SOFTWARE MANUAL

Mellanox MLNX-OS User Manual

Rev 5.5

Software Version 3.7.1000

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

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

© Copyright 2018. Mellanox Technologies Ltd. All Rights Reserved.

Mellanox®, Mellanox logo, Accelio®, BridgeX®, CloudX logo, CompustorX®, Connect-IB®, ConnectX®, CoolBox®, CORE-Direct®, EZchip®, EZchip logo, EZappliance®, EZdesign®, EZdriver®, EZsystem®, GPUDirect®, InfiniHost®, InfiniBridge®, InfiniScale®, Kotura®, Kotura logo, Mellanox CloudRack®, Mellanox CloudXMellanox®, Mellanox Federal Systems®, Mellanox HostDirect®, Mellanox Multi-Host®, Mellanox Open Ethernet®, Mellanox OpenCloud®, Mellanox OpenCloud Logo®, Mellanox PeerDirect®, Mellanox ScalableHPC®, Mellanox StorageX®, Mellanox TuneX®, Mellanox Connect Accelerate Outperform logo, Mellanox Virtual Modular Switch®, MetroDX®, MetroX®, MLNX-OS®, NP-1c®, NP-2®, NP-3®, NPS®, Open Ethernet logo, PhyX®, PlatformX®, PSIPHY®, SiPhy®, StoreX®, SwitchX®, Tilera®, Tilera logo, TestX®, TuneX®, The Generation of Open Ethernet logo, UFM®, Unbreakable Link®, Virtual Protocol Interconnect®, Voltaire® and Voltaire logo are registered trademarks of Mellanox Technologies, Ltd.

All other trademarks are property of their respective owners.

For the most updated list of Mellanox trademarks, visit http://www.mellanox.com/page/trademarks

Table of Contents

Document Revision History 13

About this Manual 22

Chapter 1 Introduction 25

1.1 System Features 25

1.2 InfiniBand Features 26

Chapter 2 Getting Started 27

2.1 Configuring the Switch for the First Time 27

2.1.1 Configuring the Switch with ZTP 34

2.1.2 Rerunning the Wizard 34

2.2 Starting the Command Line (CLI) 34

2.3 Starting the Web User Interface (WebUI) 35

2.4 Zero-touch Provisioning 38

2.4.1 Running DHCP-ZTP 38

2.4.2 ZTP on Director Switches 40

2.4.3 ZTP and MLNX-OS Software Upgrade 40

2.4.4 DHCPv4 Configuration Example 41

2.4.5 DHCPv6 Configuration Example 41

2.4.6 Commands 42

2.5 Licenses 45

2.5.1 Installing MLNX-OS License (CLI) 45

2.5.2 Installing MLNX-OS License (Web) 45

2.5.3 Retrieving a Lost License Key 48

2.5.4 Commands 49

Chapter 3 User Interfaces 54

3.1 LED Indicators 54

3.2 Command Line Interface Overview 54

3.2.1 CLI Modes 54

3.2.2 Syntax Conventions 55

3.2.3 Getting Help 56

3.2.4 Prompt and Response Conventions 57

3.2.5 Using the “no” Form 57

3.2.6 Parameter Key 58

3.2.7 CLI Pipeline Operator Commands 59

3.2.7.1 “include” and “exclude” CLI Filtration Options 59

3.2.7.2 “watch” CLI Monitoring Option 60

3.2.7.3 “json-print” CLI Option 61

3.2.8 CLI Shortcuts 62
3.3 Web Interface Overview 63
3.3.1 Setup Menu 64
3.3.2 System Menu 65
3.3.3 Security Menu 66
3.3.4 Ports Menu 66
3.3.5 Status Menu 67
3.3.6 IB SM Mgmt 68
3.3.7 Fabric Inspector 68
3.3.8 IB Router 69
3.4 Secure Shell (SSH) 69
3.4.1 Adding a Host and Providing an SSH Key 69
3.4.2 Retrieving Return Codes when Executing Remote Commands 70
3.5 Management Information Bases (MIBs) 70
3.6 Commands 74
3.6.1 CLI Session 74
3.6.2 Banner 84
3.6.3 SSH 92
3.6.4 Remote Login 109
3.6.5 Web Interface 112
Chapter 4 System Management 126
4.1 Management Interface 126
4.1.1 Configuring Management Interfaces with Static IP Addresses 126
4.1.2 Configuring IPv6 Address on the Management Interface 126
4.1.3 Dynamic Host Configuration Protocol (DHCP) 127
4.1.4 Default Gateway 127
4.1.5 Configuring Hostname via DHCP (DHCP Client Option 12) 127
4.1.6 Commands 129
4.1.6.1 Interface 129
4.1.6.2 Hostname Resolution 149
4.1.6.3 Routing 155
4.1.6.4 Network to Media Resolution (ARP & NDP) 159
4.1.6.5 DHCP 165
4.1.6.6 IP Diagnostic Tools 167
4.2 NTP, Clock & Time Zones 171
4.2.1 NTP Authenticate 171
4.2.2 NTP Authentication Key 171
4.2.3 Commands 172
4.3 Unbreakable Links 201
4.3.1 Commands 203
4.4 Software Management 204

4.4.1 Important Pre-OS Upgrade Notes 204
4.4.2 Upgrading MLNX-OS Software 204
4.4.3 Upgrading MLNX-OS Software on Director Switches 208
4.4.4 Upgrading MLNX-OS HA Groups 209
4.4.5 Upgrading MLNX-OS MLAG-STP Setup 209
4.4.6 Deleting Unused Images 210
4.4.7 Downgrading MLNX-OS Software 211
4.4.7.1 Downloading Image 211
4.4.7.2 Downgrading Image 212
4.4.7.3 Switching to Partition with Older Software Version 213
4.4.8 Upgrading System Firmware 214
4.4.8.1 After Updating MLNX-OS Software 214
4.4.8.2 After Inserting a Switch Spine or Leaf 215
4.4.8.3 Importing Firmware and Changing the Default Firmware 215
4.4.9 Commands 217
4.5 Configuration Management 229
4.5.1 Saving a Configuration File 229
4.5.2 Loading a Configuration File 229
4.5.3 Restoring Factory Default Configuration 230
4.5.4 Managing Configuration Files 230
4.5.4.1 BIN Configuration Files 230
4.5.4.2 Text Configuration Files 231
4.5.5 Commands 233
4.5.5.1 File System 233
4.5.5.2 Configuration Files 244
4.6 Logging 264
4.6.1 Monitor 264
4.6.2 Remote Logging 264
4.6.3 Commands 265
4.7 Link Diagnostic Per Port 290
4.7.1 General 290
4.7.2 List of Possible Output Messages 290
4.7.3 Commands 291
4.8 Signal Degradation Monitoring 295
4.8.1 Effective-BER Monitoring 295
4.8.2 Configuring Signal Degradation Monitoring 295
4.8.3 Commands 296
4.9 Event Notifications 298
4.9.1 Supported Events 298
4.9.2 SNMP Trap Notifications 300
4.9.3 Terminal Notifications 300
4.9.4 Email Notifications 301

4.9.5 Commands . . . 303
4.9.5.1 Email Notification . . . 303
4.10 Telemetry . . . 324
4.10.1 Commands . . . 325
4.11 mDNS . . . 345
4.11.1 Commands . . . 346
4.12 User Management and Security . . . 347
4.12.1 User Accounts . . . 347
4.12.2 Authentication, Authorization and Accounting (AAA) . . . 347
4.12.2.1 User Re-authentication . . . 348
4.12.2.2 RADIUS . . . 348
4.12.2.3 TACACS+ . . . 348
4.12.2.4 LDAP . . . 348
4.12.3 System Secure Mode . . . 349
4.12.4 Commands . . . 351
4.12.4.1 User Accounts . . . 351
4.12.4.2 AAA Methods . . . 356
4.12.4.3 RADIUS . . . 370
4.12.4.4 TACACS+ . . . 373
4.12.4.5 LDAP . . . 377
4.12.4.6 System Secure Mode . . . 393
4.13 Cryptographic (X.509, IPSec) and Encryption . . . 395
4.13.1 System File Encryption . . . 395
4.13.1.1 Commands . . . 397
4.14 Scheduled Jobs . . . 413
4.14.1 Commands . . . 413
4.15 Statistics and Alarms . . . 423
4.15.1 Commands . . . 423
4.16 Chassis Management . . . 443
4.16.1 System Health Monitor . . . 443
4.16.1.1 Re-Notification on Errors . . . 443
4.16.1.2 System Health Monitor Alerts Scenarios . . . 444
4.16.2 Power Management . . . 445
4.16.2.1 Power Supply Options . . . 445
4.16.2.2 Width Reduction Power Saving . . . 446
4.16.2.3 Managing Chassis Power . . . 447
4.16.3 Monitoring Environmental Conditions . . . 448
4.16.4 USB Access . . . 449
4.16.5 Unit Identification LED . . . 450
4.16.6 High Availability (HA) . . . 450
4.16.6.1 Chassis High Availability Nodes Roles . . . 450
4.16.6.2 Malfunctioned CPU Behavior . . . 451

4.16.6.3 Box IP Centralized Location 452
4.16.6.4 System Configuration 452
4.16.6.5 Takeover Functionally 452
4.16.7 System Reboot 454
4.16.7.1 Rebooting 1U Switches 454
4.16.7.2 Rebooting Director Switches 454
4.16.8 Commands 455
4.16.8.1 Chassis Management 455
4.16.8.2 Chassis High Availability 485
4.17 Network Management Interfaces 490
4.17.1 SNMP 490
4.17.1.1 Standard MIBs 490
4.17.1.2 Private MIB 491
4.17.1.3 Proprietary Traps 491
4.17.1.4 Configuring SNMP 492
4.17.1.5 Resetting SNMPv3 Engine ID 493
4.17.1.6 Configuring an SNMPv3 User 494
4.17.1.7 Configuring an SNMP Notification 494
4.17.1.8 SNMP SET Operations 496
4.17.1.9 IF-MIB and Interface Information 500
4.17.2 JSON API 500
4.17.2.1 Authentication 500
4.17.2.2 Sending the Request 501
4.17.2.3 JSON Request Format 501
4.17.2.4 JSON Response Format 503
4.17.2.5 Supported Commands 506
4.17.2.6 JSON Examples 506
4.17.2.7 JSON Request Using WebUI 511
4.17.3 XML API 513
4.17.4 Commands 514
4.17.4.1 SNMP Commands 514
4.17.4.2 XML API Commands 540
4.17.4.3 JSON API Commands 542
4.18 Puppet Agent 545
4.18.1 Setting the Puppet Server 545
4.18.2 Accepting the Switch Request 545
4.18.3 Installing Modules on the Puppet Server 546
4.18.4 Supported Configuration Capabilities 546
4.18.4.1 InfiniBand Interface Capabilities 546
4.18.4.2 SNMP Capabilities 547
4.18.4.3 Fetched Image Capabilities 547
4.18.4.4 Installed Image Capabilities 548
4.18.5 Supported Resources for Each Type 548

4.18.6 Troubleshooting 548
4.18.6.1 Switch and Server Clocks are not Synchronized 548
4.18.6.2 Outdated or Invalid SSL Certificates Either on the Switch or the Server 548
4.18.6.3 Communications Issue 549
4.18.7 Commands 550
4.19 Control Plane Policing 556
4.19.1 IP Table Filtering 557
4.19.1.1 Configuring IP Table Filtering 557
4.19.1.2 Modifying IP Table Filtering 559
4.19.1.3 Rate-limit Rule Configuration 559
4.19.2 Commands 560
4.19.3 572
Chapter 5 InfiniBand Switching 575
5.1 Node Name 575
5.1.1 Commands 575
5.2 Fabric 577
5.2.1 Commands 577
5.3 IB Router 582
5.3.1 Configuring IB Router 583
5.3.2 Subnet Prefix Checking 585
5.3.3 Commands 586
5.4 Interface 592
5.4.1 Transceiver Information 592
5.4.2 High Power Transceivers 592
5.4.3 Forward Error Correction 592
5.4.4 Break-Out Cables 593
5.4.4.1 Changing System Profile to Allow for Split-Ready Configuration 594
5.4.4.2 Changing the Module Type to a Split Mode 594
5.4.4.3 Unsplitting a Split Port 595
5.4.5 Commands 596
5.5 Subnet Manager (SM) 618
5.5.1 Partitions 618
5.5.1.1 Relationship with ib0 Interface 618
5.5.1.2 Configuring Partition 619
5.5.2 Adaptive Routing 619
5.5.3 Scatter Ports 620
5.5.4 GUID Routing Order 620
5.5.5 Bulk Update Mode 620
5.5.6 Commands 622
5.5.6.1 Subnet Manager (SM) 622
5.5.6.2 Partitions 763

5.5.6.3 Quality of Service (SM) 773
5.5.6.4 Scatter Ports 790
5.5.6.5 GUID Routing Order 792
5.5.6.6 Bulk Update Mode 801
5.6 Subnet Manager (SM) High Availability (HA) 803
5.6.1 Joining, Creating or Leaving an InfiniBand Subnet ID 803
5.6.2 MLNX-OS Management Centralized Location 804
5.6.3 High Availability Node Roles 804
5.6.4 Configuring MLNX-OS SM HA Centralized Location 805
5.6.5 Creating and Adding Systems to an InfiniBand Subnet ID 805
5.6.6 Restoring Subnet Manager Configuration 805
5.6.6.1 Subnet Manager Configuration 806
5.6.6.2 Mellanox High Availability and Opensm Handover/Failover 806
5.6.7 Commands 808
5.7 Fabric Inspector 814
5.7.1 Running Diagnostics 814
5.7.2 Mapping GUIDs to Node Names 819
5.7.3 Importing ibdiagnet Fabric Data 820
5.7.4 Commands 821
Appendix A Enhancing System Security According to NIST SP 800-131A . . 843
A.1 Overview 843
A.2 Web Certificate 843
A.3 Code Signing 845
A.4 SNMP 845
A.5 SSH 845
A.6 HTTPS 846
A.7 LDAP 847
Appendix B Splunk Integration with Mellanox Products 849
B.1 Getting Started with Splunk 849
B.2 Switch Configuration 849
B.3 Adding a Task 850
B.4 Retrieving Data from TCP and UDP Ports 852
B.5 SNMP Input to Poll Attribute Values and Catch Traps 854
B.6 Getting Started 854
B.7 Configuration 854

List of Tables

Table 1: Reference Documents 22
Table 2: Glossary 22
Table 3: General System Features 25
Table 4: InfiniBand Features 26
Table 5: Serial Terminal Program Configuration 28
Table 6: Configuration Wizard Session - IP Configuration by DHCP 29
Table 7: Configuration Wizard Session - IP Zeroconf Configuration 31
Table 8: Configuration Wizard Session - Static IP Configuration 32
Table 9: LED Behavior Details 54
Table 10: CLI Modes and Config Context 54
Table 11: Syntax Conventions 55
Table 12: Angled Brackets Parameter Description 58
Table 13: CLI Keyboard Shortcuts 62
Table 14: WebUI Setup Submenus 64
Table 15: WebUI System Submenus 65
Table 16: WebUI Security Submenus 66
Table 17: WebUI Ports Submenus 66
Table 18: WebUI Status Submenus 67
Table 19: WebUI IB SM Mgmt Submenus 68
Table 20: WebUI Fabric Inspctr Submenus 68
Table 21: WebUI IB Router Submenus 69
Table 22: Module Type 71
Table 23: Device Type 71
Table 24: Sensor Type 72
Table 25: Supported Event Notifications and MIB Mapping 298
Table 26: User Roles (Accounts) and Default Passwords 347
Table 27: Chassis Manager Information 443
Table 28: System Health Monitor Alerts Scenarios 444
Table 29: LWR Configuration Behavior 447
Table 30: Standard MIBs – Textual Conventions and Conformance MIBs 490
Table 31: Standard MIBs – Chassis and Switch 490
Table 32: Private MIBs Supported 491

Table 33: SNMP MELLANOX-EFM-MIB Traps 491
Table 34: SNMP MELLANOX-POWER-CYCLE Traps 492
Table 35: Supported SET OIDs 497
Table 36: Ethernet and Port-Channel Interface Capabilities 546
Table 37: Protocol Enable/Disable Capabilities 547
Table 38: Fetched Image Capabilities 547
Table 39: Installed Image Capabilities 548
Table 40: Fetched Image Capabilities 548
Table 41: Supported Event Notifications and MIB Mapping. 843

List of Figures

Figure 1: Managing an InfiniBand Software Using MLNX-OS 26
Figure 2: Console Ports for CS75x0 Managed Systems 27
Figure 3: Console Ports for SB7xxx Managed Systems 27
Figure 4: MLNX-OS Login Window 35
Figure 5: EULA Prompt 36
Figure 6: Welcome Popup (Example) 37
Figure 7: Display After Login 37
Figure 8: No Licenses Installed 46
Figure 9: Enter License Key(s) in Text Box 47
Figure 10: Installed License 47
Figure 11: WebUI 64
Figure 12: Index Scheme 70
Figure 13: JSON API WebUI Example 512
Figure 14: JSON API Asynchronous Job WebUI Example 513
Figure 15: Accepting an Agent Request through the Console 546
Figure 16: Site-Local Unicast GID Format 582
Figure 17: Host-to-Host IB Router Unicast Flow 583
Figure 18: Break-Out Cable 593
Figure 19: SM HA Subnet 803
Figure 20: Add Data Option 850
Figure 21: Monitor Icon 851
Figure 22: TCP/UDP 852
Figure 23: TCP/UDP Fields 852
Figure 24: Input Settings 853
Figure 25: Start Searching 854
Figure 26: SNMP 855
Figure 27: SNMP Attributes Polling Settings 855
Figure 28: SNMP Attributes Polling Settings 856
Figure 29: Mellanox-Switch 856
Figure 30: Add to Search 857
Figure 31: Search Options 857

Document Revision History

Rev 5.5 – November 29, 2018

Added:

- the command "email autosupport mailhub" on page 312
- the command "email autosupport recipient" on page 313
- the command "snmp-server cache enable" on page 515
- Section 5.4.4, "Break-Out Cables," on page 593

Updated:

- Section 3.3.6, "IB SM Mgmt," on page 68
- Section 4.1.6.6, "IP Diagnostic Tools," on page 167
-
-
- Section 4.9.1, "Supported Events," on page 298
- the command "aaa authorization" on page 366
- the command "show aaa" on page 368
- Section 4.13.1, "System File Encryption," on page 395
- Table 28, "System Health Monitor Alerts Scenarios," on page 444
- the command "show memory" on page 471
- the command "Configuring an SNMPv3 User" on page 494
- the command "snmp-server user" on page 532
- the command "show snmp auto-refresh" on page 535
- the command "show puppet-agent" on page 555
- Section 5.3.1, "Configuring IB Router," on page 583
- the command "ib sm m-key" on page 651
- the command "show ib sm m-key" on page 724

Removed Appendix "Show Commands Not Supported by JSON"

Rev 5.4 – November 5, 2018

No changes made since last revision.

Rev 5.3 – August 30, 2018

Added:

- the command "web proxy auth authtype" on page 122
- the command "web proxy auth basic" on page 123
- the command "web proxy auth host" on page 124

Updated:

- the command "{ip | ipv6} route" on page 155
- the command "image install" on page 224
- the command "image options" on page 226
- Section 4.12.2, "Authentication, Authorization and Accounting (AAA)," on page 347
- the command "aaa authorization" on page 366
- the command "show virtual-machine install" on page 611
- the command "show telemetry" on page 340
- the command "show telemetry threshold record" on page 341
- the command "show system profile" on page 478
- the command "start" on page 642
- the command "show ib fabric messages" on page 830

Rev 5.2 – August 1, 2018

Removed SwitchX content from the document

Updated:

- the command "hostname" on page 149
- the command "telemetry threshold record" on page 332
- the command "show telemetry threshold record" on page 341

Rev 5.1 – June 28, 2018

Added:

- the command "web https ssl renegotiation enable" on page 120
- the command "web https ssl secure-cookie enable" on page 121
- the command "show interfaces mgmt0" on page 145
- the command "show interfaces mgmt0 brief" on page 147
- the command "show interfaces mgmt0 configured" on page 148
- the command "ldap hostname-check enable" on page 381
- the command "show ldap crl" on page 392
- the command "clear telemetry threshold" on page 335
- the command "clear telemetry threshold record" on page 336
- the command "show telemetry threshold record" on page 341
- Table 34, "SNMP MELLANOX-POWER-CYCLE Traps," on page 492
- Section 4.17.1.5, "Resetting SNMPv3 Engine ID," on page 493
- the command "show snmp" on page 534
- the command "show snmp engineID" on page 536

- Section 5.8.6, “Interoperability with MLAG,” on page 804
- Section 6.1.4, “ARP Neighbor Discovery Responder,” on page 1164
- the command “show interfaces” on page 1189
- the command “show interfaces vlan” on page 1190
- the command “show ip interface” on page 1191
- the command “show ip interface brief” on page 1193
- the command “show interface configured” on page 1194
- the command “show ip” on page 1195
- the command “show ip interface mgmt0” on page 1198
- the command “ip arp responder” on page 1232
- the command “default-information originate” on page 1293
- the command “clear ip pim counters” on page 1465
- the command “show ip pim interface brief” on page 1470
- the command “show ip igmp groups” on page 1496
- the command “show ip igmp interface brief” on page 1499
- the command “use-secondary-ip” on page 1531
- Section 5.5.3, “Scatter Ports,” on page 620
- Section 5.5.4, “GUID Routing Order,” on page 620
- Section 5.5.5, “Bulk Update Mode,” on page 620
- Section 5.5.6.4, “Scatter Ports,” on page 790
- Section 5.5.6.5, “GUID Routing Order,” on page 792
- Section 5.5.6.6, “Bulk Update Mode,” on page 801
- Appendix B, “Show Commands Not Supported by JSON” on page 1943

Updated:

- the command “show web” on page 125
- Table 25, “Supported Event Notifications and MIB Mapping,” on page 298
- Section 4.10, “Telemetry,” on page 324
- the command “show telemetry threshold record” on page 341
- the command “show files stats telemetry” on page 344
- the command “ldap ssl” on page 386
- the command “show ldap” on page 391
- Section 4.17.2.7.1, “To Execute a JSON Request,” on page 512
- Section 4.17.2.7.2, “To Query an Asynchronous JSON Request,” on page 512
- the command “show interfaces ethernet” on page 679
- the command “show lacp interfaces ethernet” on page 711
- the command “show interfaces port-channel compatibility-parameters” on page 720

