular Switch™, MetroX™, MetroDX™, ScalableHPC™, Unbreakable-Link™ are trademarks of Mellanox Technologies, Ltd.

All other trademarks are property of their respective owners.

Table of Contents

Document Revision History	5
About this Manual	6
Intended Audience	6
Related Documentation	6
Glossary	7
Chapter 1 Introduction	9
1.1 MLNX-OS Features	9
Chapter 2 Getting Started	11
2.1 Configuring the Switch for the First Time	11
2.2 Starting the Command Line (CLI)	11
2.3 Starting the Web Interface	12
2.4 Licenses	14
2.4.1 Installing MLNX-OS® License (CLI)	15
2.4.2 Installing MLNX-OS License (Web)	15
2.4.3 Retrieving a Lost License Key	18
Chapter 3 User Interfaces	19
3.1 Command Line Interface (CLI)	19
3.1.1 CLI Modes	19
3.1.2 Syntax Conventions	20
3.1.3 Getting Help	20
3.1.4 Prompt and Response Conventions	21
3.1.5 Using the “no” Form	22
3.1.6 Parameter Key	23
3.2 Web Interface	24
3.2.1 Setup Menu	25
3.2.2 System Menu	26
3.2.3 Security Menu	27
3.2.4 Ports Menu	27
3.2.5 Status Menu	28
3.2.6 IB SM Mgmt	29
3.2.7 Fabric Inspector	29
3.2.8 ETH Mgmt	30
Chapter 4 System Management	31
4.1 Management Interface	31
4.1.1 Configuring Management Interfaces with Static IP Addresses	31
4.1.2 Configuring IPv6 Address on the Management Interface	31
4.1.3 Dynamic Host Configuration Protocol (DHCP)	31
4.1.4 Default Gateway	32
4.2 Unbreakable Links	32
4.2.1 Link Level Retransmission (LLR)	32
4.2.2 Configuring Phy Profile & LLR	33

4.3	Software Management	34
4.3.1	Upgrading MLNX-OS Software - Preconditions	34
4.3.2	Upgrading MLNX-OS® Software	35
4.3.3	Deleting Unused Images	38
4.3.4	Downgrading MLNX-OS Software	39
4.3.5	Upgrading System Firmware	42
4.4	File Management	43
4.4.1	Saving a Configuration File	43
4.4.2	Loading a Configuration File	43
4.4.3	Restoring Factory Default Configuration on a Switch System (Single Management Module).....	44
4.5	Remote Logging	44
4.5.1	Configuring Remote Syslog to “info” Level.....	44
4.6	Event Notifications	44
4.6.1	E-mail Notifications	44
4.7	Diagnostics	45
4.7.1	Retrieving Return Codes when Executing Remote Commands	46
4.8	User Management and Security.....	46
4.8.1	Authentication, Authorization and Accounting (AAA)	46
4.8.2	Secure Shell (SSH)	48
4.8.3	User Accounts.....	49
4.9	Network Management Interfaces.....	49
4.9.1	SNMP	49
4.9.2	MLNX-OS XML API.....	56

Document Revision History

Table 1 - Document Revision History - InfiniBand

Document Revision	Date	Changes
Rev 1.6.6	Apr 2013	Added Section 4.9.1.4, "Traps and Events Mapping," on page 52.
Rev 1.6.3	Jan 2013	Updated Section 4.2, "Unbreakable Links," on page 32.
Rev. 1.6.1	Nov. 2012	Added Section 3.2.4, "Ports Menu," on page 27.
Rev. 1.5.2	June 2012	Updated Section 4.9.1, "SNMP," on page 49. Added Phy section.
Rev 1.5	May 2012	Initial release.

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.
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
MLNX-OS® Command Reference Guide	Command Reference Guide for MLNX-OS listing all of the commands available through MLNX-OS with explanations and examples.