- the command “show interfaces port-channel” on page 716
- the command “lldp tlv-select” on page 731
- Section 5.8.5, “Upgrading MLAG Pair,” on page 804
- the command “show mlag-vip” on page 824
- the command “show interfaces mlag-port-channel” on page 825
- the command “show access-lists log config” on page 897
- the command “openflow add-flows” on page 917
- the command “show ip igmp snooping” on page 986
- the command “show ip igmp snooping groups” on page 987
- the command “show ip routing” on page 1174
- the command “show ip interface vrf” on page 1203
- the command “show interfaces loopback” on page 1217
- the command “show ip route” on page 1220
- the command “show ip route vrf” on page 1222
- the command “show ip route failed” on page 1225
- the command “show ip route static” on page 1226
- the command “show ip route static multicast-override” on page 1227
- the command “neighbor update-source” on page 1370
- Section 6.7.4.3, “Configuring PIM,” on page 1449
- the command “ip pim bsr-candidate” on page 1454
- the command “ip pim register-source” on page 1456
- the command “show ip pim protocol” on page 1466
- the command “show ip pim bsr” on page 1467
- the command “show ip pim interface” on page 1468
- the command “show ip pim neighbor” on page 1471
- the command “show ip pim rp” on page 1472
- the command “show ip pim rp-candidate” on page 1474
- the command “show ip pim ssm range” on page 1475
- the command “show ip pim upstream joins” on page 1476
- the configuration mode for the command “clear ip mroute” on page 1480
- the command “show ip mroute” on page 1481
- the command “show ip mroute summary” on page 1485
- the configuration mode for the command “clear ip igmp groups” on page 1495
- the command “show ip igmp groups” on page 1496
- the command “show ip igmp interface brief” on page 1499
- the command “address” on page 1506

- the command “show vrrp detail” on page 1513
- the command “show ip dhcp relay” on page 1536
- the command “show ip dhcp relay counters” on page 1537
- the command “show interfaces ib” on page 607
- the command “show interfaces ib” on page 607
- the command “ib partition” on page 763
- the command “ipoib” on page 767
- the command “show ib partition” on page 772
- Appendix A, “Enhancing System Security According to NIST SP 800-131A” on page 843

Rev 5.0 – March 29, 2018

Added:

- Section 4.8, “Signal Degradation Monitoring,” on page 295
- the command “show interfaces ethernet transceiver brief” on page 685
- the command “clear ip routing counters” on page 1173
- the command “show ip routing counters” on page 1175
- the command “ip pim sg-expiry-timer” on page 1452
- the command “ip pim register-source” on page 1456
- the command “clear ip mroute” on page 1480
- the command “ib sm aguid_default_hop_limit” on page 649
- the command “show ib sm aguid-default-hop-limit” on page 720

Updated:

- Table 14, “WebUI Setup Submenus,” on page 64
- Step 5 in Section 4.17.1.7, “Configuring an SNMP Notification,” on page 494
- Table 38, “LR4/ER4 Switch and Port Support,” on page 660
- the command “show interfaces switchport” on page 753
- Step 1 in the procedure “To verify MLAG configuration:” on page 808.
- the command “show mlag” on page 823
- the command “show mlag statistics” on page 829
- the command “dcb priority-flow-control mode” on page 1000
- the command “ip pim rp-candidate” on page 1457
- the command “show ip pim rp-hash” on page 1473
- the command “ip pim ssm range” on page 1463
- the command “show ip pim protocol” on page 1466
- the command “show ip pim bsr” on page 1467
- the command “show ip pim interface” on page 1468

- the command “show ip pim rp” on page 1472

Rev 4.90 – March 4, 2018

Added:

- Step 1 in section Section 2.5.1, “Installing MLNX-OS License (CLI),” on page 45
- Section 3.3.8, “IB Router,” on page 69
- the command “show banner” on page 91
- the command “show ssh server host-keys” on page 108
- the command “show web” on page 125
- the command “image default-chip-fw” on page 220
- the command “logging event enable” on page 269
- the command “logging event error-threshold” on page 270
- the command “logging event interval” on page 271
- the command “logging event rate-limit” on page 272
- the command “show logging events” on page 288
- the command “show logging events source-counters” on page 289
- the command “show ip filter” on page 565
- the command “show ip filter all” on page 566
- the command “show ip filter configured” on page 567
- the command “show ipv6 filter” on page 568
- the command “show ipv6 filter all” on page 569
- the command “show ipv6 filter configured” on page 570
- the command “show ip route failed” on page 1225
- the command “show ip route static multicast-override” on page 1227
- the command “show ip bgp vrf summary” on page 1396
- the command “show ip pim ssm range” on page 1475
- Section 6.10.2, “Upstream and Downstream Interfaces,” on page 1524
- the command “show ib fabric sys” on page 839

Updated:

- Section 3.3.1, “Setup Menu,” on page 64
- Section 3.3.4, “Ports Menu,” on page 66
- the command “show ssh server” on page 107
- the command “show clock” on page 186
- the command “show ntp” on page 187
- the command “show radius” on page 372
- the command “show tacacs” on page 376

- the command “show snmp auto-refresh” on page 535
- the command “speed” on page 672
- the command “show interfaces ethernet” on page 679
- the command “show interfaces ethernet transceiver diagnostics” on page 688
- the command “show lacp counters” on page 710
- the command “show interfaces port-channel compatibility-parameters” on page 720
- the command “switchport mode” on page 748
- the command “switchport access” on page 750
- the command “show spanning-tree” on page 782
- the command “show spanning-tree mst” on page 786
- the command “show interfaces mlag-port-channel” on page 825
- the command “show interfaces mlag-port-channel summary” on page 828
- the command “show ipv4 access-lists” on page 889
- the command “show mac access-lists” on page 892
- the command “show access-lists policers (ipv4/ipv4-udk/ipv6/mac/mac-udk)” on page 898
- the command “clear ip igmp snooping counters” on page 985
- the command “dcb priority-flow-control mode” on page 1000
- Section 6.1.3, “Virtual Routing and Forwarding,” on page 1164
- the command “vrf definition” on page 1167
- the command “show vrf” on page 1177
- the command “show ip interface vrf” on page 1203
- the command “ip route” on page 1218
- the command “show ip route” on page 1220
- the command “show {ip | ipv6} bgp” on page 1379
- the command “show ip pim rp-candidate” on page 1474
- the command “ip mroute” on page 1478
- the command “ip dhcp relay instance (interface config)” on page 1533
- the command “show ip dhcp relay” on page 1536
- the command “show interfaces ib internal llr” on page 612
- the command “show interfaces ib transceiver diagnostics” on page 615
- the command “show ib fabric connections” on page 829
- the command “show ib fabric node” on page 832
- the command “show ib fabric node ports” on page 833
- the command “show ib fabric nodes” on page 834
- the command “show ib fabric port” on page 835
- the command “show ib fabric ports” on page 837

- the command “show ib fabric system” on page 840
- the command “show ib fabric system nodes” on page 841
- the command “show ib fabric system ports” on page 842
- Appendix B, “Show Commands Not Supported by JSON” on page 1943

Rev 4.80

Software Ver. 3.6.5000 – November 05, 2017

Added:

- Section 2.1.1, “Configuring the Switch with ZTP,” on page 34
- Section 2.4, “Zero-touch Provisioning,” on page 38
- the command “logging level” on page 280
- the command “show log” on page 286
- Section 4.19, “Control Plane Policing,” on page 556
- Section 5.11.3, “ACL Logging,” on page 840
- Section 5.11.4, “ACL Capability Summary,” on page 841
- the command “clear ip dhcp relay counters” on page 1534
- the command “show magp interface vlan” on page 1523
- the command “width” on page 602

Deleted:

- the command “mc-unaware tc binding”

Updated:

- Table 19, “WebUI IP Route Submenus,” on page 73
- the command “cli max-sessions” on page 76
- the command “show ip dhcp” on page 166
- the command “show interfaces ethernet” on page 679
- the command “show interfaces counters” on page 675
- the command “show isolation-group” on page 699
- the command “show interfaces port-channel” on page 716
- the command “show spanning-tree detail” on page 784
- the command “show spanning-tree vlan” on page 788
- the command “show interfaces mlag-port-channel” on page 825
- the command “show access-lists summary” on page 900
- the command “destination interface” on page 1109
- the command “show monitor session summary” on page 1116
- the command “show ip interface vrf” on page 1203

- the command "show ip route summary" on page 1228
- the command "show ip route interface" on page 1229
- the command "show vrrp detail" on page 1513
- the command "show vrrp statistics" on page 1514
- the command "show magp" on page 1522
- the command "show ip dhcp relay counters" on page 1537
- Updated max SM nodes supported on switches in Section 5.5, "Subnet Manager (SM)," on page 618
- Appendix B, "Show Commands Not Supported by JSON" on page 1943

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' switch platforms.

Related Documentation

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

Table 1 - Reference Documents

Document Name	Description
InfiniBand Architecture Specification, Vol. 1, Release 1.2.1	The InfiniBand Architecture Specification that is provided by IBTA.
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 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.
MLNX-OS XML API Reference Guide	This manual provides general information concerning MLNX-OS XML API.

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

Glossary

Table 2 - Glossary

AAA	Authentication, Authorization, and Accounting. Authentication - verifies user credentials (username and password). Authorization - grants or refuses privileges to a user/client for accessing specific services. Accounting - tracks network resources consumption by users.
ARP	Address Resolution Protocol. A protocol that translates IP addresses into MAC addresses for communication over a local area network (LAN).

Table 2 - Glossary

CLI	Command Line Interface. A user interface in which you type commands at the prompt
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.
Director Class Switch	A high density InfiniBand chassis switch system
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.
Fabric Management	The use of a set of tools (APIs) to configure, discover, and manage and a group of devices organized as a connected fabric.
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
GID (Global Identifier)	A 128-bit number used to identify a Port on a network adapter (see below), a port on a Router, or a Multicast Group.
GUID (Globally Unique Identifier)	A 64-bit number that uniquely identifies a device or component in a subnet
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
IB	InfiniBand
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.
LID (Local Identifier)	A 16 bit address assigned to end nodes by the subnet manager Each LID is unique within its subnet.
LLDP (Link Layer Discovery Protocol)	A vendor neutral link layer protocol used by network devices to advertise their identify, capabilities and for neighbor discovery

Table 2 - Glossary

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
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.
SM (Subnet Manager)	An entity that configures and manages the subnet, discovers the network topology, assign LIDs, determines the routing schemes and sets the routing tables. There is only one master SM and possible several slaves (Standby mode) at a given time. The SM administers switch routing tables thereby establishing paths through the fabric
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' switch system platforms.

MLNX-OS provides a full suite of management options, including support for Mellanox's Unified Fabric Manager® (UFM), SNMPv1, 2, 3, and web user interface (WebUI). In addition, it incorporates a familiar industry-standard CLI, which enables administrators to easily configure and manage the system.

1.1 System Features

Table 3 - General System Features

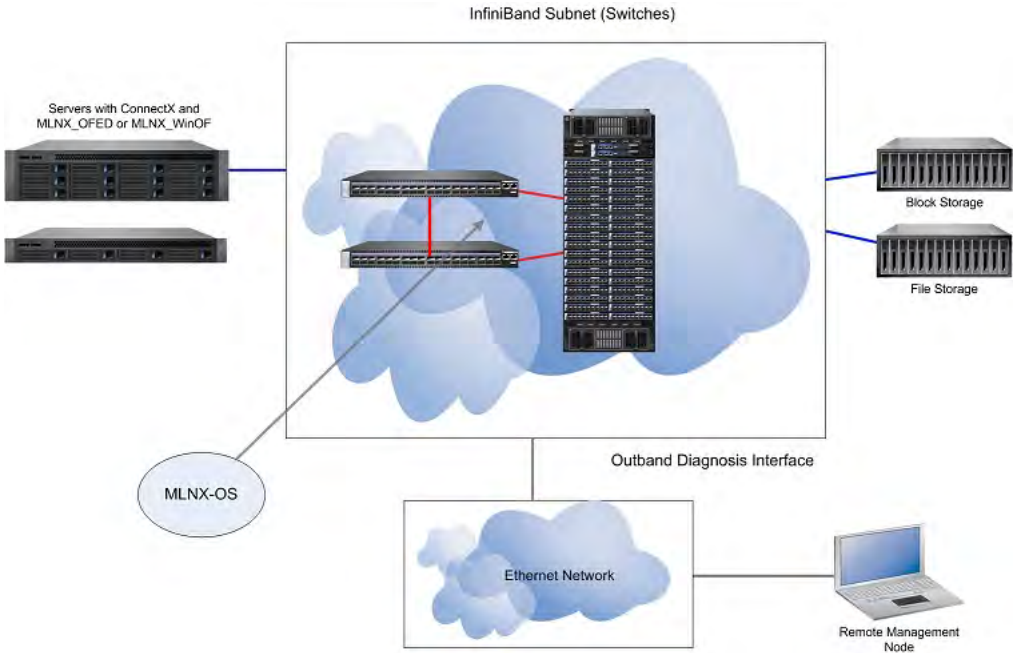
Feature	Detail
Software management	• Dual software image • Software and firmware updates
File management	• FTP • TFTP • SCP
Logging	• Event history log • SysLog support
Management interface	• DHCP/Zeroconf • IPv6
Chassis management	• Monitoring environmental controlsPower management • Auto-temperature control • High availability
Network management interfaces	• SNMP v1,v2c,v3 • interfaces (XML Gateway) • Puppet Agent
Security	• SSH • Telnet • RADIUS • TACACS+
Date and time	• NTP
Cables & transceivers	• Transceiver info
Unbreakable links	• LLR

1.2 InfiniBand Features

Table 4 - InfiniBand Features

Feature	Detail
Subnet manager	• OpenSM • Partitions • High availability
Fabric diagnostics	• Fabric inspector

Figure 1: Managing an InfiniBand Software Using MLNX-OS



2 Getting Started

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

2.1 Configuring the Switch for the First Time

➢ ***To configure the switch:***

Step 1. Connect the host PC to the console (RJ-45) port of the switch system using the supplied cable. The console ports for systems are shown below.

Figure 2: Console Ports for CS75x0 Managed Systems

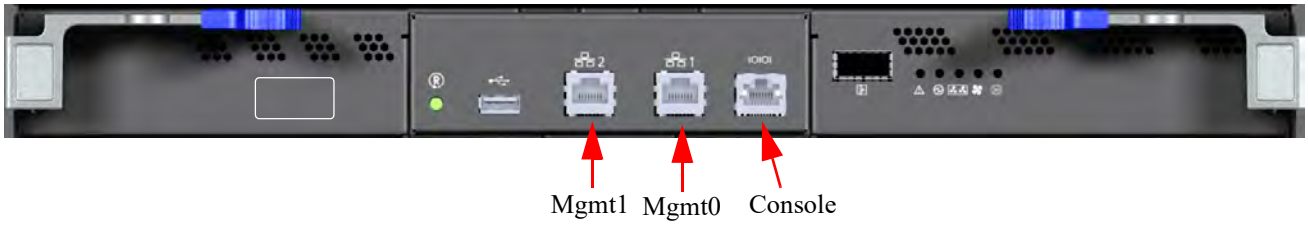
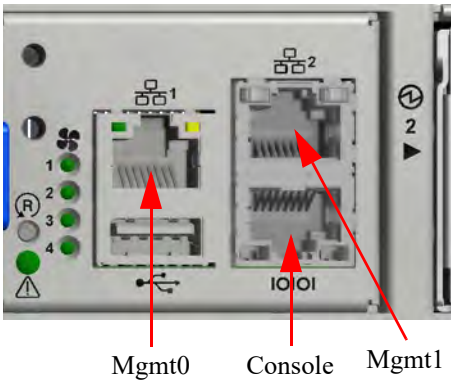


Figure 3: Console Ports for SB7xxx Managed Systems



Make sure to connect to the console RJ-45 port of the switch and not to the MGT port.

DHCP is enabled by default over the MGT port. Therefore, if you have configured your DHCP server and connected an RJ-45 cable to the MGT port, simply log in using the designated IP address.

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

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

Table 5 - Serial Terminal Program Configuration

Parameter	Setting
Baud Rate	115200
Data bits	8
Stop bits	1
Parity	None
Flow Control	None

Step 3. You are prompted with the boot menu.

```
Mellanox MLNX-OS Boot Menu:

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

   Choice:
```

Select “1” to boot with software version installed on partition #1.
Select “2” to boot with software version installed on partition #2.
Selecting “u” is not currently supported.

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

Step 4. Log in as *admin* and use *admin* as password.

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

Step 5. Go through the configuration wizard.

The following table shows an example of a wizard session.

Table 6 - Configuration Wizard Session - IP Configuration by DHCP (Sheet 1 of 2)

Wizard Session Display (Example)	Comments
Mellanox configuration wizard Do you want to use the wizard for initial configuration? yes	You must perform this configuration the first time you operate the switch or after resetting the switch to the factory defaults. Type “y” and then press <Enter>.
Step1: Hostname? [switch-1]	If you wish to accept the default hostname, then press <Enter>. Otherwise, type a different hostname and press <Enter>.
Step 2: Use DHCP on mgmt0 interface? [yes]	Perform this step to obtain an IP address for the switch. (mgmt0 is the management port of the switch.) If you wish the DHCP server to assign the IP address, type “yes” and press <Enter>. If you type “no” (no DHCP), then you will be asked whether you wish to use the “zeroconf” configuration or not. If you enter “yes” (yes Zeroconf), the session will continue as shown in Table 7. If you enter “no” (no Zeroconf), then you need to enter a *static* IP, and the session will continue as shown in Table 8.
Step 3: Enable IPv6 [yes]	Perform this step to enable IPv6 on management ports. If you wish to enable IPv6, type “yes” and press <Enter>. If you enter “no” (no IPv6), then you will automatically be referred to Step 5.
Step 4: Enable IPv6 autoconfig (SLAAC) on mgmt0 interface	Perform this step to enable StateLess address autoconfig on external management port. If you wish to enable it, type “yes” and press <Enter>. If you wish to disable it, enter “no”.
Step 5: Use DHCPv6 on mgmt0 interface? [yes]	Perform this step to enable DHCPv6 on the MGMT0 interface.
Step 5: Admin password (Press <Enter> to leave unchanged)? <new_password> Step 4: Confirm admin password? <new_password>	To avoid illegal access to the machine, please type a password and then press <Enter>. Then confirm the password by re-entering it. Note that password characters are *not* printed.

Table 6 - Configuration Wizard Session - IP Configuration by DHCP (Sheet 2 of 2)

Wizard Session Display (Example)	Comments
You have entered the following information: 1. Hostname: <switch name> 2. Use DHCP on mgmt0 interface: yes 3. Enable IPv6: yes 4. Enable IPv6 autoconfig (SLAAC) on mgmt0 interface: yes 5. Enable DHCPv6 on mgmt0 interface: no 6. Admin password (Enter to leave unchanged): (CHANGED) To change an answer, enter the step number to return to. Otherwise hit <enter> to save changes and exit. Choice: <Enter> Configuration changes saved. To return to the wizard from the CLI, enter the "configuration jump-start" command from configuration mode. Launching CLI... <switch name> [standalone: master] >	The wizard displays a summary of your choices and then asks you to confirm the choices or to re-edit them. Either press <Enter> to save changes and exit, or enter the configuration step number that you wish to return to. Note: To run the command "configuration jump-start" you must be in Config mode.

Table 7 - Configuration Wizard Session - IP Zeroconf Configuration

Wizard Session Display - IP Zeroconf Configuration (Example)
Mellanox configuration wizard Do you want to use the wizard for initial configuration? y Step 1: Hostname? [switch-112126] Step 2: Use DHCP on mgmt0 interface? [no] Step 3: Use zeroconf on mgmt0 interface? [no] yes Step 4: Default gateway? [192.168.10.1] Step 5: Primary DNS server? Step 6: Domain name? Step 7: Enable IPv6? [yes] yes Step 8: Enable IPv6 autoconfig (SLAAC) on mgmt0 interface? [no] no Step 9: Admin password (Enter to leave unchanged)? You have entered the following information: 1. Hostname: switch-112126 2. Use DHCP on mgmt0 interface: no 3. Use zeroconf on mgmt0 interface: yes 4. Default gateway: 192.168.10.1 5. Primary DNS server: 6. Domain name: 7. Enable IPv6: yes 8. Enable IPv6 autoconfig (SLAAC) on mgmt0 interface: yes 9. 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. To return to the wizard from the CLI, enter the “configuration jump-start” command from configure mode. Launching CLI... <switch name> [standalone: master] >

Table 8 - Configuration Wizard Session - Static IP Configuration

Wizard Session Display - Static IP Configuration (Example)
Mellanox configuration wizard Do you want to use the wizard for initial configuration? y Step 1: Hostname? [switch-112126] Step 2: Use DHCP on mgmt0 interface? [yes] n Step 3: Use zeroconf on mgmt0 interface? [no] Step 4: Primary IP address? 192.168.10.4 Mask length may not be zero if address is not zero (interface mgmt0) Step 5: Netmask? [0.0.0.0] 255.255.255.0 Step 6: Default gateway? 192.168.10.1 Step 7: Primary DNS server? Step 8: Domain name? Step 9: Enable IPv6? [yes] yes Step 10: Enable IPv6 autoconfig (SLAAC) on mgmt0 interface? [no] no Step 11: Admin password (Enter to leave unchanged)? You have entered the following information: 1. Hostname: switch-112126 2. Use DHCP on mgmt0 interface: no 3. Use zeroconf on mgmt0 interface: no 4. Primary IP address: 192.168.10.4 5. Netmask: 255.255.255.0 6. Default gateway: 192.168.10.1 7. Primary DNS server: 8. Domain name: 9. Enable IPv6: yes 10. Enable IPv6 autoconfig (SLAAC) on mgmt0 interface: no 11. 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. To return to the wizard from the CLI, enter the “configuration jump-start” command from configure mode. Launching CLI... <switch name>[standalone: master] >

Step 6. Check the mgmt0 interface configuration before attempting a remote (for example, SSH) connection to the switch. Specifically, verify the existence of an IP address.

```
switch # show interfaces mgmt0

Interface mgmt0 status:
  Comment         :
  Admin up        : yes
  Link up         : yes
  DHCP running    : yes
  IP address      : 10.12.67.34
  Netmask         : 255.255.0.0
  IPv6 enabled    : yes
  Autoconf enabled: no
  Autoconf route  : yes
  Autoconf privacy: no
  DHCPv6 running  : no
  IPv6 addresses  : 1

  IPv6 address:
    fe80::268a:7ff:fe53:3d8e/64

  Speed           : 1000Mb/s (auto)
  Duplex          : full (auto)
  Interface type  : ethernet
  Interface source: physical
  MTU             : 1500
  HW address      : 00:02:C9:11:A1:B2

  Rx:
   11700449  bytes
      55753  packets
          0  mcast packets
          0  discards
          0  errors
          0  overruns
          0  frame

  Tx:
   5139846  bytes
     28452  packets
         0  discards
         0  errors
         0  overruns
         0  carrier
         0  collisions
      1000  queue len
```

2.1.1 Configuring the Switch with ZTP

MLNX-OS® Zero-touch Provisioning (ZTP) automates initial configuration of switch systems at boot time. It helps minimize manual operation and reduce customer initial deployment cost.

For more information, please refer to Section 2.4, “Zero-touch Provisioning,” on page 38.

2.1.2 Rerunning the Wizard

➢ ***To rerun the wizard:***

Step 1. Enter the config mode:

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

Step 2. Rerun the wizard:

```
switch (config) # configuration jump-start
```

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. Log into 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:
https://www.mellanox.com/related-docs/prod_management_software/MLNX-OS_EULA.pdf

switch >
```

2.3 Starting the Web User Interface (WebUI)

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

WebUI access is enabled by default.
To disable web access, run the command “no web http enable” or “no web https enable” through the CLI.

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

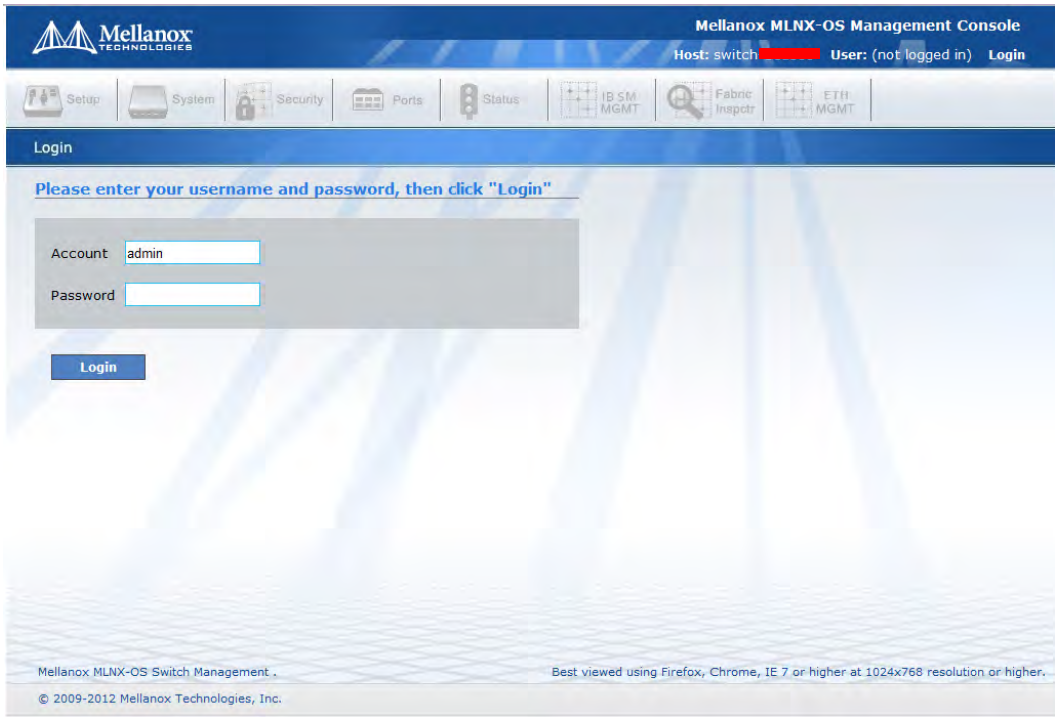
Step 2. Open a web browser – Firefox 12, Chrome 18, IE 8, Safari 5 or higher.

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

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

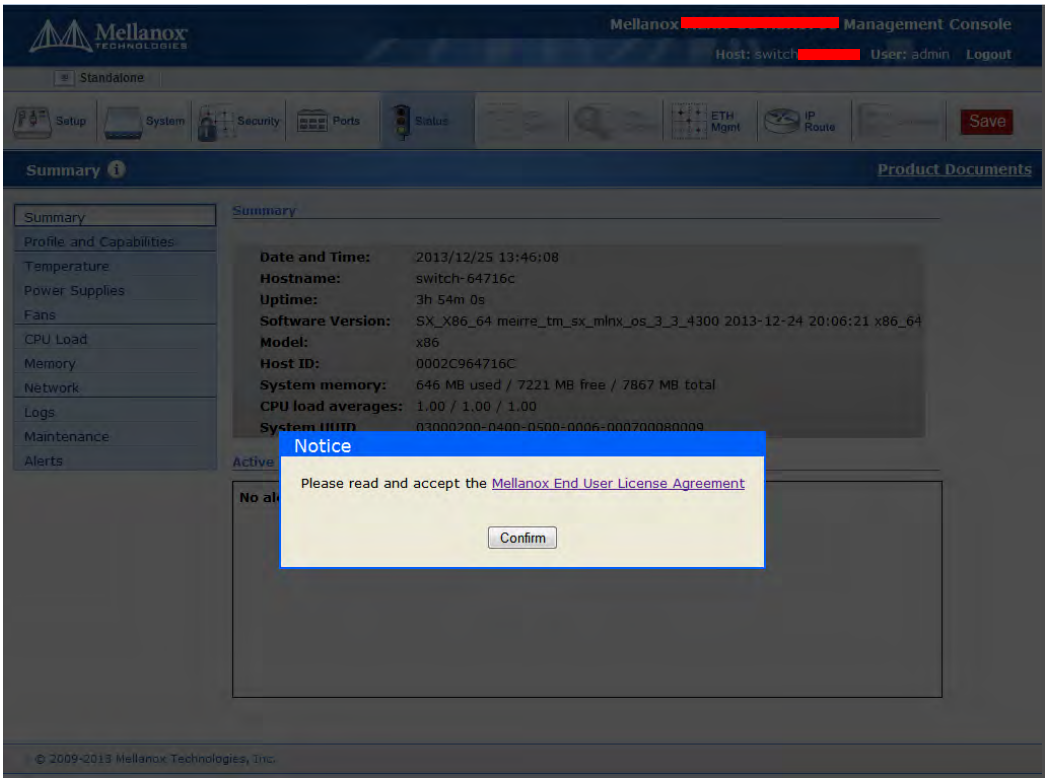
Step 4. Log into the switch (default user name is *admin*, password *admin*).

Figure 4: 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 5: EULA Prompt



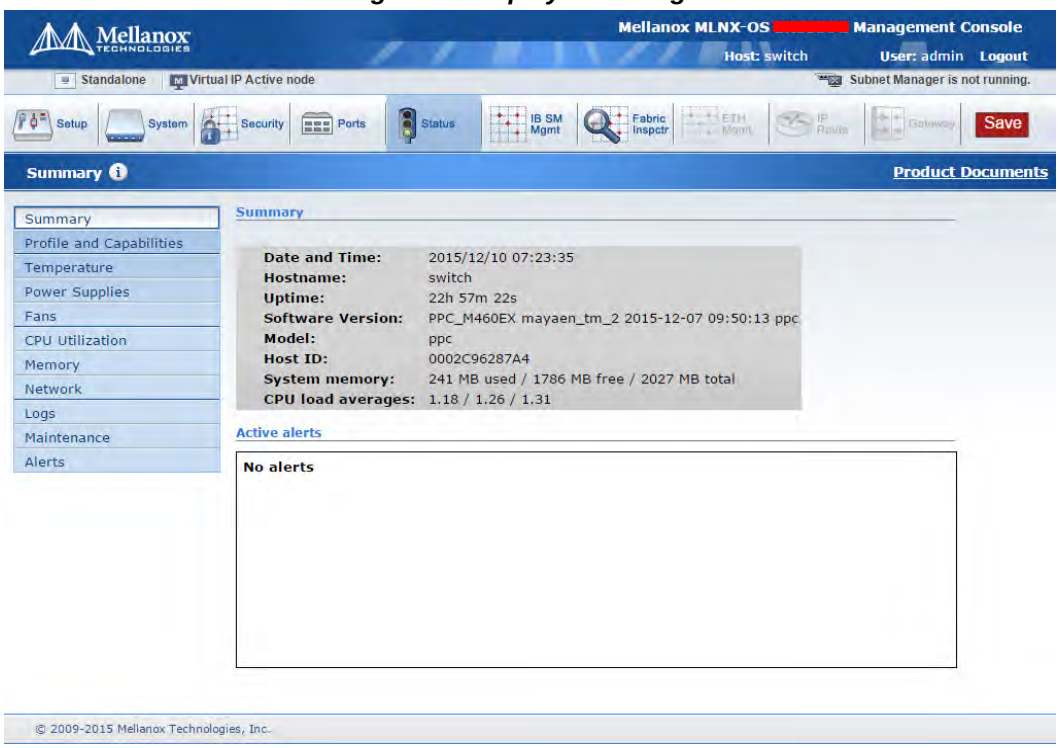
Step 6. The Welcome popup appears. After reading through the content, click OK to continue.
You may click on the links under Documentation to reach the MLNX-OS documentation.
The link under What's New takes you straight to the Changes and New Features section of the switch OS Release Notes.

Figure 6: Welcome Popup (Example)

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

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

Figure 7: Display After Login



2.4 Zero-touch Provisioning

MLNX-OS Zero-touch Provisioning (ZTP) automates initial configuration of Mellanox switches at boot time. It helps minimize manual operation and reduce customer initial deployment cost. MLNX-OS ZTP allows the customer to automatically upgrade the switch with a specified OS image, set up initial configuration database, and load and run a container image file.

The initial configuration is applied using a regular text file. The user can create such a configuration file by editing the output of a "`show running-config`" command.

Only a textual configuration files is supported.

The user-defined docker image can be used by customers to run their own applications in a sandbox on a MLNX-OS platform. And can therefore be also used for automating initial configuration.

Only one docker container could be launched in ZTP.

2.4.1 Running DHCP-ZTP

There is no explicit command to enable ZTP. It is enabled by default. Disabling it is performed by a user-initiated configuration save (using the command "`configuration write`"). The only way to re-enable ZTP would be to run a "`reset factory`" command, clearing the configuration of the switch and rebooting the system.

MLNX-OS ZTP is based on DHCP. For ZTP to work, MLNX-OS enables DHCP by default on all its management interfaces. MLNX-OS requests option 66 (tftp-server-name) and 67 (bootfile-name) from the DHCPv4 server or option 58 (bootfile-url) from the DHCPv6 server, and waits for the DHCP responses which contain file URLs. The DHCP server must be configured to send back the URLs for the software image, configuration file, and docker container image via these two options. Option 66 would contain the URL prefix to the location of the files, option 67 would contain the name of files, and option 58 would contain the complete URLs of files. The format of these two options is a string list separated by commas. The list items are placed in a fixed order:

```
<image file>, <config file>, <docker container file>
```

The item value can be empty, but the comma shall not be omitted.

To have DHCP server figure out the proper files based on switch specific information, MLNX-OS must provide some sort of identity information for the server to classify the switches. Besides the aforementioned options, MLNX-OS attaches option 43 (vendor specific information) and option 60 (vendor class identifier) in DHCPv4 requests, and option 17 (vendor-opts) in DHCPv6. Option 60 is set as string "Mellanox" and options 17 and 43 contain the following Mellanox-specific sub-options:

- System Model
- Chassis Part Number

- Chassis Serial Number
- Management MAC
- System Profile
- MLNX-OS Release Version

The corresponding subtypes respectively are defined as:

```
DHCP_VENDOR_ENCAPSULATED_SUBOPTION_TLV_TYPE_MODEL       1
DHCP_VENDOR_ENCAPSULATED_SUBOPTION_TLV_TYPE_PARTNUM     2
DHCP_VENDOR_ENCAPSULATED_SUBOPTION_TLV_TYPE_SERIAL      3
DHCP_VENDOR_ENCAPSULATED_SUBOPTION_TLV_TYPE_MAC         4
DHCP_VENDOR_ENCAPSULATED_SUBOPTION_TLV_TYPE_PROFILE     5
DHCP_VENDOR_ENCAPSULATED_SUBOPTION_TLV_TYPE_RELEASE     6
```

Upon receiving such DHCP requests from a client, the server should be able to map the switch-specific information to the target file URLs according to predefined rules.

Once MLNX-OS receives the URLs from the DHCP server, it executes ZTP as follows:

1. If the software image URL is not specified, this step is skipped. Otherwise:
   - Perform disk space cleanup if necessary and fetch the image if it does not exist locally
   - Resolve the image version:
     - If it is already installed on active partition, proceed to step 2
     - If it is installed on a standby partition, switch partition and reboot
     - If it is not installed locally, install it and switch to the new image and then reboot
     - In case of reboot, ZTP performs step 1 again and no image upgrade will occur
2. If configuration file URL is not specified, skip this step. Otherwise:
   - Fetch the configuration file
   - Apply the configuration file
3. Skip these steps if a docker image file URL is not specified. Otherwise:
   - Fetch the docker image file
   - Load the docker image
   - Clean up the docker images with the same name and different tag.
   - Start the container based on the image
   - Remove the downloaded docker image file

While performing file transfer via HTTP, the same information as DHCP option 43 is expected to be carried in a HTTP GET request. MLNX-OS supports the following proprietary HTTP headers:

- MlnxSysProfile
- MlnxMgmtMac
- MlnxSerialNumber
- MlnxModelName
- MlnxPartNumber
- MlnxReleaseVersion

In case of failure, the switch waits a random number of seconds between 1 and 20 and reattempts the operation. The switch attempts this up to 10 times.

ZTP progress is printed to terminals including console and active SSH sessions.

2.4.2 ZTP on Director Switches

For director switch systems, the two management nodes start ZTP individually. Status synchronization is then performed between the two nodes:

- Target software image version needs to be the same, otherwise ZTP fails
- Both nodes must install the software image successfully, otherwise ZTP fails
- ZTP failure for one node leads to failure for both
- ZTP disable on one node leads to ZTP disable for both
- ZTP abort on one node leads to ZTP abort for both

In ZTP configuration files, commands between #<CHASSIS_MASTER> and #</CHASSIS_MASTER> pair are only executed on the master.

```
#<CHASSIS_MASTER>
   chassis ha bip 10.7.146.34 /24
#</CHASSIS_MASTER>
```

Node reboot caused by ZTP is also synchronized:

1. Master node asks slave to reboot.
2. Slave node switches to next boot location and acknowledges the reboot request.
3. Master node reboots slave node via hardware.
4. Master node reboots itself.

2.4.3 ZTP and MLNX-OS Software Upgrade

Software upgrade from non-ZTP versions to ZTP versions and vice versa is supported. When upgrading from a non-ZTP version, ZTP is disabled because ZTP is always assumed to start with an empty configuration, otherwise the final configuration becomes a mixture of the existing configuration from the stored database and new configuration from the server and hence not deterministic.

2.4.4 DHCPv4 Configuration Example

The following is a URL configuration example for ISC DHCPv4 server:

```
 host master {
          hardware ethernet E4:1D:2D:5B:72:80;
          fixed-address 3.1.2.13;
          option tftp-server-name "scp://<user>:<password>@3.1.3.100/ztp/,scp://
                                   <user>:<password>@3.1.3.100/ztp/,scp://
                                   <user>:<password>@3.1.3.100/ztp/";
          option bootfile-name "image-X86_64-3.6.4612.img, switch-1.conf,
ubuntu.img.gz";
     }
```

DHCPv4 request is made out of the following components:

- Option 43 (vendor-encapsulated-options) and option 60 (vendor-class-identifier) are added in the DHCPv4 request packet
- Option 66 (tftp-server-name) and option 67 (bootfile-name) are added in the parameter request list of DHCPv4 request packet

2.4.5 DHCPv6 Configuration Example

The following is a DHCPv6 configuration example:

```
 host master {
         ......
        option dhcp6.bootfile-url "scp://<user>:<password>@[2000::1]/ztp/image-X86_64-
                                   3.6.4612.img, scp://<user>:<password>@[2000::1]/ztp/
                                   switch.conf, scp://<user>:<password>@[2000::1]/ztp/
                                   ubuntu.img.gz";
     }
```

DHCPv6 request is made out of the following components:

- Option 17 (vendor-opts) is added in the DHCPv6 request packet
- Option 59 (bootfile-url) is added in the parameter request list of DHCPv6 request packet

2.4.6 Commands

no zero-touch suppress-write

no zero-touch suppress-write

The no form of the command disables suppression of configuration write.

Syntax Description	N/A
Default	Enabled
Configuration Mode	config
History	3.6.5000
Role	admin
Example	`switch (config) # no zero-touch suppress-write`
Related Commands	show zero-touch
Notes	When ZTP is active, “configuration write” is suppressed because it may interfere with ZTP operation. Therefore, after running “no zero-touch suppress-write” if “configuration write” is performed, then ZTP is disabled as a consequence of the database save.

zero-touch abort

	zero-touch abort Aborts on-going zero-touch process.
Syntax Description	N/A
Default	Enabled
Configuration Mode	config
History	3.6.5000
Role	admin

Example	`switch (config) # zero-touch abort`
	
	`Zero-touch failed [Zero-touch is aborted by operator]`
	`Zero-touch provisioning will be aborted`

Related Commands	show zero-touch
Notes	

show zero-touch

	show zero-touch Displays zero-touch status.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.5000
Role	admin

Example	`switch (config) # show zero-touch`
	`Zero-Touch status:`
	`  Active: yes`
	`  Status: Waiting for zero-touch start`
	`  Suppress-write: no`
	`  Configured by zero-touch: no`
	`  Configuration changed after zero-touch: no`

Related Commands	zero-touch abort zero-touch suppress-write
Notes	

2.5 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.

2.5.1 Installing MLNX-OS License (CLI)

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

Step 1. Before applying a license, please make sure your system's time is configured correctly by manually setting it using the CLI command "clock set", or by using NTP using the command "ntp".

Step 2. Login as *admin* and change to *Config* mode.

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

Step 3. Install the license using the key. Run:

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

Step 4. 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 5. 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.

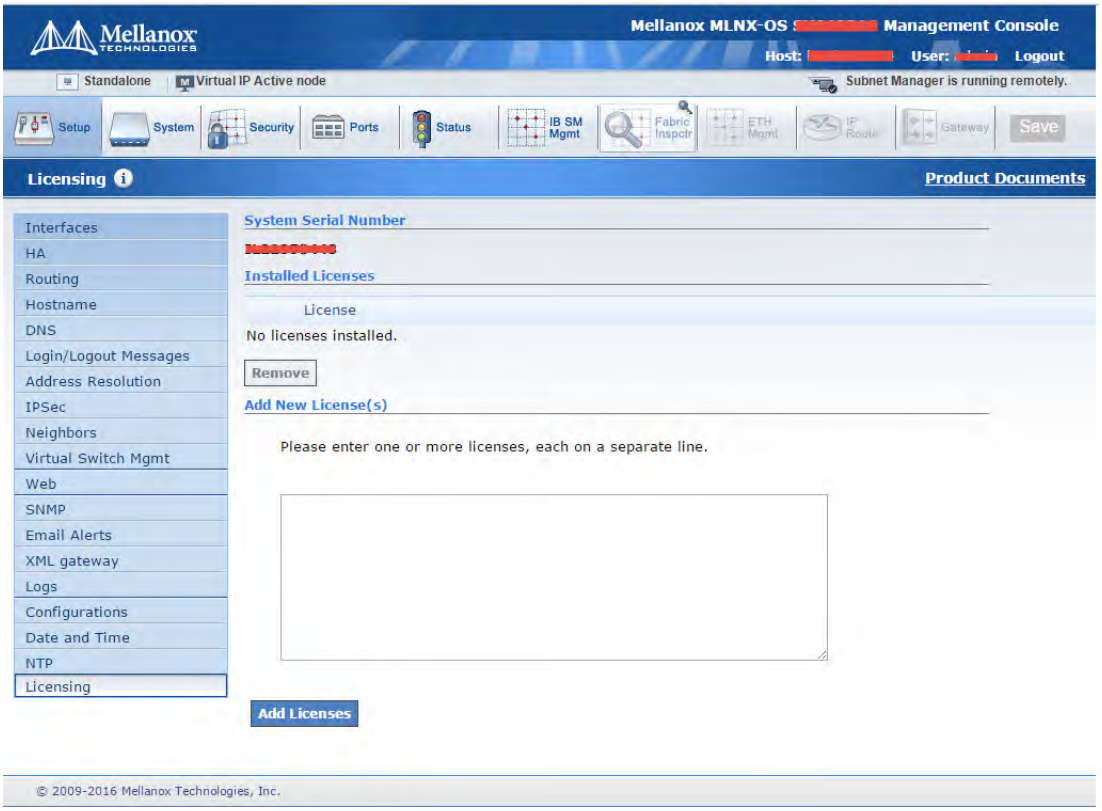
2.5.2 Installing MLNX-OS License (Web)

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

Step 1. Log in as *admin*.

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

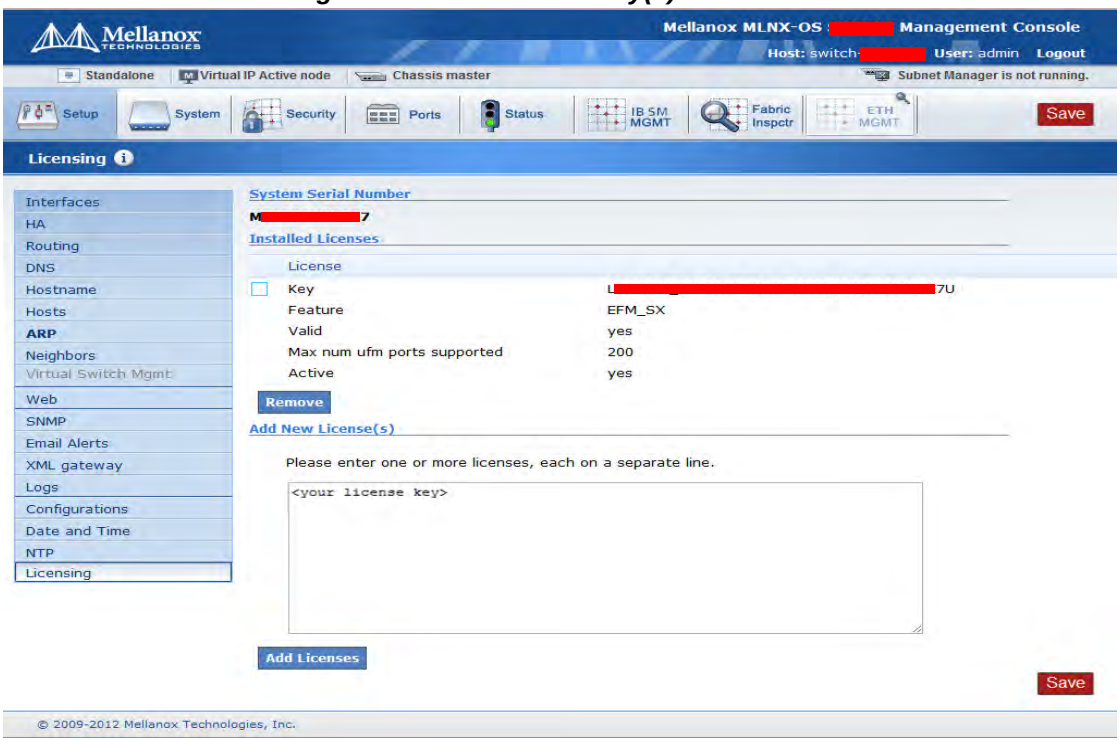
Figure 8: No Licenses Installed



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

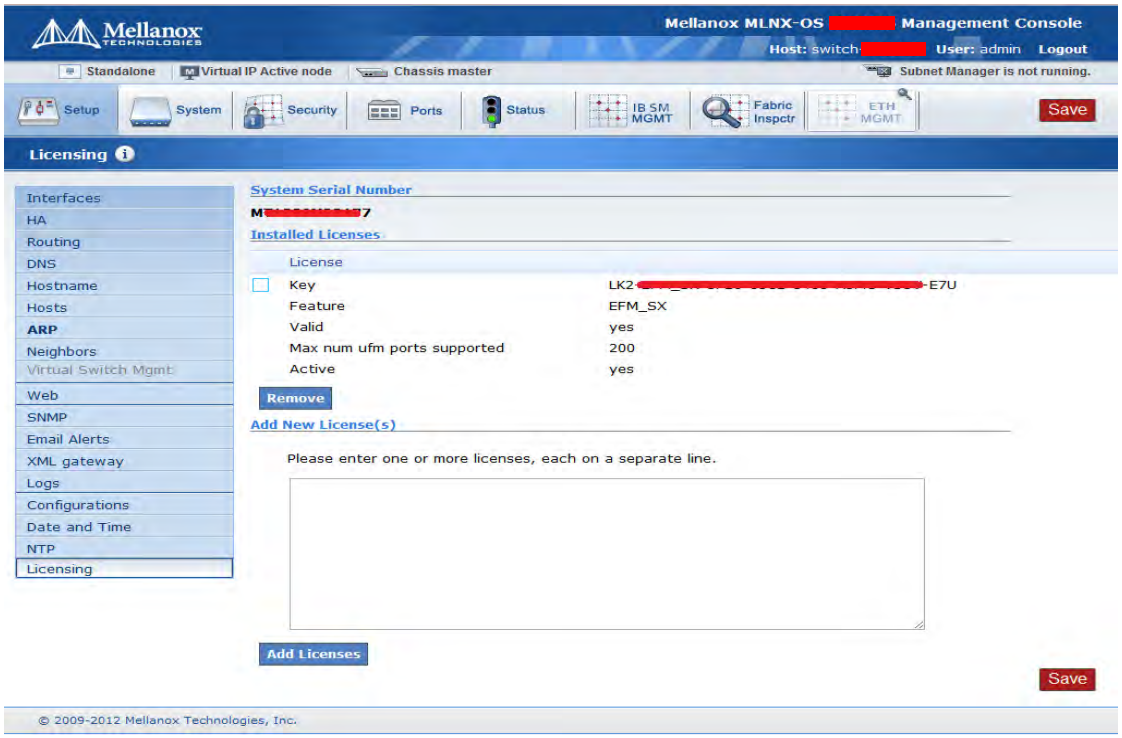
If you wish to add another license key in the future, you can simply enter it in the text box and click “Add Licenses” to install it.

Figure 9: Enter License Key(s) in Text Box



All installed licenses should now be displayed.

Figure 10: Installed License



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

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

2.5.3 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           Part Number        Serial Number        Asic Rev.    HW Rev.
---------------------------------------------------------------------------
CHASSIS          MSB7800-ES2F       MT1602X17464         N/A          A1
MGMT             MSB7800-ES2F       MT1602X17464         0            A1
FAN1             MTEF-FANF-A        MT1602X16943         N/A          A3
FAN2             MTEF-FANF-A        MT1602X16944         N/A          A3
FAN3             MTEF-FANF-A        MT1602X16956         N/A          A3
FAN4             MTEF-FANF-A        MT1602X16957         N/A          A3
PS1              MTEF-PSF-AC-A      MT1601X09908         N/A          A3
```