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
DHCP	The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks.
DNS	Domain Name System. A hierarchical naming system for devices in a computer network
FTP/TFTP/sFTP	File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another over a TCP-based network, such as the Internet.
Gateway	A network node that interfaces with another network using a different network protocol
HA (High Availability)	A system design protocol that provides redundancy of system components, thus enables overcoming single or multiple failures in minimal downtime
Host	A computer platform executing an Operating System which may control one or more network adapters
LDAP	The Lightweight Directory Access Protocol is an application protocol for reading and editing directories over an IP network.
MAC	A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies including Ethernet.
MTU (Maximum Transfer Unit)	The maximum size of a packet payload (not including headers) that can be sent /received from a port
Network Adapter	A hardware device that allows for communication between computers in a network
RADIUS	Remote Authentication Dial In User Service. A networking protocol that enables AAA centralized management for computers to connect and use a network service.
RDMA (Remote Direct Memory Access)	Accessing memory in a remote side without involvement of the remote CPU
SA (Subnet Administrator)	The interface for querying and manipulating subnet management data

Table 3 - Glossary

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

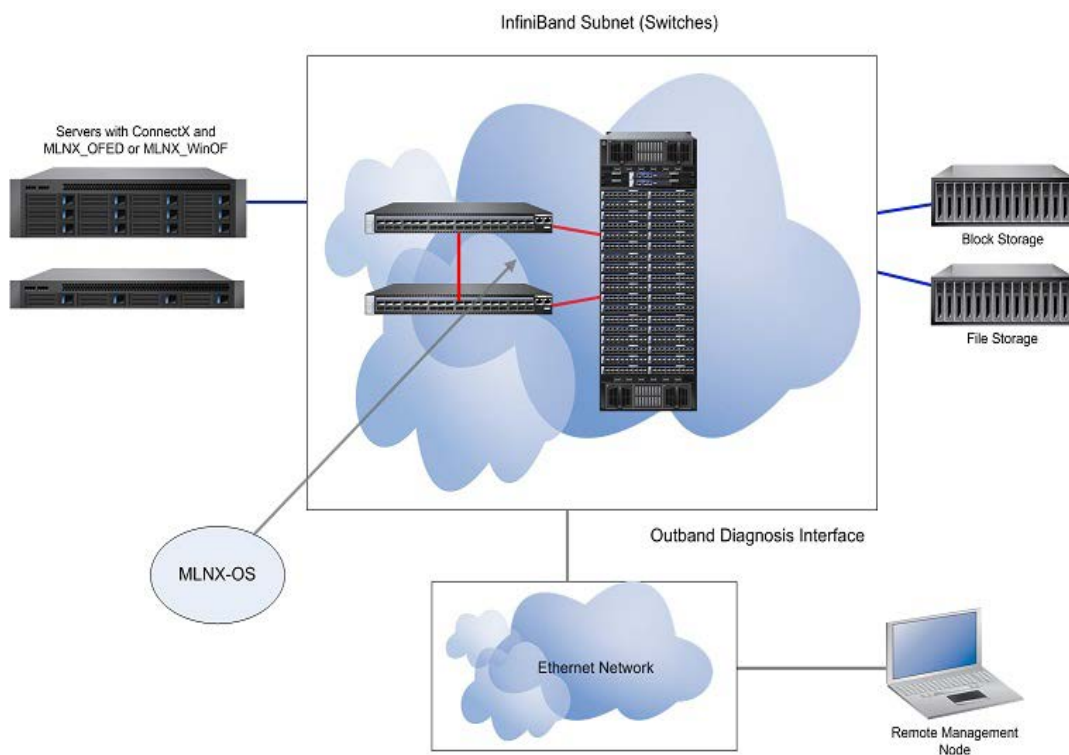
Mellanox® Operating System (MLNX-OS®) enables the management and configuration of Mellanox Technologies' SwitchX® silicon based switch platforms. MLNX-OS supports the Virtual Protocol Interconnect (VPI) technology which enables it to be used for both Ethernet and InfiniBand technology providing the user 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. In addition, it incorporates a familiar industry-standard CLI, which enables administrators to easily configure and manage the system.

1.1 MLNX-OS 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

Figure 1: Managing an InfiniBand Software Using MLNX-OS

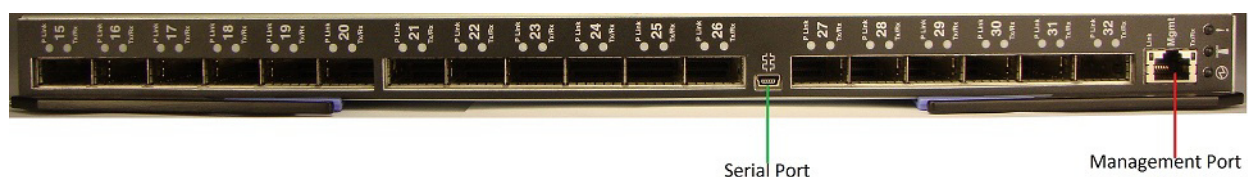
2 Getting Started

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

2.1 Configuring the Switch for the First Time

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 5 - Serial Terminal Program Configuration

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>

Mellanox MLNX-OS Switch Management

Last login: Thu Apr 28 11:24:13 2011 from 192.168.10.1
Mellanox Switch

switch >
```

- Step 3.** Login to the switch (default username is *admin*, password *admin*)
- Step 4.** Once you get the prompt, you are ready to use the system. Refer to *MLNX-OS Command Reference Guide* for additional information on the CLI commands.

2.3 Starting the Web 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*).

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

Figure 3: MLNX-OS Login Window

Mellanox TECHNOLOGIES

Mellanox MLNX-OS Management Console

Host: switch-5ea580 User: (not logged in) Login

Setup System Security Ports Status JB SM MGMT Fabric Inspector ETH MGMT

Login

Please enter your username and password, then click "Login"

Account:

Password:

Login

Mellanox MLNX-OS Switch Management . Best viewed using Firefox, Chrome, IE 7 or higher at 1024x768 resolution or higher.

© 2009-2012 Mellanox Technologies, Inc.

After you log in to MLNX-OS, a (default) status summary window will be displayed containing the following information:

Figure 4: Display After Login

Mellanox TECHNOLOGIES

Mellanox MLNX-OS SX1016 Management Console

Host: switch-5e0aee User: admin Logout

Standalone

Setup System Security Ports Status VPI Cpbity VPI Cpbity ETH MGMT

Summary

Summary	Summary
System Capabilities	Date and Time: 2012/02/07 16:04:06
Temperature	Hostname: switch-5e0aee
Power Supplies	Uptime: 4h 36m 47s
Fans	Version: SX_PPC_M460EX 3.0.0000-dev-HA 2012-02-06 08:49:05 ppc
CPU Load	Model: ppc
Memory	Host ID: 0002c95e0aee
Network	System memory: 372 MB used / 1655 MB free / 2027 MB total
Logs	CPU load averages: 0.41 / 0.36 / 0.25
Maintenance	Active alerts
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 6 - MLNX-OS Licenses

OPN	Valid on product	Description
LIC-FDR10	SX1035/SX1036	InfiniBand FDR-10 SW license for Ethernet Switches
LIC-1035-L2	SX1035	Full Ethernet L2
LIC-6018-L2	SX6018	Full Ethernet L2
LIC-6036-L2	SX6036F/T	Full Ethernet L2
LIC-1016-L3	SX1016	Full Ethernet L3
LIC-1035-L3	SX1035	Full Ethernet L2 + L3
LIC-1036-L3	SX1036	Full Ethernet L3
LIC-1024-L3	SX1024	Full Ethernet L2 + L3
LIC-6036-L3	SX6036F/T	Full Ethernet L2 + L3
LIC-1024-56E	SX1024	Ethernet 56GE
LIC-1036-56E	SX1036	Ethernet 56GE
LIC-6036F-56GE	SX6036F	Ethernet 56GE
LIC-fabric-inspector	SX6036F/T / SX65XX	InfiniBand fabric inspector monitoring and health.
LIC-1036-GW	SX1036	L3 Ethernet + Gateway software license for Mellanox 1036 Series Ethernet Switch
LIC-6036-GW	SX6036	Full Ethernet L2 + L3 + Gateway software license for Mellanox 6036 Series Switch

If your switch system includes one or more internal management modules, then to activate extended MLNX-OS features you must install the license that was purchased along with the switch system.