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

- The chassis serial number
- The type of license you need to retrieve. Refer to "Licenses" on page 45.

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

2.5.4 Commands

file eula upload

file eula upload <filename> <URL>

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

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

file help-docs upload

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

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

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

license delete

license delete <license-number>

Removes license keys by ID.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.4.1100
Role	admin
Example	`switch (config) # license delete <license-number>`
Related Commands	
Note	Before deleting a license from a switch which is configured to a system profile other than its default, the user must first disable all interfaces and then return the switch to its default system profile.

license install

license install <license-key>

Installs a new license key.

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

show licenses

	show licenses Displays a list of all installed licenses. For each license, the following is displayed: • a unique ID which is a small integer • the text of the license key as it was added • whether or not it is valid and active • which feature(s) it is activating • a list of all licensable features specifying whether or not it is currently activated by a license
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.4.1100
Role	admin

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

Related Commands	
Note	

3 User Interfaces

3.1 LED Indicators

Table 9 - LED Behavior Details

LED	Qty.	Color	Description
QSFP LEDs	8	Green/Amber	Off – link is down Solid green – link is up Blinking green – data activity. Blinking frequency is proportional to data transfer speed. Blinking amber – link error
Health LED	1	Red/Green/Amber	Off – no power Blinking amber – fault Solid green – normal Solid red – CANMIC boot failure
UID LED	1	Blue	Solid – LED is activated to identify this module

3.2 Command Line Interface Overview

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

3.2.1 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 following are some of the CLI configuration modes:

Table 10 - CLI Modes and Config Context

Configuration Mode	Description
Standard	When the CLI is launched, it begins in Standard mode. This is the most restrictive mode and only has commands to query a restricted set of state information. Users cannot take any actions that directly affect the system, nor can they change any configuration.
Enable	The `enable` command moves the user to Enable mode. This mode offers commands to view all state information and take actions like rebooting the system, but it does not allow any configurations to be changed. Its commands are a superset of those in Standard mode.

Table 10 - CLI Modes and Config Context

Configuration Mode	Description
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 super-set of those in Enable mode. To return to Enable mode, enter `exit` or `no configure`. Note that moving directly from/to Standard mode to/from Config mode is not possible.
config interface management	Configuration mode for management interface mgmt0, mgmt1 and loopback
Any command mode	Several commands such as "show" can be applied within any context

3.2.2 Syntax Conventions

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

Table 11 - 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.

3.2.3 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`.)

3.2.4 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.

3.2.5 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
  ...
```

3.2.6 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 12 - 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.

Table 12 - Angled Brackets Parameter Description

Parameter	Description
<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.
<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.

3.2.7 CLI Pipeline Operator Commands

3.2.7.1 “include” and “exclude” CLI Filtration Options

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

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

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

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

Examples:

```
switch (config) # show asic-version | include SX
MGMT              SX                 9.3.3150

arc-switch14 [standalone: master] (config) # show module | exclude PS
=====================
Module    Status
=====================
MGMT      ready
FAN1      ready
FAN2      ready

switch (config) # show interfaces | include "Eth|discard pac"
Eth1/1
0 discard packets
0 discard packets
Eth1/2
0 discard packets
0 discard packets
Eth1/3
0 discard packets
0 discard packets
Eth1/4
0 discard packets
0 discard packets
switch (config) # show interfaces | include "Tx" next 5 | exclude broad
Tx
0 packets
0 unicast packets
0 multicast packets
0 bytes
--
Tx
0 packets
0 unicast packets
0 multicast packets
0 bytes
```

3.2.7.2 “watch” CLI Monitoring Option

MLNX-OS also allows viewing a live feed of the progress of any “show” command by using the “watch” option as follows:

```
switch (config) # <show command> | watch [diff] [interval <1-100 secs>]
```

Running the command as such displays an output of the show command that gets updated at a time interval which may be specified using the “interval” parameter (2 seconds by default).

The “diff” parameter highlights the differences between each iteration of the command. For example running the command “`show power | watch diff interval 1`” yields something similar to the following:

```
-------------------------------------------------------------------------------------
Module  Device           Sensor  Power   Voltage  Current  Capacity  Feed  Status
                                 [Watts] [Volts]  [Amp]    [Watts]
-------------------------------------------------------------------------------------
PS1     power-mon        input   85.00   230.00   0.38     460.00    AC    OK
PS2     power-mon        -       -       -        -        -         -     FAIL

Total power used : 85.00 Watts
Total power capacity : 460.00 Watts
Total power available : 375.00 Watts
Maximum consumed power of all turned on modules: 462.00 Watts
```

With the highlighted black blocks indicating the change that has occurred between one iteration of the command from one second to the next.

To exit “watch” mode, press Ctrl+C.

The “watch” option may also be used in conjunction with the “include” and “exclude” options as follows:

```
switch (config) # <show command> | {include | exclude} <extended regular expression> |
watch [diff] [interval <1-100 secs>]
```

For example:

```
switch (config) # show power | include PS | watch diff interval 1
```

3.2.7.3 “json-print” CLI Option

The OnyxMLNX-OS CLI supports printing “show” commands in JSON syntax.

To print the output of the “show” commands as JSON, use the following format:

```
switch (config) # <show command> | json-print
```

Running the command displays an output of the “show” command in JSON syntax structure instead of its regular format. For example:

```
switch (config) # show system profile
Profile: eth-single-switch
Switch (config) # show system profile | json-print
{
"Profile": "eth-single-switch"
}
```

The “json-print” option cannot be used together with filtering (“include” and “exclude”) and/or monitoring (“watch”).

For more information on JSON usage, please refer to Section 4.17.2, “JSON API,” on page 500.

For a list of commands supporting the JSON API, please refer to Appendix B,“Show Commands Not Supported by JSON,” on page 1943.

3.2.8 CLI Shortcuts

Table 13 presents the available keyboard shortcuts on the MLNX-OS CLI.

Table 13 - CLI Keyboard Shortcuts

Key Combination	Description
Ctrl-a	Move cursor to beginning of line
Ctrl-b	Move cursor backward one character without deleting
Ctrl-c	Terminate operation
Ctrl-d	If cursor is in the middle of the line, delete one character forward If cursor is at the end of the line, show auto-complete options for current word or word fragment If cursor at an empty line, same as Esc
Ctrl-e	Move cursor to end of line
Ctrl-f	Move cursor forward one character
Ctrl-h	Delete one character backwards from cursor
Ctrl-i	Auto-complete current word (same as TAB)
Ctrl-j	Return carriage (same as ENTER)
Ctrl-k	Delete line after cursor
Ctrl-l	Clear screen and show line at the top of terminal window
Ctrl-m	Return carriage (same as ENTER)
Ctrl-n	Next line (same as DOWN ARROW)
Ctrl-p	Next line (same as UP ARROW)
Ctrl-t	Transpose the two characters on either side of cursor
Ctrl-u	Delete line
Ctrl-y	Retrieve (“yank”) last item deleted
Esc b	Move cursor one word backward
Esc c	Capitalizes first letter in word after cursor
Esc d	Delete one word forward from cursor
Esc f	Move one word forward from cursor
Esc l	Change word after cursor to lowercase letters
Esc Ctrl-h	Delete one word backward from cursor
Esc [A	Next line (same as DOWN ARROW)
Esc [B	Next line (same as UP ARROW)
Esc [C	Move forward one character from cursor
Esc [D	Move backward one character from cursor

3.3 Web Interface Overview

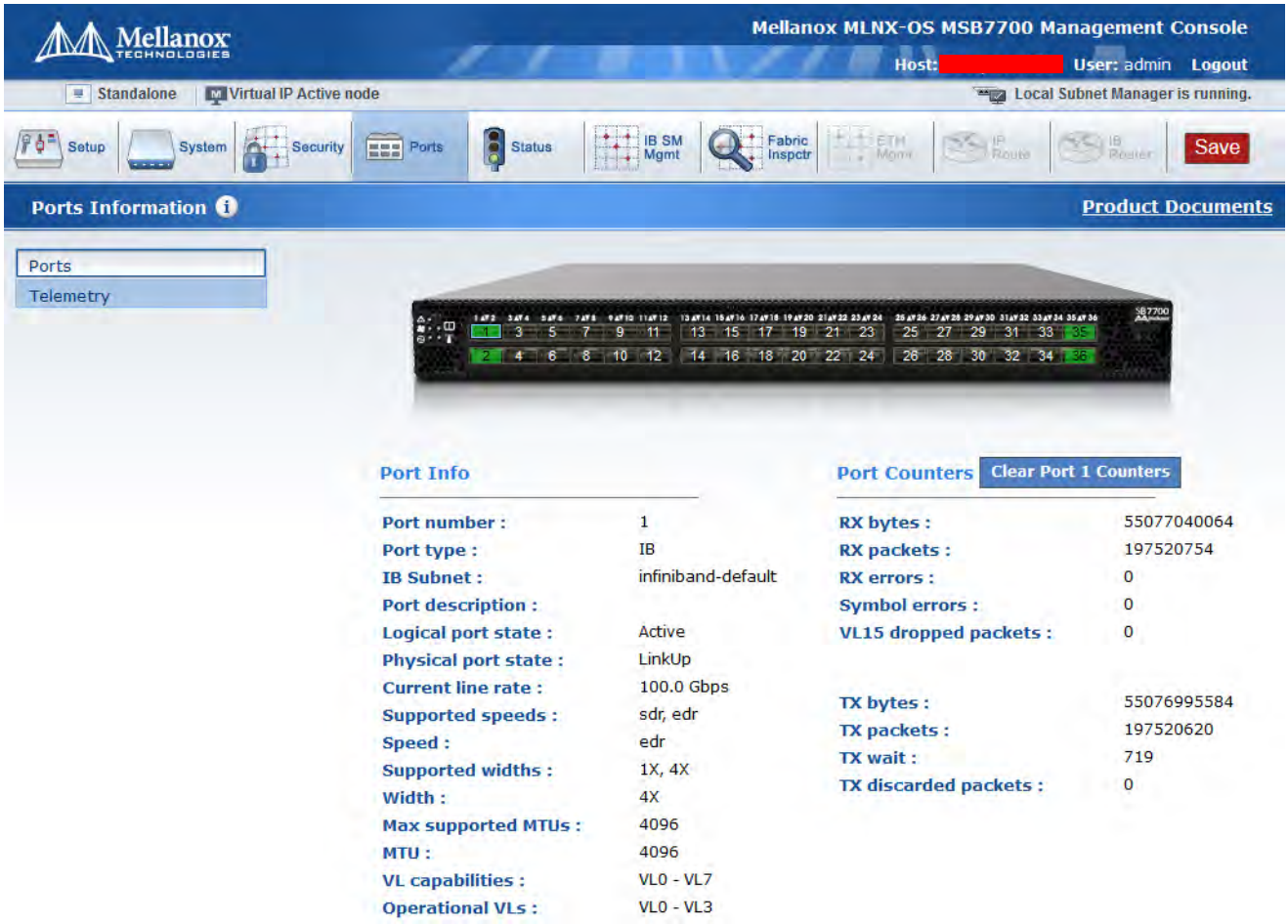
The MLNX-OS package equipped with web interface which is a web GUI that accept input and provide output by generating webpages which can be viewed by the user using a web browser.

The web interface makes available the following perspective tabs:

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

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

Figure 11: WebUI



3.3.1 Setup Menu

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

Table 14 - WebUI Setup Submenus

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

Table 14 - WebUI Setup Submenus

Submenu Title	Description
DNS	Configures, removes, modifies or displays static and dynamic name servers
Login Messages	Edits the login messages: Message of the Day (MOTD), Remote Login message, and Local Login message
Address Resolution	Adds static and dynamic ARP entries, and clears the dynamic ARP cache
IPSec	Configures IPSec
Neighbors	Displays IPv6 neighbor discovery protocol
Virtualization	Manages the virtualization and virtual machines
Virtual Switch Mgmt	Configures the system profile
Web	Configures web user interface and proxy settings
SNMP	Configures SNMP attributes, SNMP admin user, and trap sinks
Email Alerts	Configures the destination of email alerts and the recipients to be notified
XML gateway	Provides an XML request-response protocol to get and set hardware management information
JSON API	Manages JSON API
Logging	Sets up system log files, remote log sinks, and log formats
Configurations	Manages, activates, saves, and imports MLNX-OS configuration files, and executes CLI commands
Docker	Manages docker images and containers.
Date and Time	Configures the date, time, and time zone of the switch system
NTP	Configures NTP (Network Time Protocol) and NTP servers
Licensing	Manages MLNX-OS licenses

3.3.2 System Menu

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

Table 15 - WebUI System Submenus

Submenu Title	Description
Modules	Displays a graphic illustration of the system modules. By moving the mouse over the ports in the front view, a pop-up caption is displayed to indicate the status of the port. The port state (active/down) is differentiated by a color scheme (green for active, gray/black for down). By moving the mouse over the rear view, a pop-up caption is displayed to indicate the leaf part information.
Inventory	Displays a table with the following information about the system modules: module name, type, serial number, ordering part number and ASIC firmware version

Table 15 - WebUI System Submenus

Submenu Title	Description
Power Management	Displays a table with the following information about the system power supplies: power supply name, power, voltage level, current consumption, and status. A total power summary table is also displayed providing the power used, the power capacity, and the power available.
MLNX-OS Upgrade	Displays the installed MLNX-OS images (and the active partition), uploads a new image, and installs a new image
Reboot	Reboots the system. Make sure that you save your configuration prior to clicking reboot.

3.3.3 Security Menu

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

Table 16 - WebUI Security Submenus

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

3.3.4 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 17 - WebUI Ports Submenus

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

Table 17 - WebUI Ports Submenus

Submenu Title	Description
Protocol Type	Manages the link protocol type
Telemetry	Displays and configures telemetry

3.3.5 Status Menu

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

Table 18 - WebUI Status Submenus

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

3.3.6 IB SM Mgmt

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

Table 19 - WebUI IB SM Mgmt Submenus

Submenu Title	Description
Summary	Displays the local Subnet Manager (SM) status (running time, failures, etc)
Base SM	Manages basic SM configuration (enabling SM, priority level, and restoring initial configuration)
Advanced SM	Manages basic SM configuration (enabling SM, priority level, and restoring initial configuration)
Expert SM	1. Configures security and GUID based prefixes (m_key, sm_key, sa_key, etc), and manages special SM attributes that should not be changed except by expert users of the Subnet Manager who understand the risks of manipulating these attributes. 2. Fabric inspector, and many standalone InfiniBand utilities, may not function on subnets with a non-default m-key.
Compute nodes	Adds compute nodes using network adapter port GUIDs
Root nodes	Adds root nodes using switch GUIDs
Partitions	Manages partition keys (sets removes or displays the partition keys)
Basic Qos	Configures basic QoS attributes such as default QoS settings, and VL arbitration low and high entries. It also displays and manages SL-to-VL mappings.

3.3.7 Fabric Inspector

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 20 - WebUI 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 20 - WebUI 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

3.3.8 IB Router

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

Table 21 - WebUI IB Router Submenus

Submenu Title	Description
IB Router Global	Enables/disables IB router
IB Router Configuration	Manages IB router admin state and IB router interfaces

3.4 Secure Shell (SSH)

It is recommended not to use more than 50 concurrent SSH sessions to the switch.

3.4.1 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
AAAAB3NzaC1yc2EAAAABIwAAAIEAsXeklqc8T0EN2mnMcVcfhueaRYzIVqt4rVsrERIjmlJh4mkYYIa8hGGikN
a+t5xw2dRrNxnHYLK51bUsSG1ZNwZT1Dpme3pAZeMY7G4ZMgGIW9xOuaXgAA3eBeoUjFdi6+1BqchWk0nTb+gM
fI/MK/heQNns7AtTrvqg/O5ryIc="
switch [standalone: master] (config) #
```

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

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

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

No SSH user identities configured.

No SSH authorized keys configured.