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.

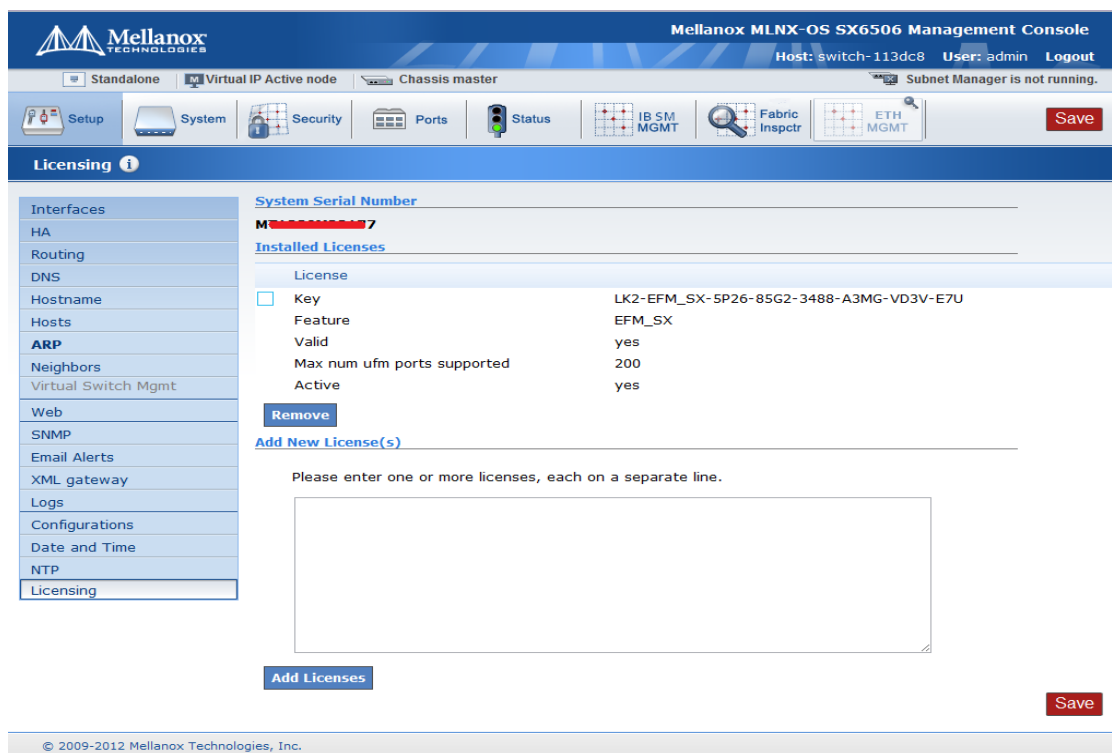
2.4.2 Installing MLNX-OS License (Web)

➤ *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 5: 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 Insctr 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 6: 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 7: 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 14.

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

3 User Interfaces

3.1 Command Line Interface (CLI)

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).

Refer to the *MLNX-OS Command Reference Guide* for complete set of commands, syntax and examples.

3.1.1 CLI Modes

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

Table 7 - CLI Modes and Config Context

Mode/Context	Description
Standard	When the CLI is launched, it begins in Standard mode. This is the most restrictive mode and only has commands to query a restricted set of state information. Users cannot take any actions that directly affect the system, nor can they change any configuration.
Enable	The <code>enable</code> 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 <code>configure terminal</code> 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 <code>exit</code> or <code>no configure</code> . Note that moving directly from/to Standard mode to/from Config mode is not possible.
Config Interface Management	Configuration mode for management interface <code>mgmt0</code> , <code>mgmt1</code> and loopback.
Config interface ethernet	Configuration mode for Ethernet interface.
Config Interface Port Channel	Configuration mode for Port channel (LAG).
Config Vlan	Configuration mode for VLAN.
Any Command Mode	Several commands such as “show” can be applied within any context.

3.1.2 Syntax Conventions

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

Table 8 - Syntax Conventions

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



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



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

3.1.3 Getting Help

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

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

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

```

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

```

If you type a legal string and then you 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”: c clear, c li and configure.)

3.1.4 Prompt and Response Conventions

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

```

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

```

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

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

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

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

3.1.5 Using the “no” Form

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

The following example performs the following:

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

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