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

3.4.2 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"'
```

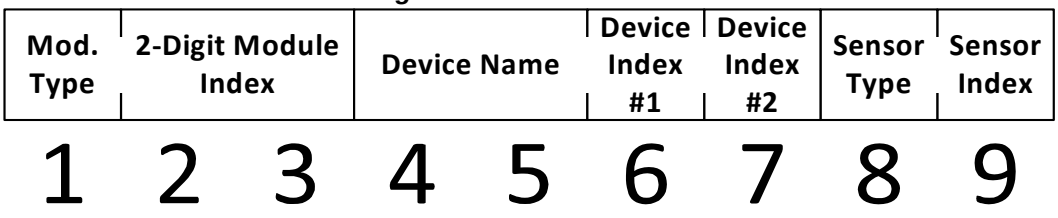
3.5 Management Information Bases (MIBs)

The inventory in the switch system can be accessed through a MIB browser. These devices are indexed (entPhysicalIndex) using three levels:

1. Module layer which includes modules located on system (e.g. cables, fan, power supply, etc.). See table Table 22 for more details.
2. Device layer which includes system devices (e.g. switch devices, sensor aggregators, etc.). See table Table 23 for more details.
3. Sensor layer which includes system sensors (e.g. fan, and temperature sensors) located in the devices. See table Table 24 for more details.

Each layer is assigned a fixed position in the index number to represent it.

Figure 12: Index Scheme



Each position could indicate different types of component according to the following criteria:

Table 22 - Module Type

Number	Description
1	Chassis
2	Management
3	Spine
4	Leaf
5	Fan
6	Power supply
7	BBU
8	x86 CPU
9	Port module

Table 23 - Device Type

Number	Description
01	PS
02	FAN
03	BOARD_MONITOR
04	CPU_BOARD_MONITOR
05	SX
06	SIB
07	CPU_MEZZ_TEMP
08	CPU Package Sensor
09	CPU Core Sensor
10	SX_AMBIENT_TEMP
11	SX_MONITOR
12	AUX_IN_TMP_SNSR
13	AUX_OUT_TMP_SNSR
14	MAIN_IN_TMP_SNSR
15	MAIN_OUT_TMP_SNSR
16	CPU_MEZZ_TEMP
17	Controller
18	QSFP_TEMP
19	QSFP-ASIC
20	Board AMB temp
21	Ports AMB temp

Table 23 - Device Type

Number	Description
22	Power monitor
23	PS_MONITOR
24	SWB AMB temp
25	pcie-switch-temp
26	SPC

Table 24 - Sensor Type

Number	Description
1	t – temperature sensor
2	f – fan sensor

For example:

- 401191311

  The first layer is “401” where:

  - “4”, according to Table 22, indicates a leaf
  - “01” indicates index #1 (Leaf #1)

  The second layer is “1913” where:

  - “19”, according to Table 23, indicates a QSFP ASIC
  - “1” indicates ASIC #1
  - “3” indicates sensor #3 (QSFP-ASIC1-3)

  The third layer is “11” where:

  - “1”, according to Table 24, indicates a temperature sensor
  - “1” indicates sensor #1 (T1)

  The resulting output in the entPhysicalDescr column of the MIB would be: L01/QSFP-ASIC-1/T1.

- 501020021

  The first layer is 501 where

  - “5”, according to Table 22, indicates a fan
  - “01 indicates index #1 (Fan #1)

  The second layer is 0200 where:

  - 02, according to Table 23, indicates a fan
  - 0 – indicates that there is no first index
  - 0 – indicates that there is no second index

  The third layer is 21 where:

  - “2”, according to Table 24, indicates a fan sensor
  - “1” indicates sensor #1 (F1)

The resulting output in the entPhysicalDescr column of the MIB would be: FAN1/FAN/F1.

3.6 Commands

3.6.1 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`	
Related Commands	show cli	
Note		

cli max-sessions

cli max-sessions <number>
no cli max-sessions

Configures the maximum number of simultaneous CLI sessions allowed. The no form of the command resets this value to its default.

Syntax Description	number Range: 3-30
Default	30 sessions
Configuration Mode	config
History	3.5.0200
Role	admin
Example	`switch (config) # cli max-sessions 40`
Related Commands	show terminal
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`
Related Commands	show terminal
Note	

terminal

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

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

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

terminal sysrq enable

	terminal sysrq enable **no terminal sysrq enable** Enable SysRq over the serial connection (RS232 or Console port). The no form of the command disables SysRq over the serial connection (RS232 or Console port).
Syntax Description	N/A
Default	Enabled
Configuration Mode	config
History	3.4.3000
Role	admin
Example	`switch (config) # terminal sysrq enable` `switch (config) #`
Related Commands	show terminal
Note	

show cli

	show cli Displays the CLI configuration and status.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

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

Related Commands	cli default
Note	

show cli max-sessions

	show cli max-sessions Displays maximum number of sessions.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.5.0200
Role	admin

Example	`switch (config) # show cli max-sessions`
	`Maximum number of CLI sessions: 5`
	`switch (config) #`

Related Commands	
Note	

show cli num-sessions

	show cli num-sessions Displays current number of sessions.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.5.0200
Role	admin

Example	`switch (config) # show cli num-sessions`
	`Current number of CLI sessions: 40`
	`switch (config) #`

Related Commands	
Note	

3.6.2 Banner

banner login

banner login <string>
no banner login

Sets the CLI welcome banner message.
The no form of the command resets the system login banner to its default.

Syntax Description	string Text string.
Default	"Mellanox MLNX-OS Switch Management"
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # banner login Example`
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	
	3.5.0200	Added no form of the command
Role	admin	
Example	`switch (config) # banner login-local Testing` `switch (config) #`	
Related Commands	show banner	
Note	• The login-local refers to the serial connection banner • If more than 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	
	3.5.0200	Added no form of the command
Role	admin	
Example	`switch (config) # banner login-remote Testing` `switch (config) #`	
Related Commands	show banner	
Note	• The login-remote refers to the SSH connections banner • If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).	

banner logout

banner logout <string>
no banner logout

Set system logout banner (for both local and remote logins).
The no form of the command resets the banner.

Syntax Description	string	Text string.
Default	N/A	
Configuration Mode	config	
History	3.5.0200	
Role	admin	
Example	`switch (config) # banner logout Testing` `switch (config) #`	
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 logout-local

banner logout-local <string>
no banner logout-local

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

Syntax Description	string	Text string.
Default	N/A	
Configuration Mode	config	
History	3.5.0200	
Role	admin	
Example	`switch (config) # banner logout-local Testing` `switch (config) #`	
Related Commands	show banner	
Note	• The logout-local refers to the serial connection banner • If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).	

banner logout-remote

banner logout-remote <string>
no banner logout-remote

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

Syntax Description	string	Text string.
Default	N/A	
Configuration Mode	config	
History	3.5.0200	
Role	admin	
Example	`switch (config) # banner logout-remote Testing` `switch (config) #`	
Related Commands	show banner	
Note	• The logout-remote refers to SSH connections banner • If more than 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

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

Syntax Description	string Text string
Default	“Mellanox Switch”
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # banner motd “My Banner”`
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”). • To insert a multi-line MotD, hit Ctrl-V (escape sequence) followed by Ctrl-J (new line sequence). The symbol “^J” should appear. Then, whatever is typed after it becomes the new line of the MotD. Remember to also include the string between quotation marks.

show banner

	show banner Displays configured banners.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000 3.5.0200 Updated Example 3.6.6000 Updated Example
Role	Any command mode

Example	`switch (config) # show banner`
	
	`Banners:`
	`  Message of the Day (MOTD):`
	`  Mellanox Switch`
	
	`  Login:`
	`  Mellanox MLNX-OS Switch Management`
	
	`  Logout:`
	`  Goodbye`

Related Commands	banner login banner login-local banner login-remote banner logout banner logout-local banner logout-remote banner motd
Note	

3.6.3 SSH

ssh server enable

ssh server enable
no ssh server enable

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

Syntax Description	N/A
Default	SSH server is enabled
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # ssh server enable`
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}

Configures host keys for SSH.

Syntax Description	key-type	• rsa1 - RSAv1 • rsa2 - RSAv2 • dsa2 - DSAv2
	private-key	Sets new private-key for the host keys of the specified type
	public-key	Sets new public-key for the host keys of the specified type
	generate	Generates new RSA and DSA host keys for SSH
Default	SSH keys are locally generated	
Configuration Mode	config	
History	3.1.0000	
	3.4.2300	Added notes
Role	admin	

Example	`switch (config) # ssh server host-key dsa2 private-key`
	`Key: ********************************************`
	`Confirm: ********************************************`	

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

ssh server listen

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

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

Syntax Description	enable	Enables SSH interface restrictions on access to this system.
	interface <inf>	Adds interface to SSH server access restriction list. Possible interfaces are “lo”, and “mgmt0”.
Default	SSH listen is enabled	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ssh server listen enable`	
Related Commands	show ssh server	
Note		

ssh server login attempts

ssh server login attempts <number>
no ssh server login attempts

Configures maximum login attempts on SSH server.
The no form of the command resets the login attempts value to its default.

Syntax Description	number	Range: 3-100 attempts.
Default	6 attempts	
Configuration Mode	config	
History	3.5.0200	
	3.5.1000	Increased minimum number of attempts allowed
Role	admin	
Example	`switch (config) # ssh server login attempts 5`	
Related Commands	show ssh server	
Note		

ssh server login timeout

ssh server login timeout <time>
no ssh server login timeout

Configures login timeout on SSH server.
The no form of the command resets the timeout value to its default.

Syntax Description	time	Range: 1-600 seconds
Default	120 seconds	
Configuration Mode	config	
History	3.5.0200	
Role	admin	
Example	`switch (config) # ssh server login timeout 130`	
Related Commands	show ssh server	
Note		

ssh server min-version

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

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

Syntax Description	version	Possible versions are 1 and 2.
Default	2	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ssh server min-version 2`	
Related Commands	show ssh server	
Note		

ssh server ports

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

Specifies which ports the SSH server listens on.

Syntax Description	port	Port number in [1...65535].
Default	22	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ssh server ports 22`	
Related Commands	show ssh server	
Note	• Multiple ports can be specified by repeating the <port> parameter • The command will remove any previous ports if not listed in the command	

ssh server security strict

	ssh server security strict Enables strict security settings. The no form of the command disables strict security settings.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.3.5060 3.6.4000
Role	admin
Example	`switch (config) # ssh server security strict`
Related Commands	show ssh server
Note	The following ciphers are disabled for SSH when strict security is enabled: • aes256-cbc • aes192-cbc • aes128-cbc • arcfour • blowfish-cbc • cast128-cbc • rijndael-cbc@lysator.liu.se • 3des-cbc

ssh server tcp-forwarding enable

	ssh server tcp-forwarding enable Enables TCP port forwarding. The no form of the command disables TCP port forwarding.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # ssh server tcp-forwarding enable`
Related Commands	show ssh server
Note	

ssh server x11-forwarding

	ssh server x11-forwarding enable **no ssh server x11-forwarding enable** Enables X11 forwarding on the SSH server. The no form of the command disables X11 forwarding.
Syntax Description	N/A
Default	X11-forwarding is disabled.
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # ssh server x11-forwarding enable`
Related Commands	N/A
Note	

ssh client global

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

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

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

Example

```
switch (config) # ssh client global host-key-check no
switch (config) # ssh client global known-host "72.30.2.2 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEArB9i5OnukAHNUOkwpCmEl0m88kJgB-
zL22+F5tfaSn+S0pVYxrceZeyuzXsoZ1VtFTk2Fydwy0YvMS0Kcv2PuCrPZV/
GYd31QEnn22rEmrlPrKCrMl1XlUy6DFlr3OgwWm1baobmDlG/gSziWz/gc4Jgqf2CyX-
Fq4pzaR1jar1Vk="

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

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

No SSH user identities configured.

No SSH authorized keys configured.

switch (config) #
```

Related Commands	show ssh client
Note	

ssh client user

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

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

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

slogin

slogin [<slogin options>] <hostname>

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

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

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

Related Commands	N/A	
Note		

show ssh client

	show ssh client Displays the client configuration of the SSH server.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

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

Related Commands	N/A
Note	

show ssh server

	show ssh server Displays SSH server configuration.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
	3.4.0000 Updated Example
	3.5.0200 Added SSH login timeout and max attempts
	3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show ssh server`
	`SSH server configuration:`
	`SSH server enabled: yes`
	`Server security strict mode: no`
	`Minimum protocol version: 2`
	`TCP forwarding enabled: yes`
	`X11 forwarding enabled: no`
	`SSH login timeout: 120`
	`SSH login max attempts: 6`
	`SSH server ports: 22`
	
	`Interface listen enabled: yes`
	`Listen Interfaces:`
	`No interface configured.`
	
	`Host Key Finger Prints and Key Lengths:`
	`RSA v1 host key: SHA256:sMgangJjG9FmSch/9Y9aZ/WJ2wKf3c+SeF8XKgYYdCA (2048)`
	`RSA v2 host key: SHA256:gVu6qLW1ZifEp8wRer2jkvILZMGNl6VCYU3HqC1INC8 (2048)`
	`DSA v2 host key: SHA256:JnldTEla20ZF/c5LdIqo9251DzO742k3hFCQh3Jt4ZA (1024)`

Related Commands	ssh server
Note	

show ssh server host-keys

show ssh server host-keys

Displays SSH host key configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show ssh server host-keys`
	`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 login timeout: 120`
	`SSH login max attempts: 6`
	`SSH server ports: 22`
	
	`Interface listen enabled: yes`
	`Listen Interfaces:`
	`No interface configured.`
	
	`Host Key Finger Prints and Key Lengths:`
	`RSA v1 host key: SHA256:sMgangJjG9FmSch/9Y9aZ/WJ2wKf3c+SeF8XKgYYdCA (2048)`
	`RSA v2 host key: SHA256:gVu6qLW1ZifEp8wRer2jkvILZMGNl6VCYU3HqC1INC8 (2048)`
	`DSA v2 host key: SHA256:JnldTEla20ZF/c5LdIqo9251DzO742k3hFCQh3Jt4ZA (1024)`
	
	`Host Keys:`
	`RSA v1 host key: "kebo-2100-1 2048 65537 21801469875<...>27851"`
	`RSA v2 host key: "kebo-2100-1 ssh-rsa AAAAB3Nza<...>KE5"`
	`DSA v2 host key: "kebo-2100-1 ssh-dss AAAAB3Nza<...>/s="`

Related Commands	ssh server host-keys
Note	

3.6.4 Remote Login

telnet

telnet

Logs into another system using telnet.

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

telnet-server enable

	telnet-server enable **no telnet-server enable** Enables the telnet server. The no form of the command disables the telnet server.
Syntax Description	N/A
Default	Telnet server is disabled
Configuration Mode	config
History	3.1.0000
Role	admin

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

Related Commands	show telnet-server
Note	

show telnet-server

	show telnet-server Displays telnet server settings.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

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

Related Commands	telnet-server enable
Note	

3.6.5 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	
Role	admin	
Example	`switch (config) # web auto-logout 60`	
Related Commands	show web	
Note	The no form of the command does not automatically log users out due to inactivity.	

web cache-enable

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

web client cert-verify

	web client cert-verify **no web client cert-verify** Enables verification of server certificates during HTTPS file transfers. The no form of the command disables verification of server certificates during HTTPS file transfers.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.2.3000
Role	admin
Example	`switch (config) # web client cert-verify`
Related Commands	N/A
Note	

web client ca-list

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

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

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

web enable

	web enable **no web enable** Enables the web-based management console. The no form of the command disables the web-based management console.
Syntax Description	N/A
Default	enable
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # web enable`
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 disabled HTTP TCP port is 80 HTTP redirect to HTTPS is disabled	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # web http enable`	
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	`switch (config) # web httpd listen enable`	
Related Commands	N/A	
Note	If enabled, and if at least one of the interfaces listed is eligible to be a listen interface, then HTTP/HTTPS requests will only be accepted on those interfaces. Otherwise, HTTP/HTTPS requests are accepted on any interface.	

web https

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

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

Syntax Description	certificate regenerate	Re-generates certificate to use for HTTPS connections.
	certificate name	Configure the named certificate to be used for HTTPS connections
	certificate default-cert	Configure HTTPS to use the configured default certificate
	enable	Enables HTTPS access to the web-based management console.
	port	Sets a TCP port for HTTPS access.
	ssl ciphers {all | TLS | TLS1.2}	Sets ciphers to be used for HTTPS.
Default	HTTPS is enabled Default port is 443	
Configuration Mode	config	
History	3.1.0000	
	3.4.0000	Added “ssl ciphers” parameter
	3.4.0010	Added TLS parameter to “ssl ciphers”
Role	admin	
Example	`switch (config) # web https enable`	
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 https ssl renegotiation enable

	web https ssl renegotiation enable **no web https ssl renegotiation enable** Enables SSL renegotiation flag in httpd web server. The no form of the command disables SSL renegotiation flag in httpd web server.
Syntax Description	N/A
Default	HTTPS is enabled Default port is 443
Configuration Mode	config
History	3.6.8008
Role	admin
Example	`switch (config) # web https ssl renegotiation enable`
Related Commands	show web web enable
Note	

web https ssl secure-cookie enable

	web https ssl secure-cookie enable **no web https ssl secure-cookie enable** Enables SSL secure-cookie flag in httpd web server. The no form of the command disables secure-cookie flag in httpd web server.
Syntax Description	N/A
Default	Enabled
Configuration Mode	config
History	3.6.8008
Role	admin
Example	`switch (config) # web https ssl secure-cookie enable`
Related Commands	show web web enable
Note	

web proxy auth authtype

web https auth authtype <auth-type>
no web https auth authtype

Configures type of authentication to use with web proxy.
The no form of the command resets web proxy authentication type to its default.

Syntax Description	auth-type	Possible values: • none – no authentication • basic – HTTP basic authentication
Default	Basic authentication settings	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # web https auth authtype basic`	
Related Commands	show web web enable	
Note		

web proxy auth basic

web https auth basic {password <password> | username <username>}
no web https auth basic {password | username}

Configures HTTP basic authentication settings for proxy.
The no form of the command clears password or username configuration.

Syntax Description	password	Sets plaintext password for HTTP basic authentication with web proxy
	username	Sets username for HTTP basic authentication with web proxy
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # web https auth basic password 57R0ngP455w0rD`	
Related Commands	show web web enable	
Note		

web proxy auth host

web https auth host <ip-address> [port <number>]

Configures web proxy host.

Syntax Description	port	Sets web proxy default port
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # web https auth host 2001:0db8:85a3::8a2e:0370:7334 port 3`	
Related Commands	show web web enable	
Note		

show web

	show web Displays WebUI configuration.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.6000 3.6.8008 Updated Example
Role	admin

Example	`switch (config) # show web`
	`Web User Interface:`
	`  Web interface enabled:  yes`
	`  Web caching enabled:  no`
	`  HTTP enabled:  no`
	`  HTTP port:  80`
	`  HTTP redirect to HTTPS:  no`
	`  HTTPS enabled:  yes`
	`  HTTPS port:  443`
	`  HTTPS ssl-ciphers:  TLS1.2`
	`  HTTPS ssl-renegotiation: no`
	`  HTTPS ssl-secure-cookie: yes`
	`  HTTPS certificate name:  default-cert`
	`  Listen enabled:  yes`
	`  Listen Interfaces:`
	`  No interface configured.`
	
	`  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`

Related Commands	
Note	

4 System Management

4.1 Management Interface

Management interfaces are used in order to provide access to switch management user interfaces (e.g. CLI, WebUI). Mellanox switches support out-of-band (OOB) dedicated interfaces (e.g. mgmt0, mgmt1) and in-band dedicated interfaces. In addition, most Mellanox switches feature a serial port that provides access to the CLI only.

On switch systems with two OOB management ports, both of them may be configured on the same VLAN if needed. In this case, ARP replies to the IP of those management interfaces is answered from either of them.

4.1.1 Configuring Management Interfaces with Static IP Addresses

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

Step 1. Enter Config configuration mode. Run:

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

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

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

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

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

4.1.2 Configuring IPv6 Address on the Management Interface

Step 1. Enable IPv6 on this interface. Run:

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

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

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

Step 3. Verify the IPv6 address is configured correctly. Run:

```
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 10.10.0.2
switch (config)# show ip route
Destination      Mask            Gateway         Interface   Source   Distance/Metric
default          0.0.0.0          10.10.0.2      mgmt0       static   0/0
10.10.0.0        255.255.254.0    0.0.0.0        mgmt0       direct   0/0
switch (config)#
```

4.1.5 Configuring Hostname via DHCP (DHCP Client Option 12)

This feature, also known as the DHCP Client Option 12, is enabled by default and assigns the switch system a hostname via DHCP as long as network manager configures hostname to the management interfaces’ (i.e. mgmt0, mgmt1) MAC address. If a network manager configures the hostname manually through any of the user interfaces, the hostname is not retrieved from the DHCP server.

- ***To enable fetching hostname from DHCP server, run:***

```
switch (config interface mgmt0) # dhcp hostname
```

- ***To disable fetching hostname from DHCP server, run:***

```
switch (config interface mgmt0) # no dhcp hostname
```

Getting the hostname through DHCP is enable by default and will change the switch hostname if the hostname is not set by the user. Therefore, if a switch is part of an HA cluster (e.g. SM HA, GW HA) the user would need to make sure the HA master has the same HA node names as the DHCP server.

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> | ib0}

Enters a management interface context.

Syntax Description	mgmt0	Management port 0 (out of band).
	mgmt1	Management port 1 (out of band).
	lo	Loopback interface.
	vlan<id>	In-band management interface (e.g. vlan10).
	ib0	IPoIB in-band management
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # interface mgmt0` `switch (config interface mgmt0) #`	
Related Commands	show interfaces <ifname>	
Notes		

ip address

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

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

Syntax Description	IP address	IPv4 address
	netmask	Subnet mask of IP address
Default	0.0.0.0/0	
Configuration Mode	config interface management	
History	3.1.0000	
Role	admin	
Example	`switch (config) # interface mgmt0` `switch (config interface mgmt0) # ip address 10.10.10.10 255.255.255.0`	
Related Commands	show interfaces <ifname>	
Notes	If DHCP is enabled on the specified interface, then the DHCP IP assignment will hold until DHCP is disabled.	

ip default-gateway

	ip default-gateway <next hop IP address or interface name> **no ip default-gateway** Configures a default route. The no form of the command removes the current default route.
Syntax Description	next hop IP address or interface name — IP address, lo, mgmt0, or mgmt1.
Default	N/A
Configuration Mode	config interface management
History	3.1.0000
Role	admin
Example	`switch (config) # ip default-gateway mgmt1` `switch (config) #`
Related Commands	
Notes	

alias

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

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

Syntax Description	index	A number that is to be aliased to (associated with) the secondary IP.
	IP address	Additional IP address.
	netmask	Subnet mask of the IP address.
Default	N/A	
Configuration Mode	config interface management	
History	3.1.0000	
Role	admin	
Example	`switch (config interface mgmt0) # alias 2 ip address 9.9.9.9 255.255.255.255`	
Related Commands	show interfaces <ifname>	
Notes	• If DHCP is enabled on the specified interface, then the DHCP IP assignment will hold until DHCP is disabled • More than one additional IP address can be added to the interface	

mtu

mtu <bytes>
no mtu <bytes>

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

Syntax Description	bytes	The entry range is 68-1500.
Default	1500	
Configuration Mode	config interface management	
History	3.6.3004	
Role	admin	
Example	`switch (config interface mgmt0) # mtu 1500`	
Related Commands	show interfaces <ifname>	
Notes		

duplex

duplex <duplex>
no duplex

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

Syntax Description	duplex	Sets the duplex mode of the interface. The following are the possible values: • half - half duplex • full - full duplex • auto - auto duplex sensing (half or full)
Default	auto	
Configuration Mode	config interface management	
History	3.1.0000	
Role	admin	
Example	`switch (config interface mgmt0) # duplex auto`	
Related Commands	show interfaces <ifname>	
Notes	• Setting the duplex to “auto” also sets the speed to “auto” • Setting the duplex to one of the settings “half” or “full” also sets the speed to a manual setting which is determined by querying the interface to find out its current auto-detected state	

speed

speed <speed>
no speed

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

Syntax Description	speed	Sets the speed of the interface. The following are the possible values: • 10 - fixed to 10Mbps • 100 - fixed to 1000Mbps • 1000 - fixed to 1000Mbps • auto - auto speed sensing (10/100/1000Mbps)
Default	auto	
Configuration Mode	config interface management	
History	3.1.0000	
Role	admin	
Example	`switch (config interface mgmt0) # speed auto`	
Related Commands	show interfaces <ifname>	
Notes	• Setting the speed to “auto” also sets the duplex to “auto” • Setting the speed to one of the manual settings (generally “10”, “100”, or “1000”) also sets the duplex to a manual setting which is determined by querying the interface to find out its current auto-detected state	

dhcp

dhcp [renew]
no dhcp

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

Syntax Description	renew	Forces a renewal of the IP address. A restart on the DHCP client for the specified interface will be issued.
Default	Could be enabled or disabled (per part number) manufactured with 3.2.0500	
Configuration Mode	config interface management	
History	3.1.0000	
Role	admin	
Example	`switch (config interface mgmt0) # dhcp`	
Related Commands	show interfaces <ifname> configured	
Notes	• When enabling DHCP, the IP address and netmask are received via DHCP hence, the static IP address configuration is ignored • Enabling DHCP disables zeroconf and vice versa • Setting a static IP address and netmask does not disable DHCP. DHCP is disabled using the “no” form of this command, or by enabling zeroconf.	

dhcp hostname

	dhcp hostname **no dhcp hostname** Enables fetching the hostname from DHCP for this interface. The no form of the command disables fetching the hostname from DHCP for this interface.
Syntax Description	N/A
Default	Enabled
Configuration Mode	config interface management
History	3.5.1000
Role	admin
Example	`switch (config interface mgmt0) # dhcp hostname` `switch (config interface mgmt0) #`
Related Commands	hostname <hostname> show interfaces <ifname> configured
Notes	• If a hostname is configured manually by the user, that configuration would override the “dhcp hostname” configuration • After upgrading to version 3.5.1000 when a default hostname is not configured, the DHCP server assigns the new hostname for your machine • These commands do not work on in-band interfaces

shutdown

	shutdown **no shutdown** Disables the specified interface. The no form of the command enables the specified interface.
Syntax Description	N/A
Default	no shutdown
Configuration Mode	config interface management
History	3.1.0000
Role	admin
Example	`switch (config interface mgmt0) # no shutdown`
Related Commands	show interfaces <ifname> configured
Notes	

zeroconf

	zeroconf **no zeroconf** Enables zeroconf on the specified interface. It randomly chooses a unique link-local IPv4 address from the 169.254.0.0/16 block. This command is an alternative to DHCP. The no form of the command disables the use of zeroconf on the specified interface.
Syntax Description	N/A
Default	no zeroconf
Configuration Mode	config interface management
History	3.1.0000
Role	admin
Example	`switch (config interface mgmt0) # zeroconf`
Related Commands	show interfaces <ifname> configured
Notes	Enabling zeroconf disables DHCP and vice versa.

comment

comment <comment>
no comment

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

Syntax Description	comment	A free-form string that has no semantics other than being displayed when the interface records are listed.
Default	no comment	
Configuration Mode	config interface management	
History	3.1.0000	
Role	admin	
Example	`switch (config interface mgmt0) # comment my-interface`	
Related Commands	N/A	
Notes		

ipv6 enable

	ipv6 enable **no ipv6 enable** Enables all IPv6 addressing for this interface. The no form of the command disables all IPv6 addressing for this interface.
Syntax Description	N/A
Default	IPv6 addressing is disabled
Configuration Mode	config interface management
History	3.1.0000
Role	admin
Example	`switch (config interface mgmt0) # ipv6 enable`
Related Commands	ipv6 address show interface <ifname>
Notes	• The interface identifier is a 64-bit long modified EUI-64, which is based on the MAC address of the interface • If IPv6 is enabled on an interface, the system will automatically add a link-local address to the interface. Link-local addresses can only be used to communicate with other hosts on the same link, and packets with link-local addresses are never forwarded by a router. • A link-local address, which may not be removed, is required for proper IPv6 operation. The link-local addresses start with “fe80::”, and are combined with the interface identifier to form the complete address.

ipv6 address

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

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

Syntax Description	IPv6 address/netmask	Configures a static IPv6 address and netmask. Format example: 2001:db8:1234::5678/64.
	autoconfig	Enables IPv6 stateless address auto configuration (SLAAC) for this interface. An address will be automatically added to the interface based on an IPv6 prefix learned from router advertisements, combined with an interface identifier.
	autoconfig default	Enables default learning routes. The default route will be discovered automatically, if the autoconfig is enabled.
	autoconfig privacy	Uses privacy extensions for SLAAC to construct the autoconfig address, if the autoconfig is enabled.
Default	No IP address available, auto config is enabled	
Configuration Mode	config interface management	
History	3.1.0000	
Role	admin	
Example	`switch (config interface mgmt0) # ipv6 fe80::202:c9ff:fe5e:a5d8/64`	
Related Commands	ipv6 enable show interface <ifname>	
Notes	• On a given interface, up to 16 addresses can be configured • For Ethernet, the default interface identifier is a 64-bit long modified EUI-64, which is based on the MAC address of the interface	

ipv6 dhcp primary-intf

	ipv6 dhcp primary-intf <if-name> **no ipv6 dhcp primary-intf** Sets the interface from which non-interface-specific (resolver) configuration is accepted via DHCPv6. The no form of the command resets non-interface-specific (resolver) configuration.	
Syntax Description	if-name	Interface name: • lo • mgmt0 • mgmt1
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ipv6 dhcp primary-intf mgmt0` `switch (config) #`	
Related Commands	ipv6 enable ipv6 address show interface <ifname>	
Notes		

ipv6 dhcp stateless

	ipv6 dhcp stateless **no ipv6 dhcp stateless** Enables stateless DHCPv6 requests. The no form of the command disables stateless DHCPv6 requests.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # ipv6 dhcp stateless` `switch (config) #`
Related Commands	ipv6 enable ipv6 address show interface <ifname>
Notes	• This command only gets DNS configuration, not an IPv6 address • The no form of the command requests all information, including an IPv6 address

show interfaces mgmt0

	show interface mgmt0 Displays information on the management interface configuration and status.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.6.8008 Updated Example
Role	admin

Example