```

Terminal length:      60 rows
Terminal type:        xterm
Auto-logout:         disabled
Paging:              enabled
Progress tracking:    enabled
Prefix modes:        enabled
...
// 4. Re-enable auto-logout after 15 minutes
switch (config) # cli session auto-logout 15
// 5. Display the final CLI session options
switch (config) # show cli
CLI current session settings:
Maximum line size:    8192
Terminal width:       157 columns
Terminal length:      60 rows
Terminal type:        xterm
Auto-logout:         15 minutes
Paging:              enabled
Progress tracking:    enabled
Prefix modes:        enabled
...

```

3.1.6 Parameter Key

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

Table 9 - Angled Brackets Parameter Description

Parameter	Description
<domain>	A domain name, e.g. “mellanox.com”.
<hostname>	A hostname, e.g. “switch-1”.
<ifname>	An interface name, e.g. “mgmt0”, “mgmt1”, “lo” (loopback), etc.
<index>	A number to be associated with aliased (secondary) IP addresses.
<IP address>	An IPv4 address, e.g. “192.168.0.1”.
<log level>	A syslog logging severity level. Possible values, from least to most severe, are: “debug”, “info”, “notice”, “warning”, “error”, “crit”, “alert”, “emerg”.
<GUID>	Globally Unique Identifier. A number that uniquely identifies a device or component.
<MAC address>	A MAC address. The segments may be 8 bits or 16 bits at a time, and may be delimited by “:” or “.”. So you could say “11:22:33:44:55:66”, “1122:3344:5566”, “11.22.33.44.55.66”, or “1122.3344.5566”.
<netmask>	A netmask (e.g. “255.255.255.0”) or mask length prefixed with a slash (e.g. “/24”). These two express the same information in different formats.

Table 9 - Angled Brackets Parameter Description

Parameter	Description
<network prefix>	An IPv4 network prefix specifying a network. Used in conjunction with a net-mask 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.
<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.

3.2 Web Interface

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 8: WebUI

3.2.1 Setup Menu

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

Table 10 - Setup Submenus

Submenu Title	Description
Interfaces	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.

Table 10 - Setup Submenus

Submenu Title	Description
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.
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 11 - System Submenus

Submenu Title	Description
Modules	Displays a graphic illustration of the system modules. By moving the mouse over the ports in the front view, a pop-up caption is displayed to indicate the status of the port. The port state (active/down) is differentiated by a color scheme (green for active, gray/black for down). By moving the mouse over the rear view, a pop-up caption is displayed to indicate the leaf part information.

Table 11 - System Submenus

Submenu Title	Description
Inventory	Displays a table with the following information about the system modules: module name, type, serial number, ordering part number and Asic firmware version.
Power Management	Displays a table with the following information about the system power supplies: power supply name, power, voltage level, current consumption, and status. A total power summary table is also displayed providing the power used, the power capacity, and the power available.
MLNX-OS Upgrade	Displays the installed MLNX-OS images (and the active partition), 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 12 - 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 13 - Ports Submenus

Submenu Title	Description
Ports	Manages port attributes, counters, transceiver info and displays a graphical counters histogram.

Table 13 - Ports Submenus

Submenu Title	Description
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 14 - Status Submenus

Submenu Title	Description
Summary	Displays general information about the switch system and the MLNX-OS image, including: current date and time, hostname, uptime of system, system memory, CPU load averages, etc.
Profile and Capabilities	Displays general information about the switch system capabilities such as the enabled profiles (e.g IB/ETH) and their corresponding values.
Temperature	Provides a graphical display of the switch module sensors' temperature levels over time (1 hour). It is possible to display either the temperature level of one module's sensor or the temperature levels of all the module sensors' together.
Power Supplies	Provides a graphical display of one of the switch's power supplies voltage level over time (1 hour).
Fans	Provides a graphical display of fan speeds over time (1 hour). The display is per fan unit within a fan module.
CPU Load	Provides a graphical display of the management CPU load over time (1 hour).
Memory	Provides a graphical display of memory utilization over time (1 day).
Network	Provides a graphical display of network usage (transmitted and received packets) over time (1 day). It also provides per interface statistics.
Logs	Displays the system log messages. It is possible to display either the currently saved system log or a continuous system log.
Maintenance	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 15 - IB SM Mgmt Submenus

Submenu Title	Description
Summary	Displays the local Subnet Manager (SM) status (running time, failures, etc).
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 Inspectr** menu makes available the following sub-menus (listed in order of appearance from top to bottom):

Table 16 - Fabric Inspectr 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).
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 17 - 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.

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>
```

For further definitions of the interface, please refer to *Mellanox MLNX-OS® Command Reference Guide*.

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@192.168.10.101
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? [switch-6287a4]
Step 2: Use DHCP on mgmt0 interface? [yes] no
<localhost>#
```

In such case the serial connection should be used.

4.1.4 Default Gateway

In order 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)#
```

Step 4.

4.2 Unbreakable Links

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

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

4.2.1 Link Level Retransmission (LLR)

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

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

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



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



LLR is not operational for cables longer than 30m.

LLR Mode

The following LLR modes are applicable per port per speed:

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

LLR Negotiation

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

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



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

LLR Status

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

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

4.2.2 Configuring Phy Profile & LLR

➤ To configure a phy profile:

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

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

Step 2. Configure LLR attributes. Run:

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

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

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

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

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

Step 4. Verify LLR configuration and status. Run:

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

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

Step 5. Display phy-profile configuration. Run:

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

4.3 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 35.

4.3.2 Upgrading MLNX-OS® Software

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 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) #
```

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 35.



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) #
```

For further information, please refer to *Mellanox MLNX-OS Command Reference Guide*.

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 software will first compare 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 will automatically attempt to burn the default firmware version instead.



If a firmware update takes place, then the login process will be delayed for a few minutes.

To verify that the firmware update was successful, login to 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.

Warning: Some of the subsystems are not updated with default FW <ver>.



If you detect a firmware version mismatch 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 (.tgz file). Run:

```
switch (config) # image fetch
switch (config) # image default-chip-fw fw-SX-rel-9_1_2090.tgz
Default Firmware 9.1.2090 updated. Please save configuration and reboot for new FW to
take effect.
switch (config) #
```

Step 2. Save the configuration. Run:

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

Step 3. Reboot the system to enable auto update.

4.4 File 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) #
```

For further information, please refer to *Mellanox MLNX-OS Command Reference Guide*.

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) #
```

For further information, please refer to *Mellanox MLNX-OS Command Reference Guide*.

4.4.3 Restoring Factory Default Configuration on a Switch System (Single Management Module)

In cases where the system configuration becomes corrupted it is suggested that you restore the factory default configuration.

- Step 1.** Connect to the IBM chassis manager and move into the correct Switch blade context.
- Step 2.** Run the command “clear -cnfg” (for more assistance, please refer to the IBM CMM User Manual).
- Step 3.** Wait for the switch blade to reboot itself twice.



It might take a few minutes between one reboot and the other. Please avoid using the system during that time.

For further information, please refer to *Mellanox MLNX-OS Command Reference Guide*.

4.5 Remote Logging

4.5.1 Configuring Remote Syslog to “info” Level

➤ *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>
```

For further information, please refer to *Mellanox MLNX-OS Command Reference Guide*.

4.6 Event Notifications

4.6.1 E-mail 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 10.0.X.X
```

Step 3. Add your email address for notifications.

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

Step 4. Have the system send you a test email.

```
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.

For further information, please refer to *Mellanox MLNX-OS Command Reference Guide*.

4.7 Diagnostics

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 will be stored inside the "POST Diagnostic Register".

Table 18 lists the POST return codes and their meanings.

Table 18 - POST Return Codes

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

Table 18 - POST Return Codes

Return Code	Severity	Meaning	POST Section
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

4.7.1 Retrieving Return Codes when Executing Remote Commands

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

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"'
```

4.8 User Management and Security

4.8.1 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.

For information on the AAA commands, please refer to *Mellanox MLNX-OS Command Reference Guide*.

4.8.1.1 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

For information on the RADIUS commands, please refer to *Mellanox MLNX-OS Command Reference Guide*.

4.8.1.2 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

For information on the TACACS+ commands, please refer to *Mellanox MLNX-OS Command Reference Guide*.