```
switch (config) # show interfaces mgmt0

Interface mgmt0 status:
  Comment         :
  Admin up        : yes
  Link up         : yes
  DHCP running    : yes
  IP address      : 10.12.67.33
  Netmask         : 255.255.255.128
  IPv6 enabled    : yes
  Autoconf enabled: no
  Autoconf route  : yes
  Autoconf privacy: no
  DHCPv6 running  : yes (but no valid lease)
  IPv6 addresses  : 1

  IPv6 address:
    fe80::268a:7ff:fe53:3d8e/64

  Speed           : 1000Mb/s (auto)
  Duplex          : full (auto)
  Interface type  : ethernet
  Interface source: bridge
  MTU             : 1500
  HW address      : 24:8A:07:53:3D:8E

  Rx:
    2055054  bytes
      28830  packets
          0  mcast packets
          0  discards
          0  errors
          0  overruns
          0  frame

  Tx:
    377716  bytes
      3200  packets
         0  discards
         0  errors
         0  overruns
         0  carrier
         0  collisions
         0  queue len
```

Related Commands N/A

Notes

show interfaces mgmt0 brief

show interface mgmt0 brief

Displays brief information on the management interface configuration and status.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.6.8008 Updated Example
Role	admin

Example	`switch (config) # show interfaces mgmt0 brief`
	
	`Interface mgmt0 status:`
	`  Comment : `
	`  Admin up : yes`
	`  Link up : yes`
	`  DHCP running : yes`
	`  IP address : 10.12.67.33`
	`  Netmask : 255.255.255.128`
	`  IPv6 enabled : yes`
	`  Autoconf enabled: no`
	`  Autoconf route : yes`
	`  Autoconf privacy: no`
	`  DHCPv6 running : yes (but no valid lease)`
	`  IPv6 addresses : 1`
	
	`  IPv6 address:`
	`  fe80::268a:7ff:fe53:3d8e/64`
	
	`  Speed : 1000Mb/s (auto)`
	`  Duplex : full (auto)`
	`  Interface type : ethernet`
	`  Interface source: bridge`
	`  MTU : 1500`
	`  HW address : 24:8A:07:53:3D:8E`

Related Commands	N/A
Notes	

show interfaces mgmt0 configured

show interface mgmt0 configured

Displays configuration information about the specified interface.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
	3.5.1000 Updated Example with “DHCP Hostname”
	3.6.8008 Updated Example
Role	admin

Example	`switch (config) # show interfaces mgmt0 configured`
	
	`Interface mgmt0 configuration:`
	`  Comment  :`
	`  Enabled  : yes`
	`  DHCP  : yes`
	`  DHCP Hostname  : yes`
	`  Zeroconf  : no`
	`  IP address  :`
	`  Netmask  :`
	`  IPv6 enabled  : yes`
	`  Autoconf enabled: no`
	`  Autoconf route  : yes`
	`  Autoconf privacy: no`
	`  DHCPv6 enabled  : yes`
	`  IPv6 addresses  : 0`
	`  Speed  : auto`
	`  Duplex  : auto`
	`  MTU  : 1500`

Related Commands	N/A
Notes	

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	
	3.6.3004	Added support for the character “.”
Role	admin	
Example	`switch (config) # hostname my-switch-hostname`	
Related Commands	show hosts	
Notes	• Hostname may contain letters, numbers, periods (‘.’), and hyphens (‘-’), in any combination • Hostname may be 1-63 characters long • Hostname may not begin with a hyphen • Hostname may not contain other characters, such as “%”, “_” etc. • Hostname may not be set to one of the valid logging commands (i.e. debug-files, fields, files, format, level, local, monitor, receive, trap) • Changing the hostname stamps a new HTTPS certificate	

ip name-server

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

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

Syntax Description	IPv4/v6 address	IPv4 or IPv6 address.
Default	No server name	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ip name-server 9.9.9.9`	
Related Commands	show hosts	
Notes		

ip domain-list

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

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

Syntax Description	domain-name	The domain name in a string form. A domain name is an identification string that defines a realm of administrative autonomy, authority, or control in the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS).
Default	No static domain name	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ip domain-list mydomain.com`	
Related Commands	show hosts	
Notes		

ip/ipv6 host

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

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

Syntax Description	hostname	The hostname in a string form.
	IP Address	The IPv4 or IPv6 address.
Default	No static domain name.	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ip host my-host 2.2.2.2` `switch (config) # ipv6 host my-ipv6-host  2001::8f9`	
Related Commands	show hosts	
Notes		

ip/ipv6 map-hostname

	{ip |ipv6} map-hostname **no {ip | ipv6} map-hostname** Maps between the currently-configured hostname and the loopback address 127.0.0.1. The no form of the command clears the mapping.
Syntax Description	N/A
Default	IPv4 mapping is enabled by default IPv6 mapping is disabled by default
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # ip map-hostname`
Related Commands	show hosts
Notes	• If no mapping is configured, a mapping between the hostname and the IPv4 loop-back address 127.0.0.1 will be added • The no form of the command maps the hostname to the IPv6 loopback address if there is no statically configured mapping from the hostname to an IPv6 address (disabled by default) • Static host mappings are preferred over DNS results. As a result, with this option set, you will not be able to look up your hostname on your configured DNS server; but without it set, some problems may arise if your hostname cannot be looked up in DNS.

show hosts

	show hosts Displays hostname, DNS configuration, and static host mappings.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

Example	`switch (config) # show hosts`
	`Hostname: my-host-name`
	`Name server: 9.9.9.9 (configured)`
	`Name server: 11.11.11.11 (dynamic)`
	`Name server: 12.12.12.12 (dynamic)`
	`Name server: 13.13.13.13 (dynamic)`
	`Domain name: mydomain.com (configured)`
	`Domain name: example1.com (dynamic)`
	`Domain name: example2.com (dynamic)`
	`Domain name: example3.com (dynamic)`
	`Domain name: example4.com (dynamic)`
	`IP 1.1.1.1 maps to hostname p`
	`IP 3.3.3.3 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`

Related Commands	N/A
Notes	

4.1.6.3 Routing

{ip | ipv6} route

{ip | ipv6} route [vrf <vrf-name>] {<network-prefix> <netmask> | <network-prefix>/<masklen>} <next-hop>
no {ip | ipv6} route [vrf <vrf-name>] {<network-prefix> <netmask> | <network-prefix>/<masklen>} <next-hop>

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`	
Related Commands	show ip route	
Notes		

ipv6 default-gateway

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

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

Syntax Description	ip address	The default gateway IP address (IPv6).
	ifname	The interface name (e.g., mgmt0, mgmt1).
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
	3.2.0500	removed IPv4 configuration option
Role	admin	
Example	`switch (config) # ipv6 default-gateway ::1`	
Related Commands	show ip/ipv6 route show ipv6 default-gateway	
Notes	• The configured default gateway will not be used if DHCP is enabled. • In order to configure ipv4 default-gateway use ‘ip route’ command.	

show ip/ipv6 route

show {ip | ipv6} route [static]

Displays the routing table in the system.

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

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

Related Commands	ip route	
Notes		

show ipv6 default-gateway

show ipv6 default-gateway [static]

Displays the default gateway.

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

Example	`switch (config) # ipv6 default-gateway 10.10.10.10`
	`switch (config) # show ipv6 default-gateway`
	`Active default gateways:`
	`  172.30.0.1 (interface: mgmt0)`
	`switch (config) # show ipv6 default-gateway static`
	`Configured default gateway: 10.10.10.10`	

Related Commands	ipv6 default-gateway	
Notes	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`	
Related Commands	show ip arp ip route	
Notes		

ip arp timeout

ip arp [vrf <vrf-name>] timeout <timeout-value>
no ip arp [vrf <vrf-name>] timeout

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

Syntax Description	timeout-value	Time (in seconds) that an entry remains in the ARP cache. Range: 60-28800.
	vrf-name	VRF session name
Default	1500 seconds	
Configuration Mode	config	
History	3.2.0230	
	3.5.1000	Added VRF parameter and updated Notes
Role	admin	
Example	`switch (config) # ip arp timeout 2000` `switch (config) #`	
Related Commands	ip arp show ip arp	
Notes	• This value is used as the default ARP timeout whenever a new IP interface is created • The time interval after which each ARP entry becomes stale may actually vary from 50-150% of the configured value	

show ip arp

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

Displays ARP table.

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

Example	`switch-626a54 [standalone: master] (config) # show ip arp`
	
	`Total number of entries: 3`
	
	`  Address             Type           Hardware Address         Interface`
	`  ------------------------------------------------------------------------`
	`---`
	`  10.209.0.1           Dynamic ETH     00:00:5E:00:01:01         mgmt0`
	`  10.209.1.120         Dynamic ETH     00:02:C9:62:E8:C2         mgmt0`
	`  10.209.1.121         Dynamic ETH     00:02:C9:62:E7:42         mgmt0`
	`switch (config) # show ip arp count`
	`ARP Table size: 3 (inband: 0, out of band: 3)`
	`switch (config) #`	

Related Commands		
Notes		

ipv6 neighbor

ipv6 neighbor <ipv6-address> <ifname> <mac-address>
no ipv6 neighbor <ipv6-address> <ifname> <mac-address>

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

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

clear ipv6 neighbors

	clear ipv6 neighbors Clears the dynamic neighbors cache.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000 3.6.4110 Updated command.
Role	admin
Example	`switch (config) # clear ipv6 neighbors` `switch (config) #`
Related Commands	ipv6 neighbor show ipv6 neighbor arp
Notes	• Clearing Neighbor Discovery Protocol (NDP) cache removes only the dynamic entries learned and not the static entries configured • Use the no form of the command to remove static entries

show ipv6 neighbors

show ipv6 neighbors [static]

Displays the Neighbor Discovery Protocol (NDP) table.

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

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

Related Commands	ipv6 neighbor clear ipv6 neighbor show ipv6	
Notes		

4.1.6.5 DHCP

ip dhcp

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

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

Syntax Description	yield-to-static|	Does not allow you to install a default gateway from DHCP if there is already a statically configured one.
	hostname	Specifies the hostname to be sent during DHCP client negotiation if send-hostname is enabled.
	primary-intf <ifname>	Sets the interface from which a non-interface-specific configuration (resolver and routes) will be accepted via DHCP.
	send-hostname	Enables the DHCP client to send a hostname during negotiation.
Default	no ip dhcp yield-to-static no ip dhcp hostname ip ip dhcp primary-intf mgmt0 no ip dhcp send-hostname	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ip dhcp default-gateway yield-to-static`	
Related Commands	show ip dhcp dhcp [renew]	
Notes	DHCP is supported for IPv4 networks only.	

show ip dhcp

	show ip dhcp Displays the DHCP configuration and status.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.6.5000 Updated Example
Role	admin

Example	`switch (config) # show ip dhcp`
	`----------`
	`Interface DHCP DHCP Valid`
	`Enabled Running lease`
	`----------`
	`dummy0 no no no`
	`lo no no no`
	`mgmt0 yes yes yes`
	`mgmt1 no no no`
	`mgmts0 no no no`
	`mgmts1 no no no`
	`vif1 no no no`
	
	`IPv4 dhcp default gateway yields to static configuration: no`
	
	`DHCP primary interface:`
	`Configured: mgmt0`
	`Active: mgmt0`
	
	`DHCP client options:`
	`Send Hostname: no`
	`Client Hostname: 1.1.1.1`

Related Commands	ip dhcp dhcp [renew]
Notes	

4.1.6.6 IP Diagnostic Tools

ping

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

Sends ICMP echo requests to a specified host.

Syntax Description	Linux Ping options	https://www.lifewire.com/uses-of-command-ping-2201076
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

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

Related Commands	traceroutes	
Notes		

traceroute

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

Traces the route packets take to a destination.

Syntax Description	-4	Uses IPv4
	-6	Uses IPv6
	-d	Enables socket level debugging
	-F	Sets DF (do not fragment bit) on
	-I	Uses ICMP ECHO for tracerouting
	-T	Uses TCP SYN for tracerouting
	-U	Uses UDP datagram (default) for tracerouting
	-n	Does not resolve IP addresses to their domain names
	-r	Bypasses the normal routing and send directly to a host on an attached network
	-A	Performs AS path lookups in routing registries and print results directly after the corresponding addresses
	-V	Prints version info and exit
	-f	Starts from the first_ttl hop (instead from 1)
	-g	Routes packets through the specified gateway (maximum 8 for IPv4 and 127 for IPv6)
	-i	Specifies a network interface with which to operate
	-m	Sets the max number of hops (max TTL to be reached). Default is 30
	-N	Sets the number of probes to be tried simultaneously (default is 16)
	-p	Uses destination port. It is an initial value for the UDP destination port (incremented by each probe, default is 33434), for the ICMP seq number (incremented as well, default from 1), and the constant destination port for TCP tries (default is 80).
	-t	Sets the TOS (IPv4 type of service) or TC (IPv6 traffic class) value for outgoing packets
	-l	Uses specified flow_label for IPv6 packets

	-w	Sets the number of seconds to wait for response to a probe (default is 5.0). Non-integer (float point) values allowed too.
	-q	Sets the number of probes per each hop. Default is 3.
	-s	Uses source src_addr for outgoing packets.
	-z	Sets minimal time interval between probes (default is 0). If the value is more than 10, then it specifies a number in milliseconds, else it is a number of seconds (float point values allowed too).
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

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

Related Commands		
Notes		

tcpdump

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

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

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

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

Related Commands	N/A
Notes	

4.2 NTP, Clock & Time Zones

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

For an example, please refer to "HowTo enable NTP on Mellanox switches" in the Mellanox Community (https://community.mellanox.com).

4.2.1 NTP Authenticate

When authentication of incoming NTP packets is enabled, the switch ensures that they come from an authenticated time source before using them for time synchronization on the switch. Authentication keys are created and added to the trusted list.

➢ ***To add a key to be used for authentication***

Step 1. Create the key. Run:

```
switch (config)# ntp authentication-key 1 md5 password
```

Step 2. Add the key to the trusted list. Run:

```
switch (config)# ntp trusted-key 1
```

Step 3. Assign the key to the server/peer. Run:

```
switch (config)# ntp server 10.34.1.1 keyID 1
```

4.2.2 NTP Authentication Key

An authentication key may be created and used to authenticate incoming NTP packets.

For the key to be used:

1. It should be shared with the NTP server/peer sending the NTP packet.
2. It should be added to the trusted list.
3. NTP authenticate should be enabled on the switch.

4.2.3 Commands

clock set

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

Sets the time and date.

Syntax Description	hh:mm:ss	Time.
	yyyy/mm/dd	Date.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # clock set 23:23:23 2010/08/19`	
Related Commands	show clock	
Notes	If not specified, the date will be left the same.	

clock timezone

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

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

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

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

Syntax Description	zone word	The possible forms this could take include: continent, city, continent, country, city, continent, region, country, city, ocean, and/or island.
Default	GMT	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # clock timezone America North United_States Other New_York`	
Related Commands	show clock	
Notes		

ntp

ntp {disable | enable | {peer | server} <IP address> [version <number> | disable]}
no ntp {disable | enable | {peer | server} <IP address> [version <number> | 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: 3 or 4
Default	NTP is enabled NTP version number is 4	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # no ntp peer 192.168.10.24 disable` `switch (config) #`	
Related Commands	N/A	
Notes		

ntpdate

ntpdate <IP address>

Sets the system clock using the specified SNTP server.

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

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

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

ntp authenticate

	ntp authenticate **no ntp authenticate** Enables NTP authentication. The no form of the command disables NTP authentication.
Syntax Description	N/A N/A
Default	Disabled
Configuration Mode	config
History	3.5.0200
Role	admin
Example	`switch (config) # ntp authenticate`
Related Commands	N/A
Notes	

ntp authentication-key

ntp authentication-key <key_id> <encrypt_type> [<password>]
no ntp authentication-key <key_id>

Adds a new authentication key and stores it.
The no form of the command removes key ID configuration if it exists.

Syntax Description	key_id	Specifies a key ID, whether existing or a new one to be added. Range: 1-65534.
	encrypt_type	Specifies encryption type to use (md5, or sha1)
	password	Password string
Default	Disabled	
Configuration Mode	config	
History	3.5.0200	
Role	admin	

Example	`switch (config) # ntp authentication-key 123 md5 examplepass`
	`switch (config) # ntp authentication-key 1234 sha1`
	`Password: **`
	`Confirm: **`
	`switch (config) #`	

Related Commands	N/A	
Notes	If a password is not entered, a prompt appears requiring that a password is introduced.	

ntp peer disable

ntp peer <ip_address> disable
no ntp peer <ip_address> disable

Temporarily disables this NTP peer.
The no form of the command enables this NTP peer.

Syntax Description	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
Default	Disabled	
Configuration Mode	config	
History	3.5.0200	
	3.6.4000	Added hostname as option for ip_address, and added Notes.
Role	admin	
Example	`switch (config) # ntp peer 10.10.10.10 disable` `switch (config) #`	
Related Commands	N/A	
Notes	• IP addresses must be in IPv4 format (e.g., '192.168.0.1') or IPv6 format with scope zone id for IPv6 link-local addresses (e.g., '2001:db8:701f::8f9' or 'fe80::21c:23f:ec1:4fb%7'.) • The length of a hostname is limited to 255 characters. Each label (node delimited by a dot in the hostname) is limited to 63 characters and may contain letters, numbers and hyphens ('-'), but may not begin with a hyphen.	

ntp peer keyID

ntp peer <ip_address> keyID <key_id>
no ntp peer <ip_address> keyID <key_id>

Specifies the KeyID of the NTP peer.
The no form of the command removes key ID configuration from the NTP peer.

Syntax Description	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
	key_id	Range: 1-65534
Default	Disabled	
Configuration Mode	config	
History	3.5.0200	
	3.6.4000	Added hostname as ip_address option and added Notes.
Role	admin	
Example	`switch (config) # ntp peer 10.10.10.10 keyID 120`	
Related Commands	N/A	
Notes	• IP addresses must be in IPv4 format (e.g., '192.168.0.1') or IPv6 format with scope zone id for IPv6 link-local addresses (e.g., '2001:db8:701f::8f9' or 'fe80::21c:23f:ec1:4fb%7'.) • The length of a hostname is limited to 255 characters. Each label (node delimited by a dot in the hostname) is limited to 63 characters and may contain letters, numbers and hyphens ('-'), but may not begin with a hyphen.	

ntp peer version

ntp peer <ip_address> version <ver_num>
no ntp peer <ip_address> version <ver_num>

Specifies the NTP version number of this peer.
The no form of the command defaults NTP to version 4.

Syntax Description	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
	ver_num	NTP version (3 or 4)
Default	4	
Configuration Mode	config	
History	3.5.0200	
	3.6.4000	Added hostname as ip_address option and added Notes.
Role	admin	
Example	`switch (config) # ntp peer 10.10.10.10 version 4`	
Related Commands	N/A	
Notes	• IP addresses must be in IPv4 format (e.g., '192.168.0.1') or IPv6 format with scope zone id for IPv6 link-local addresses (e.g., '2001:db8:701f::8f9' or 'fe80::21c:23f:ec1:4fb%7'.) • The length of a hostname is limited to 255 characters. Each label (node delimited by a dot in the hostname) is limited to 63 characters and may contain letters, numbers and hyphens ('-'), but may not begin with a hyphen.	

ntp server disable

ntp server <ip_address> disable
no ntp server <ip_address> disable

Temporarily disables this NTP server.
The no form of the command enables this NTP server.

Syntax Description	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
Default	Disabled	
Configuration Mode	config	
History	3.5.0000	
	3.6.4000	Added hostname as ip_address option and added Notes.
Role	admin	
Example	`switch (config) # ntp server 10.10.10.10 disable` `switch (config) #`	
Related Commands	N/A	
Notes	• IP addresses must be in IPv4 format (e.g., '192.168.0.1') or IPv6 format with scope zone id for IPv6 link-local addresses (e.g., '2001:db8:701f::8f9' or 'fe80::21c:23f:ec1:4fb%7'.) • The length of a hostname is limited to 255 characters. Each label (node delimited by a dot in the hostname) is limited to 63 characters and may contain letters, numbers and hyphens ('-'), but may not begin with a hyphen.	

ntp server keyID

ntp server <ip_address> keyID <key_id>
no ntp server <ip_address> keyID <key_id>

Specifies the KeyID of the NTP server.
The no form of the command removes key ID configuration from the NTP server.

Syntax Description	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
	key_id	Range: 1-65534
Default	Disabled	
Configuration Mode	config	
History	3.5.0200	
	3.6.4000	Added hostname as ip_address option and added Notes.
Role	admin	
Example	`switch (config) # ntp server 10.10.10.10 keyID 120`	
Related Commands	N/A	
Notes	• IP addresses must be in IPv4 format (e.g., '192.168.0.1') or IPv6 format with scope zone id for IPv6 link-local addresses (e.g., '2001:db8:701f::8f9' or 'fe80::21c:23f:ec1:4fb%7'.) • The length of a hostname is limited to 255 characters. Each label (node delimited by a dot in the hostname) is limited to 63 characters and may contain letters, numbers and hyphens ('-'), but may not begin with a hyphen.	

ntp server trusted-enable

ntp server <ip_address> trusted-enable
no ntp server <ip_address> trusted-enable

Trusts this NTP server; if authentication is configured this will additionally force all time updates to only use trusted servers.
The no form of the command removes trust from this NTP server

Syntax Description	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
Default	N/A	
Configuration Mode	config	
History	3.6.2002	
	3.6.4000	Added hostname as ip_address option and added Notes.
Role	admin	
Example	`switch (config) # ntp server 10.10.10.10 trusted-enable`	
Related Commands	N/A	
Notes	• IP addresses must be in IPv4 format (e.g., '192.168.0.1') or IPv6 format with scope zone id for IPv6 link-local addresses (e.g., '2001:db8:701f::8f9' or 'fe80::21c:23f:ec1:4fb%7'.) • The length of a hostname is limited to 255 characters. Each label (node delimited by a dot in the hostname) is limited to 63 characters and may contain letters, numbers and hyphens ('-'), but may not begin with a hyphen. • NTP trusted servers can be used as a mitigation for Sybil attacks which is a vulnerability caused by NTP peers sharing the same NTP key base. This mitigation adds the concept of trusted servers which if enabled in conjunction with NTP authentication ensures that time information will only be obtained from trusted servers.	

ntp server version

ntp server <ip_address> version <ver_num>
no ntp server <ip_address> version <ver_num>

Specifies the NTP version number of this server.
The no form of the command defaults NTP to version 4.

Syntax Description	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
	ver_num	NTP version (3 or 4)
Default	4	
Configuration Mode	config	
History	3.5.0200	
	3.6.4000	Added hostname as ip_address option and added Notes.
Role	admin	
Example	`switch (config) # ntp server 10.10.10.10 version 4`	
Related Commands	N/A	
Notes	• IP addresses must be in IPv4 format (e.g., '192.168.0.1') or IPv6 format with scope zone id for IPv6 link-local addresses (e.g., '2001:db8:701f::8f9' or 'fe80::21c:23f:ec1:4fb%7'.) • The length of a hostname is limited to 255 characters. Each label (node delimited by a dot in the hostname) is limited to 63 characters and may contain letters, numbers and hyphens ('-'), but may not begin with a hyphen.	

ntp trusted-key

ntp trusted-key <key(s)>
no ntp trusted-key <key(s)>

Adds one or more keys to the trusted key list.
The no form of the command removes keys from the trusted key list.

Syntax Description	key(s) Range: 1-65534.
Default	Disabled
Configuration Mode	config
History	3.5.0200
Role	admin
Example	`switch (config) # ntp trusted-key 1,3,5` `switch (config) # ntp trusted-key 1-5`
Related Commands	ntp authentication-key
Notes	Keys may be separated with commas without any space, or they may be set as a range using a hyphen.

show clock

	show clock Displays the current system time, date and time zone.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show clock`
	`Time:  02:48:41`
	`Date:  2018/1/1`
	`Time zone:  UTC (Etc/UTC)`
	`UTC offset:  same as UTC`

Related Commands	N/A
Notes	

show ntp

	show ntp Displays the current NTP settings.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.5.0200 Updated Example 3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show ntp`
	`NTP is administratively enabled.`
	`NTP Authentication is administratively disabled.`
	`Clock is synchronized.  Reference: 108.61.73.244.  Offset: -2.833 ms.`
	`Active servers and peers:`
	
	`108.61.73.244  # Hostname configuration`
	`  Configured as  : 0.us.pool.ntp.org`
	`  Conf Type  : server`
	`  Status  : sys.peer(*)`
	`  Stratum  : 2`
	`  Offset(msec)  : -2.833`
	`  Ref clock  : 128.59.0.245`
	`  Poll Interval (sec): 256`
	`  Last Response (sec): 203`
	`  Auth state  : none`
	
	`10.7.144.19  # IP configuration`
	`  Conf Type  : peer`
	`  Status  : sys.peer(*)`
	`  Stratum  : 2`
	`  Offset(msec)  : -1.747`
	`  Ref clock  : 128.59.0.245`
	`  Poll Interval (sec): 64`
	`  Last Response (sec): 1`
	`  Auth state  : none`

Related Commands	N/A
Notes	

show ntp configured

	show ntp configured Displays NTP configuration.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.5.0200 3.6.6102 Updated Example
Role	admin

Example	`switch (config) # show ntp configured`
	`NTP enabled: yes`
	`NTP Authentication enabled: no`
	`NTP peer 0.us.pool.ntp.org  # Hostname peer configuration`
	`  Resolved as: 45.79.111.114`
	`  Enabled: yes`
	`  NTP version: 4`
	`  Key ID: none`
	`NTP peer 2.3.1.3  # IP peer configuration`
	`  Enabled: yes`
	`  NTP version: 4`
	`  Key ID: none`
	`NTP server vnc23  # Hostname server configuration`
	`  Resolved as: 10.7.2.23`
	`  Enabled: yes`
	`  NTP version: 4`
	`  Key ID: none`
	`  Trusted: no`
	`NTP server 1.2.3.4  # IP server configuration`
	`  Enabled: yes`
	`  NTP version: 4`
	`  Key ID: none`
	`  Trusted: no`
	`NTP server idontexist (DNS resolution failed. Reset or reconfigure NTP to try again)`
	`  Enabled: yes`
	`  NTP version: 4`
	`  Key ID: none`
	`  Trusted: no`

Related Commands	N/A
Notes	

show ntp keys

	show ntp configured Displays NTP keys.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.5.0200
Role	admin

Example	`switch (config) # show ntp keys`
	`NTP Key 1`
	`  Trusted: yes`
	`  Encryption Type: MD5`
	`NTP Key 2`
	`  Trusted: yes`
	`  Encryption Type: MD5`
	`NTP Key 3`
	`  Trusted: yes`
	`  Encryption Type: MD5`
	`NTP Key 4`
	`  Trusted: yes`
	`  Encryption Type: md5`
	`switch (config) #`

Related Commands	N/A
Notes	

4.3 Unbreakable Links

Mellanox MLNX-OS® offers phy profile configuration for InfiniBand interfaces. PHY profile includes Link Level Retransmission (LLR) configuration. A PHY profile is bound to any InfiniBand interface.

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

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

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

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

LLR is not operational for cables longer then 30m.

LLR Mode

The following LLR modes are applicable per port per speed:

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

LLR Negotiation

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

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

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

LLR Status

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

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

4.3.1 Commands

show interfaces ib llr

show interfaces ib [<number>] llr

Displays LLR status

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

Example	`switch (config) # show interfaces ib llr`
	`----------`
	`Interface LLR status`
	`----------`
	`IB1/1 Inactive`
	`IB1/2 Inactive`
	`IB1/3 Inactive`
	`IB1/4 Inactive`
	`IB1/5 Inactive`
	`IB1/6 Inactive`
	`IB1/7 Inactive`
	`IB1/8 Inactive`
	`IB1/9 Inactive`
	`IB1/10 Inactive`
	`IB1/11 Inactive`
	`IB1/12 Inactive`
	`IB1/13 Inactive`
	`...`	

Related Commands		
Notes		

4.4 Software Management

To inter-operate with Switch-IB™ 2 based switch systems, switch systems must at least be installed with MLNX-OS version 3.6.1002.

4.4.1 Important Pre-OS Upgrade Notes

Please consider the following items prior to upgrading the OS:

- Upgrading director switch systems can take up to 30 minutes during which time the system is indisposed.
- Upgrading the OS while embedded SM is enabled may cause the command “no hostname” to fail upon first execution. To resolve this, rerun the command.
- The upgrade procedure burns the software image as well as the firmware should there be a need
- Before upgrading the software image on your system, make sure to close all CLI sessions besides the one used to run the upgrade process
- If running a system with dual management cards, refer to Section 4.4.3, “Upgrading MLNX-OS Software on Director Switches,” on page 208
- To upgrade the Mellanox MLNX-OS® version on an SM cluster, please refer to Section 4.4.4, “Upgrading MLNX-OS HA Groups,” on page 209
- 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.
- Linux docker container names are limited to 180 characters. Upgrading to this version removes containers which do not comply with this limitation and prints the following warning to the log: “Removed configuration of container: <container name>, container name is limited to 180 characters”.
- When upgrading from a version older than 3.6.3130 with an MLAG cluster, output appears as in “UP” and “Peering” state instead of “Upgrade” on both MLAG VIP clusters. The upgrade process will not be affected.

4.4.2 Upgrading MLNX-OS Software

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

Step 1. Enter Config mode. Run:

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

Step 2. Display the currently available image (.img file).

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

  Partition 1:
  <old_image>

  Partition 2:
  <old_image>

Last boot partition: 1
Next boot partition: 1

Images available to be installed:
 webimage.tbz
  <old_image>

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

Image signing: trusted signature always required
Admin require signed images: yes

Settings for next boot only:
   Fallback reboot on configuration failure: yes (default)
```

Step 3. Delete the image 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 <old_image>
```

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>@<ip-address>/var/www/html/
<new_image>
Password (if required): ******
100.0%[##########################################################s###############]
```

Step 5. Display the available images again and verify that the new image now appears under “Images available to be installed”.

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”, and “image boot location” for more information.

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

  Partition 1:
  <old_image>

  Partition 2:
  <old_image>

Last boot partition: 1
Next boot partition: 1

Images available to be installed:
 webimage.tbz
  <new_image>

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

Image signing: trusted signature always required
Admin require signed images: yes

Settings for next boot only:
   Fallback reboot on configuration failure: yes (default)
```

Step 6. Install the new image.

```
switch (config) # image install <new_image>
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%  [################################################################]
```

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
Installed images:

  Partition 1:
  <new_image>

  Partition 2:
  <old_image>

Last boot partition: 1
Next boot partition: 1

Images available to be installed:
 webimage.tbz
  <new_image>

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

Image signing: trusted signature always required
Admin require signed images: yes

Settings for next boot only:
   Fallback reboot on configuration failure: yes (default)
```

Step 9. Save current configuration. Run:

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

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

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

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

On systems with dual management, the software must be upgraded on both the master and the slave modules.

In order to upgrade the system on dual management system refer to Section 4.4.3, “Upgrading MLNX-OS Software on Director Switches,” on page 208.

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

4.4.3 Upgrading MLNX-OS Software on Director Switches

Director switches feature dual management modules.

Step 1. Identify the chassis HA master. Run:

```
show chassis ha
```

Step 2. Upgrade the chassis master according to steps 1-8 in section Section •, “When upgrading from a version older than 3.6.3130 with an MLAG cluster, output appears as in “UP” and “Peering” state instead of “Upgrade” on both MLAG VIP clusters. The upgrade process will not be affected.,” on page 204.

Please DO NOT reboot.

Step 3. Upgrade the second management module according to steps 1-8 in section Section •, “When upgrading from a version older than 3.6.3130 with an MLAG cluster, output appears as in “UP” and “Peering” state instead of “Upgrade” on both MLAG VIP clusters. The upgrade process will not be affected.,” on page 204. Please DO NOT reboot.

Step 4. Reset the slave management module. In the master management module, run:

```
chassis ha reset other
```

Step 5. After invoking the command above, please reboot the master management immediately. Run:

On CS75x0 switch systems, run:

```
reload force immediate
```

An alternative for Step 4 and Step 5 is to power cycle the system.

Step 6. Check that 'reset count' equals 0 or 1. Run:

```
show chassis ha
```

If the reset count is not equal to either 0 or 1, power cycle the system.

Step 7. Verify all the systems are back online as members of the IB subnet ID. Run:

```
show ib smnodes {brief}
```

Using a director switch with different software versions on its two management boards is not supported.

When replacing a management board the software running on the replacement board must be aligned with the version of the software running on the other management board.

4.4.4 Upgrading MLNX-OS HA Groups

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

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

Step 1. Identify the HA group master.

for IB HA. Run:

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

Step 2. Upgrade standby node in the HA group according to steps 1-10 in Section •, “When upgrading from a version older than 3.6.3130 with an MLAG cluster, output appears as in “UP” and “Peering” state instead of “Upgrade” on both MLAG VIP clusters. The upgrade process will not be affected.,” on page 204.

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

In situations of heavy CPU load or noisy network, it is possible that another node assumes the role of cluster master before all standby nodes have rejoined the group. If this happens, you may stop waiting and proceed directly to Step 4.

Step 4. Upgrade the master node in the HA group according to steps 1-10 in Section •, “When upgrading from a version older than 3.6.3130 with an MLAG cluster, output appears as in “UP” and “Peering” state instead of “Upgrade” on both MLAG VIP clusters. The upgrade process will not be affected.,” on page 204.

4.4.5 Upgrading MLNX-OS MLAG-STP Setup

To upgrade the OS on an MLAG-STP setup from 3.6.610x to this version, there are two possible procedures:

Procedure 1:

Step 1. Make sure there are no loops in the fabric.

Step 2. Disable STP. Run:

```
switch (config) # no spanning-tree
```

Step 3. Perform the upgrade according to steps 1-10 in Section 4.4.4, on page 209.

Step 4. Enable STP – this step may lead to traffic loss while the STP state is converging. Run:

```
switch (config) # spanning-tree
```

Procedure 2:

Step 1. Shutdown all ports on the MLAG slave.

Step 2. Save configuration. Run:

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

Step 3. Upgrade MLAG slave according to steps 1-10 in Section 4.4.4, on page 209.

Step 4. Upgrade MLAG master. Run:

```
switch (config) # reload force immediate
```

Step 5. Enable all ports on the MLAG slave.

4.4.6 Deleting Unused Images

➢ ***To delete unused images:***

Step 1. Enter Config mode. Run:

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

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

```
switch (config) # show images
Images available to be installed:
  image-PPC_M460EX-3.1.1224.img
  SX-OS_PPC_M460EX 3.1.1224 2011-04-28 12:29:48 ppc
Installed images:
Partition 1:
SX-OS_PPC_M460EX 3.1.0000-dev-HA 2011-04-10 12:02:49 ppc
Partition 2:
SX-OS_PPC_M460EX 3.1.0000-dev-HA 2011-04-10 12:02:49 ppc

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

Step 3. Delete the unused images. Run:

```
switch config) # image delete image-X86_64-3.6.3234-12.img
switch (config) #
```

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

4.4.7 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.

4.4.7.1 Downloading Image

Step 1. Log into your system to obtain its product number. Run:

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

Step 2. Log into MyMellanox at https://mymellanox.force.com/support/SupportLoginand download the relevant MLNX-OS version to your system type.

Step 3. Log into the switch via the CLI using the console port.

Step 4. Change to Config mode. Run:

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

Step 5. Delete all previous images from the `Images available to be installed` prior to fetching the new image. Run:

```
switch (config) # image-X86_64-3.6.3234-12.img
```

Step 6. Fetch the requested software image. Run:

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

4.4.7.2 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. Display 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. Display 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. Configure the boot location to be the other (next) partition. Run:

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

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

In case you are downloading to an older software version which has never been run yet on the switch, use the following command sequence as well:
switch (config) # no boot next fallback-reboot enable
switch (config) # configuration write

Step 7. Reload the switch. Run:

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

4.4.7.3 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.

*****IMPORTANT NOTE*****
All configuration changes done with the new software are lost when returning to the older software version.

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

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

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 for the 2 aforementioned cases only, follow the steps below:

Step 1. Run the command:

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

Step 2. Set the boot partition. Run:

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

Step 3. Save the configuration. Run:

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

Step 4. Reload the system. Run:

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

4.4.8 Upgrading System Firmware

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

4.4.8.1 After Updating MLNX-OS Software

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

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

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

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

Some subsystems are not updated with a default firmware.

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

4.4.8.2 After Inserting a Switch Spine or Leaf

This section is applicable to director-class switch systems only.

If you insert a switch spine or leaf with a firmware version other than the default version of MLNX-OS, an automatic firmware update process will take place immediately to the inserted module *only*.

The firmware update may take a few minutes. It is recommended not to run any commands until the firmware update completes.

During firmware upgrade internal link status (up/down) notifications may be sent.

To verify that the firmware update was successful, run the command “show asic-version” (can be run in any mode). Check that the firmware version of the inserted switch spine or leaf has the default firmware version.

If you detect a firmware version mismatch for the newly inserted module, please contact your assigned Mellanox Technologies field application engineer.

4.4.8.3 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.

From version 3.3.4400 and above, the firmware update file format has been changed to mfa format. TGZ format is no longer supported.

4.4.8.3.1 Default Firmware Change on Standalone Systems

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

```
switch (config) # image fetch scp://root@1.1.1.1:/tmp/fw-SIB-rel-11_1600_0200-FIT.mfa
Password (if required): *******
100.0%
[##############################################################################]
switch (config) # image default-chip-fw fw-SIB-rel-11_1600_0200-FIT.mfa
Installing default firmware image. Please wait...
Default Firmware 11.1600.0200 updated. Please save configuration and reboot for new FW
to take effect.
```

Step 2. Save the configuration. Run:

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

Step 3. Reboot the system to enable auto update.

4.4.8.3.2 Default Firmware Change Dual Management Systems

This flow should be implemented on both management modules in parallel.

Step 1. Import the firmware image (.mfa file) on both management modules.

```
switch (config) # image fetch scp://username:password@10.7.34.115//my_directory/fw-
SIB-rel-11_1600_0200-FIT.mfa
 100.0%
[##############################################################################]
```

Step 2. Change default firmware on the management modules using the command `image default-chip-fw`.

Step 3. Verify that both master and slave have successfully installed the new firmware. The following message should be displayed:

```
Default firmware <fw> updated. Please save configuration and reboot for new FW to take
effect.
```

Step 4. Run `configuration write` on both management modules.

Step 5. Run `chassis ha reset other` on master only.

Step 6. Run `reload` on master only.

4.4.9 Commands

image boot

image boot {location <location ID> | next}

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

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

boot next

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

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

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.2.0506
Role	admin
Example	`switch (config) # boot next fallback-reboot enable` `switch (config) #`

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

boot system

boot system {location | next}
no boot system next

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

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

image default-chip-fw

image default-chip-fw <filename>
no image default-chip-fw <original-fw-filename>

Sets the default firmware package to be installed.
The no form of the command resets default firmware package.

Syntax Description	filename	Specifies the firmware filename.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
	3.6.6000	Added no form of the command
Role	admin	
Example	`switch (config) # image default-chip-fw fw-SPC-rel-13_1600_0184-FIT.mfa`	
Related Commands	show asic-version show images	
Notes		

image delete

image delete <image name>

Deletes the specified image file.

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

image fetch

image fetch <URL> [<filename>]

Downloads an image from the specified URL or via SCP.

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

Example

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

Other options:

switch (config) # image fetch http://10.1.0.40/path/filename
switch (config) # image fetch http://[fd4f:13:cc00:1::40]/path/filename
switch (config) # image fetch ftp://user:mypassword@10.1.0.40/foo/
bar.img
switch (config) # image fetch ftp://user:mypassword@[fd4f:13:cc00:1:
:40]/foo/bar.img
switch (config) # image fetch tftp://hostname/dir/filename
switch (config) # image fetch tftp://[fd4f:13:cc00:1::40]/dir/filename
switch (config) # image fetch scp://user@myhost/dir/filename
switch (config) # image fetch scp://user@myhost:1022/dir/filename
switch (config) # image fetch scp://user:pass@[fd4f:13:cc00:1::40]/dir/
filename
switch (config) # image fetch sftp://user@myhost/dir/filename
switch (config) # image fetch sftp://user@[fd4f:13:cc00:1::40]:1022/
dir/filename
switch (config) # image fetch sftp://user:pass@[fd4f:13:cc00:1::40]/
dir/filename
```

Related Commands	show images
Notes	• Please delete the previously available image, prior to fetching the new image • The path to the file in the case of TFTP depends on the server configuration. Therefore, it may not be an absolute path but a relative one. • See Section •, “When upgrading from a version older than 3.6.3130 with an MLAG cluster, output appears as in “UP” and “Peering” state instead of “Upgrade” on both MLAG VIP clusters. The upgrade process will not be affected.,” on page 204

image install

image install <image filename> [location <location ID>] | [progress <prog-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
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # image install X86_64 4100-12 2017-07-26 06:54:12 x86_64`
	`Step 1 of 4: Verify Image`
	`100.0%`
	`[####################################################################]`
	`Step 2 of 4: Uncompress Image`
	`100.0%`
	`[####################################################################]`
	`Step 3 of 4: Create Filesystems`
	`100.0%`
	`[####################################################################]`
	`Step 4 of 4: Extract Image`
	`100.0%`
	`[####################################################################]`
	`switch (config) #`	

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

image move

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

Renames the specified image file.