4.8.1.3 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
```

For information on the LDAP commands, please refer to *Mellanox MLNX-OS Command Reference Guide*.

4.8.2 Secure Shell (SSH)

4.8.2.1 Adding a Host and Providing an SSH Key

➤ *To add entries to the global known-hosts configuration file and its SSH value, perform the following steps:*

Step 1. Change to Config mode Run:

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

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

```
switch [standalone: master] (config) # ssh client global known-host "myserver ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAsXeklqc8T0EN2mnMcVcfhueaRYzIVqt4rVsRERijmLJh4mkYYIa8hGGikNa+
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) #
```

4.8.3 User Accounts

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

Table 19 - User Roles (Accounts) and Default Passwords

User Role	Default Password
admin	admin
monitor	monitor

4.9 Network Management Interfaces

4.9.1 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

4.9.1.1 Standard MIBs

Table 20 - 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 21 - 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	
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 22 - Standard MIBs – Chassis and Switch

MIB	Standard	Comments
RFC1213-MIB	RFC 1213	

Table 22 - Standard MIBs – Chassis and Switch

MIB	Standard	Comments
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.

4.9.1.2 Private MIB

Table 23 - 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 are supported.

Mellanox private MIBs can be downloaded from the [Mellanox Support](#) webpage.

4.9.1.3 Mellanox Private Traps

The following private traps are supported by MLNX-OS

Table 24 - 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.

4.9.1.4 Traps and Events Mapping

The following table maps the CLI supported events to SNMP traps.

Table 25 - Supported Traps and Events

Event Description	CLI Event	MIB OID	Comments
ASIC (chip) down	asic-chip-down	Mellanox-EFM-MIB: asicChipDown	Not supported
CPU utilization has risen too high	cpu-util-high	Mellanox-EFM-MIB: cpuUtilHigh	
File system free space has fallen too low	disk-space-low	Mellanox-EFM-MIB: diskSpaceLow	

Table 25 - Supported Traps and Events

Event Description	CLI Event	MIB OID	Comments
Health module status changed	health-module-status	Mellanox-EFM-MIB: systemHealthStatus	
Insufficient amount of fans in system	insufficient-fans	Mellanox-EFM-MIB: insufficientFans	
Insufficient amount of fans in system recovered	insufficient-fans-recover	Mellanox-EFM-MIB: insufficientFansRecover	
Insufficient power supply	insufficient-power	Mellanox-EFM-MIB: insufficientPower	
An interface's link state has changed to DOWN	interface-down	RFC1213: linkdown (SNMPv1)	Supported for Ethernet and management interfaces
An interface's link state has changed to UP	interface-up	RFC1213: linkup (SNMPv1)	Supported for Ethernet and management interfaces
Internal bus (I ² C) error	internal-bus-error	Mellanox-EFM-MIB: internalBusError	
A process in the system is detected as hung	liveness-failure	Not implemented	
Low power supply	low-power	Mellanox-EFM-MIB: lowPower	
Low power supply recover	low-power-recover	Mellanox-EFM-MIB: lowPowerRecover	
Local bridge became a root bridge	new_root	Bridge-MIB: newRoot	Supported for Ethernet
Paging activity has risen too high	paging-high	N/A	Not supported
Power redundancy mismatch	power-redundancy-mismatch	Mellanox-EFM-MIB: powerRedundancyMismatch	Supported for SX65XX only systems
A process in the system has crashed	process-crash	Mellanox-EFM-MIB: procCrash	
A process in the system unexpectedly exited	process-exit	Mellanox-EFM-MIB: procUnexpectedExit	
An SNMPv3 request has failed authentication	snmp-authtrap	Not implemented	
Topology change triggered by a local bridge	topology_change	Bridge-MIB: topologyChange	Supported for Ethernet

Table 25 - Supported Traps and Events

Event Description	CLI Event	MIB OID	Comments
Unexpected system shut-down	unexpected-shutdown	MellanoX-EFM-MIB: unexpectedShutdown	
Send a testing event	To send, use the CLI command: snmp-server notify send-test	testTrap	
Reset occurred due to over-heating of ASIC	N/A	MellanoX-EFM-MIB: asicOverTempReset	Not supported
Temperature is too high	temperature-too-high	MellanoX-EFM-MIB: asicOverTemp	

4.9.1.5 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.

```
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
```

4.9.1.6 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
```

4.9.1.7 Configuring an SNMP notifications

➤ *To set up the SNMP Notification (traps or informs) follow the next steps*

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. 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) #
```

4.9.2 MLNX-OS 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.