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

image options

image options serve all
no image options serve all

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

Syntax Description	serve all	Specifies that the image files present on this appliance should be made available for HTTP and/or HTTPS download
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # image options serve all`	
Related Commands	show images	
Notes	The parameter “serve all” affects not only the files currently present, but also any files that are later downloaded. It only applies to image files, not the installed images, which are not themselves in a downloadable format. After running “serve all” the URLs where the images will be available are: • http://<HOSTNAME>/system_images/<FILENAME> • https://<HOSTNAME>/system_images/<FILENAME>	

show bootvar

show bootvar

Displays the installed system images and the boot parameters.

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

Example	`switch [standalone: master] (config) # show bootvar`
	`Installed images:`
	
	`  Partition 1:`
	`  X86_64 3.6.4110-12 2017-07-26 06:54:12 x86_64`
	
	`  Partition 2:`
	`  X86_64 3.6.4006 2017-07-03 16:17:39 x86_64`
	
	`Last boot partition: 1`
	`Next boot partition: 1`
	
	`Serve image files via HTTP/HTTPS: no`
	
	`Boot manager password is set.`
	
	`Image signing: trusted signature always required`
	`Admin require signed images: yes`
	
	`Settings for next boot only:`
	`   Fallback reboot on configuration failure: yes (default)`
	`switch [standalone: master] (config) #`

Related Commands	N/A
Notes	

show images

	show image Displays information about the system images and boot parameters.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

Example	`switch [standalone: master] (config) # show images`
	`Installed images:`
	
	`  Partition 1:`
	`  X86_64 3.6.4110-12 2017-07-26 06:54:12 x86_64`
	
	`  Partition 2:`
	`  X86_64 3.6.4006 2017-07-03 16:17:39 x86_64`
	
	`Last boot partition: 1`
	`Next boot partition: 1`
	
	`Images available to be installed:`
	
	`  webimage.tbz`
	`  X86_64 3.6.4071-12 2017-07-26 06:54:12 x86_64`
	
	`Serve image files via HTTP/HTTPS: no`
	
	`No image install currently in progress.`
	
	`Boot manager password is set.`
	
	`Image signing: trusted signature always required`
	`Admin require signed images: yes`
	
	`Settings for next boot only:`
	`   Fallback reboot on configuration failure: yes (default)`

Related Commands	N/A
Notes	

4.5 Configuration Management

4.5.1 Saving a Configuration File

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

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

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

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

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

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

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

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

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

4.5.2 Loading a Configuration File

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

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

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

On director switch systems with dual management modules, load the configuration file according to the following:

Step 1. Power cycle the system.

Step 2. Load the configuration on the top CPU that serves as the chassis master according to the procedure described above.

If the configuration file is loaded on a different CPU than the SM HA master (SM HA master that servers the VIP), the SM configuration is overwritten.

4.5.3 Restoring Factory Default Configuration

If system configuration becomes corrupted, it is suggested to restore factory default configuration.

➢ ***To restore factory default configuration on a single management module system, run:***

```
switch (config) # reset factory keep-basic
```

➢ ***To restore factory default configuration on a dual management module system:***

If the system configuration ever becomes corrupted it is suggested to restore the factory default configuration.

Step 1. Connect to a remote console/serial connection.

Step 2. Remove the slave management module.

Step 3. Run the command `reset factory [keep-basic] [keep-all-config]`:.

```
switch (config) # reset factory keep-basic
```

Please wait for reboot to complete before moving to the next step.

Step 4. Log in as “admin” and start running the Mellanox Configuration Wizard.

Step 5. Insert the slave management module.

Step 6. Remove the master management module.

A takeover will occur changing the Slave management module role to Master.

Step 7. Repeat Step 3 on the new Master management module.

Step 8. Insert the other management module. No takeover will occur at this stage.

Step 9. Power cycle the system.

4.5.4 Managing Configuration Files

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

4.5.4.1 BIN Configuration Files

BIN configuration files are not human readable. Additionally, these files are encrypted and contain integrity verification preventing them from being edited and used on the switch.

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

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

A newly created BIN configuration file is always empty and is not created from the running-config.

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

```
switch (config) # configuration upload my-filename scp://myusername@my-server/path/to/
my/<file>
```

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

```
switch (config) # configuration fetch scp://myusername@my-server/path/to/my/<file>
```

- ***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
This requires a reboot.
Type 'yes' to confirm: yes
```

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

A binary configuration file uploaded from the switch is encrypted and has integrity verification. If the file is modified in any manner, the fetch to the switch fails.

4.5.4.2 Text Configuration Files

Text configuration files are text based and editable. It is similar in form to the output of the command "show running-config expanded".

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

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

A newly created text configuration file is always created from the running-config.

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

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

Applying a text-based configuration file to an existing/running data port configuration may result in unpredictable behavior. It is therefore suggested to first clear the switch's configuration by applying a specific configuration file (following the procedure in Section 4.5.4.1) 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. Only new or changed configuration is added. Reboot is not required.

4.5.5 Commands

4.5.5.1 File System

debug generate dump

	debug generate dump Generates a debug dump.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

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

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

file debug-dump

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

Manipulates debug dump files.

Syntax Description	delete	Deletes a debug dump file. • all: Deletes all existing debug files from this machine • latest: Deletes latest debug file from this machine
	email	Emails a debug dump file to pre-configured recipients for “informational events”, regardless of whether they have requested to receive “detailed” notifications or not. • latest: Emails the latest debug file to a pre-configured recipients
	upload	Uploads a debug dump file to a remote host. • latest: Uploads the latest debug file to a remote host
	URL	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	
	3.3.4000	Added “all” and “latest” options
Role	admin	
Example	`switch (config) # file debug-dump email sysdump-switch-112104-20114052-091707.tgz`	
Related Commands	show files debug-dump	
Notes		

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	
	3.3.4000	Added “latest” parameter
Role	admin	
Example	`switch (config) # file debug-dump email sysdump-switch-112104-20114052-091707.tgz` `switch (config) #`	
Related Commands	show files debug-dump	
Notes		

file stats

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

Manipulates statistics report files.

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

file tcpdump

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

Manipulates tcpdump output files.

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

reload

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

Reboots or shuts down the system.

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

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

Related Commands	reset factory	
Notes	BBU discharge must be disabled before any planned shutdown of the switch	

reset factory

reset factory [keep-all-config | keep-basic | keep-virt-vols | only-config] [halt]

Clears the system and resets it entirely to its factory state.

Syntax Description	keep-all-cofig	Preserves all configuration files including licenses. Removes the logs, stats, images, snapshots, history, known hosts. The user is prompted for confirmation before honoring this command, unless confirmation is disabled with the command: “no cli default prompt confirm-reset”.
	keep-basic	Preserves licenses in the running configuration file
	keep-virt-vols	Preserve all virtual disk volumes
	only-config	Removes configuration files only. The logs, stats, images, snapshots, history, and known hosts are preserved.
	halt	The system is halted after this process completes
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
	3.4.0000	Added notes and “keep-virt-vols” parameter
	3.6.2002	Updated Example and Notes
Role	admin	

Example	`switch (config) # reset factory`
	`Warning - confirming will cause system reboot.`
	`Type 'YES' to confirm reset: YES`
	`Resetting and rebooting the system -- please wait...`
	`...`	

Related Commands	reload	
Notes	• Effects of parameter “keep-all-cofig”: Licenses – not deleted; profile – no change; configuration – unchanged; management IP – unchanged • Effects of parameter “keep-basic”: Licenses – not deleted; profile – reset; configuration – reset; management IP – reset • Effects of parameter “keep-virt-vols”: Licenses – deleted; profile – reset; configuration – reset; management IP – unchanged • Confirming the command causes system reboot	

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	Any command mode	
History	3.1.0000	
Role	admin	

Example	`switch [standalone: master] (config) # show files debug-dump sysdump-switch-20170731-161038.tgz`
	`switch [standalone: master] (config) # show files debug-dump sysdump-switch-20170731-161038.tgz`
	`==========`
	`System information:`
	
	`Hostname:  switch`
	`Version:  X86_64 3.6.4006 2017-07-03 16:17:39 x86_64`
	`Current time:  2017-07-31 16:10:38`
	`System uptime: 19d 18h 20m 12s`
	
	`==========`
	
	`==========`
	`Output of 'uname -a':`
	
	`Linux switch 3.10.0-327.36.3.el7smp-x86_64 X86_64 jenkins #1 2017-06-27 12:34:55 SMP x86_64 x86_64 x86_64 GNU/Linux`
	
	`==========`	

Related Commands	file debug-dump	
Notes		

show files stats

show files stats <filename>

Displays a list of statistics report files.

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

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

Related Commands	file stats	
Notes		

show files system

show files system [detail]

Displays usage information of the file systems on the system.

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

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

Related Commands	N/A	
Notes		

show files tcpdump

	show files tcpdump Displays a list of statistics report files.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

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

Related Commands	file tcpdump tcpdump
Notes	

4.5.5.2 Configuration Files

configuration audit

configuration audit max-changes <number>

Chooses settings related to configuration change auditing.

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

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

Related Commands	show configuration	
Notes	N/A	

configuration copy

configuration copy <source name> <dest name>

Copies a configuration file.

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

configuration delete

configuration delete <filename>

Deletes a configuration file.

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

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

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

configuration fetch

configuration fetch <URL> [<name>]

Downloads a configuration file from a remote host.

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

configuration jump-start

	configuration jump-start Runs the initial-configuration wizard.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

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

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

configuration merge

configuration merge <filename>

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

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

configuration move

configuration move <source name> <dest name>

Moves a configuration file.

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

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

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

configuration new

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

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

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

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

Related Commands	show configuration	
Notes		

configuration revert

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

Reverts the system configuration to a previous state.

Syntax Description	factory	Creates new file with only factory defaults.
	keep-basic	Keeps licenses and host keys.
	keep-connect	Keeps configuration necessary for connectivity (interfaces, routes, and ARP).
	saved	Reverts running configuration to last saved configuration.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # configuration revert saved` `switch (config) #`	
Related Commands	show configuration	
Notes	This command is only available when working with an InfiniBand profile This command is not available on IB multi-SWID system profile	

configuration switch-to

configuration switch-to <filename> [no-reboot]

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

Syntax Description	no-reboot	Forces configuration change without rebooting the switch
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
	3.6.1002	Added “no-reboot” option
Role	admin	

Example	`switch (config) # show configuration files`
	`initial (active)`
	`newcon`
	`initial.prev`
	`initial.bak`
	`switch (config) # configuration switch-to newcon no-reboot`
	`switch (config) # show configuration files`
	`initial`
	`newcon (active)`
	`initial.prev`
	`initial.bak`
	`switch (config) #`	

Related Commands	show configuration files	
Notes	• The current running configuration is lost and not automatically saved to the previous active configuration file. • When running the command without the “no-reboot” parameter, the user is prompted to OK a reboot. If the answer is “yes”, the configuration is replaced and the switch is rebooted immediately.	

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	
	3.2.3000	Updated command
Role	admin	
Example	`switch (config) # configuration fetch text scp://username[:password]@hostname/path/filename`	
Related Commands	N/A	
Notes		

configuration text file

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

Performs operations on text-based configuration files.

Syntax Description	filename <file>	Specifies the filename
	apply	Applies the configuration on the system
	fail-continue	Continues execution of the commands even if some commands fail
	verbose	Displays all commands being executed and their output, instead of just those that get errors
	delete	Deletes the file
	rename <filename>	Renames the file
	upload <URL>	Supported types are HTTP, 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	
Notes		

configuration text generate

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

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

Syntax Description	active	Generates from currently active configuration.
	running	Uses running configuration.
	saved	Uses saved configuration.
	file <filename>	Generates from inactive saved configuration.
	save	Saves new file to local persistent storage.
	upload <URL>	Supported types are HTTP, 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 generate file initial.prev save example`
	`switch (config) # show configuration files`
	`initial (active)`
	`initial.prev`
	`initial.bak`
	`Active configuration: initial`
	`Unsaved changes:  yes`
	`switch (config) #`	

Related Commands	show configuration files	
Notes		

configuration upload

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

Uploads a configuration file to a remote host.

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

configuration write

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

Saves the running configuration to the active configuration file.

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

write

write {memory [local] | terminal}

Saves or displays the running configuration.

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

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

Related Commands	show running-config configuration write	
Notes		

show configuration

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

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

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

Example

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

Related Commands
Notes

show running-config

show running-config [expanded | protocol <protocol>]

Displays commands to recreate current running configuration.

Syntax Description	expanded	Displays commands in expanded format without compressing ranges
	protocol	Only displays commands relating to the specified protocol
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
	3.3.4402	Removed “full” parameter
	3.6.2002	Updated Example and added parameters
	3.6.3640	Added support for forwarding mode configuration
Role	monitor/admin	

Example

```
switch (config) # show running-config
##
## Running database "initial"
## Generated at 2018/07/25 19:34:11 +0000
## Hostname: switch
##

##
## Running-config temporary prefix mode setting
##
no cli default prefix-modes enable

##
## License keys
##
   license install <license>

##
## Other IP configuration
##
   hostname switch

##
## Local user account configuration
##
   username root nopassword

##
## AAA remote server configuration
##
# ldap bind-password ********
# radius-server key ********
# tacacs-server key ********

##
## SNMP configuration
##
   snmp-server user 7YLAyJrC77 v3 capability admin
   snmp-server user 7YLAyJrC77 v3 enable
   snmp-server user 7YLAyJrC77 v3 enable sets
no snmp-server user 7YLAyJrC77 v3 require-privacy
   snmp-server user kRg5dmdogX v3 capability admin
   snmp-server user kRg5dmdogX v3 enable
   snmp-server user kRg5dmdogX v3 enable sets
no snmp-server user kRg5dmdogX v3 require-privacy

##
## Network management configuration
##
# web proxy auth basic password ********

##
## Persistent prefix mode setting
##
cli default prefix-modes enable
```

Related Commands

Notes

4.6 Logging

4.6.1 Monitor

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

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

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

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

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

To see a list of the events, refer to Table 25, “Supported Event Notifications and MIB Mapping,” on page 298.

4.6.2 Remote Logging

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

Step 1. Enter Config mode. Run:

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

Step 2. Set remote syslog server. Run

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

Step 3. (Optional) Set the destination port of the remote host. Run:

```
switch (config) # logging <IP address/hostname> port <port>
```

Step 4. Set the minimum severity of the log level to `info`. Run:

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

Step 5. Override the log levels on a per-class basis. Run:

```
switch (config) # logging <IP address/hostname> trap override class <class name> prior-
ity <level>
```

4.6.3 Commands

logging port

logging <syslog IPv4 address/hostname> port <destination-port>
no logging <syslog IPv4 address/hostname> port

Configures remote server destination port for log messages.
The no form of the command resets the remote log port to its default value.

Syntax Description	destination-port	Range: 1-65535
	Hostname	Max 64 characters
Default	514 (UDP)	
Configuration Mode	config	
History	3.6.2002	
Role	admin	
Example	`switch (config) # logging 10.0.0.1 port 105`	
Related Commands	logging <syslog IPv4 address/hostname> trap	
Notes		

logging trap

logging <syslog IPv4 address/hostname> [trap {<log-level> | override class <class> priority <log-level>}]
no logging <syslog IPv4 address/hostname> [trap {<log-level> | override class <class> priority <log-level>}]

Enables (by setting the IPv4 address/hostname) 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 IPv4 address/hostname	IPv4 address/hostname of the remote syslog server. Hostname is limited to 64 characters
	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, the software 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`
Related Commands	show logging logging local override logging <syslog IPv4 address/hostname> port
Notes	

logging debug-files

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

Configures settings for debug log files.

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

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

	update {<number> | current}	Uploads a local debug-log file to a remote host. • current: Uploads log file “messages” to a remote host • number: Uploads compressed log file “debug.<number>.gz” to a remote host. Range is 1-10
	upload	Uploads debug log file to a remote host
	log-file	Possible values: 1-7, or current
	upload URL	HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported (e.g.: scp://username[:password]@hostname/path/filename)
Default	N/A	
Configuration Mode	config	
History	3.3.4150	
Role	admin	
Example	`switch (config) # logging debug-files delete current` `switch (config) #`	
Related Commands		
Notes		

logging event enable

	logging events {cpu-rate-limiters | interfaces | protocols} enable **no logging events {cpu-rate-limiters | interfaces | protocols} enable** Activate event tracking for a certain group. The no form of the command deactivates event tracking for a certain group.
Syntax Description	cpu-rate-limiters | interfaces | protocols — Logical groups with specified set of counters
Default	N/A
Configuration Mode	config
History	3.6.6000
Role	admin
Example	`switch (config) # logging events interfaces enable`
Related Commands	
Notes	

logging event error-threshold

logging events {interfaces | protocols} error-threshold <events>
no logging events {interfaces | protocols} error-threshold <events>

Configures number of events after which the system begins to generate events to the log file.
The no form of the command resets this parameter to its default value.

Syntax Description	interfaces	Sets threshold for interface related events
	protocols	Sets threshold for protocol related events
	events	Number of events after which the system begins to generate events to the log file. Range: 0-4294967295.
Default	interfaces – 10 events protocols – 2 events	
Configuration Mode	config	
History	3.6.6000	
Role	admin	
Example	`switch (config) # logging events interfaces error-threshold 45`	
Related Commands		
Notes		

logging event interval

logging events {interfaces | protocols} interval <seconds>
no logging events {interfaces | protocols} interval <seconds>

Configures interval in seconds between each sampling of counters in event type. The no form of the command resets this parameter to its default value.

Syntax Description	interfaces | protocols	Logical groups with specified set of counters
	seconds	Time between sampling. Range is different for each event type: • interfaces – 10-3600 • protocols – 10-3600
Default	interfaces – 5 minutes protocols – 1 minute	
Configuration Mode	config	
History	3.6.6000	
Role	admin	
Example	`switch (config) # logging events interfaces interval 120`	
Related Commands		
Notes		

logging event rate-limit

	logging events [interfaces | protocols] rate-limit {short | medium | long} [count | window] **no logging events [interfaces | protocols] rate-limit [short | medium | long] [count <number> | window <seconds>]** Configures the number of allowed events per time window and that window's duration. The no form of the command resets these parameters to their default values.
Syntax Description	interfaces | protocols — Logical groups with specified set of counters rate-limit — Three configurable periods: short, medium, and long count — Number of allowed events per time window window — Window of time in seconds for the rate limit period
Default	For "interfaces" Short window: event count – 5 window duration – 1 hour Medium window: event count – 50 window duration – 1 day Long window: event count – 350 window duration – 7 days For "protocols" Short window: event count – 10 window duration – 1 hour Medium window: event count – 100 window duration – 1 day Long window: event count – 600 window duration – 7 days
Configuration Mode	config
History	3.6.6000
Role	admin
Example	`switch (config) # logging events interfaces interval 120`
Related Commands	
Notes	• The goal of this command is to restrict the number of events in the log. To achieve this end, it is possible to specify the allowed number (parameter "count") of messages per period of time (parameter "window").

logging fields

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

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

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

Example

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

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

logging files delete

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

Deletes the current or oldest log files.

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

logging files rotation

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

Sets the rotation criteria of the logging files.

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

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

Related Commands	show logging show log files
Notes	

logging files upload

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

Uploads a log file to a remote host.

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

logging format

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

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

Syntax Description	standard	Standard format.
	welf	WebTrends Enhanced Log file (WELF) format.
	hostname	Specifies the firewall hostname that should be associated with each message logged in WELF format. If no firewall name is set, the hostname is used by default. hostname is limited to 64 characters.
Default	standard	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

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

Related Commands	show logging	
Notes		

logging level

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

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

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

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

Related Commands	show logging	
Notes		

logging 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, the software will not log anything from this class. Classes available: • debug-module - debug module functionality • protocol-stack - protocol stack modules functionality • mgmt-back - system management back-end components • mgmt-core - system management core • mgmt-front - system management front-end components • mlx-daemons - management daemons • sx-sdk - switch SDK
	log-level	• alert - alert notification, action must be taken immediately • crit - critical condition • debug - debug level messages • emerg - system is unusable (emergency) • err - error condition • info - informational condition • none - disables the logging locally and remotely • notice - normal, but significant condition • warning - warning condition
Default	Override is disabled.	
Configuration Mode	config	
History	3.1.0000	
	3.3.4150	Added debug-module class Changed iss-modules with protocol-stack
Role	admin	

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

Related Commands	show logging logging local
Notes	

logging monitor

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

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

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

logging receive

	logging receive **no logging receive** Enables receiving logging messages from a remote host. The no form of the command disables the option of receiving logging messages from a remote host.
Syntax Description	N/A
Default	Receiving logging is disabled
Configuration Mode	config
History	3.1.0000
Role	admin

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

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

logging trap

logging trap <log-level>
no logging trap

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

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

show log

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

Displays the log file with optional filter criteria.

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

Example	`switch [standalone: master] (config) # show log matching "Executing|Action"`
	`Jul 31 16:11:23 M2100-aj cli[26502]: [cli.NOTICE]: user : Executing command: enable`
	`Jul 31 16:11:24 M2100-aj cli[26507]: [cli.NOTICE]: user : Executing command: enable`
	`Jul 31 16:11:29 M2100-aj cli[26514]: [cli.NOTICE]: user : Executing command: enable`
	`Jul 31 16:11:29 M2100-aj cli[26514]: [cli.NOTICE]: user : Executing command: show license`
	`Jul 31 16:11:41 M2100-aj cli[26548]: [cli.NOTICE]: user : Executing command: enable`
	`Jul 31 16:11:42 M2100-aj cli[26553]: [cli.NOTICE]: user : Executing command: enable`
	`Jul 31 16:11:42 M2100-aj cli[26553]: [cli.NOTICE]: user : Executing command: conf termina`	

Related Commands	logging fields logging files rotation logging level logging local logging receive show logging	
Notes	• When using a regular expression containing | (OR), the expression should be surrounded by quotes (“<expression>”), otherwise it is parsed as filter (PIPE) command. • The command’s output has many of the options as the Linux “less” command. These options allow navigating the log file and perform searches. To see help for different option press “h” after running the “show log” command.	

show logging

	show logging Displays the logging configurations.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

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

Related Commands	logging fields logging files rotation logging level logging local logging receive logging <syslog IPv4 address/hostname>
Notes	

show logging events

show logging events [interfaces | protocols]

Displays configuration per selected event group or all.

Syntax Description	interfaces | protocols Logical groups with specified set of counters
Default	N/A
Configuration Mode	Any command mode
History	3.6.6000
Role	admin
Example	

```
switch (config) # show logging events

interfaces:
  Admin mode     : no
  Interval       : 5 minutes
  Error threshold: 10

  Rate-limit short window:
    Event count    : 5
    Window duration: 1 hour

  Rate-limit medium window:
    Event count    : 50
    Window duration: 1 day

  Rate-limit long window:
    Event count    : 350
    Window duration: 7 days


protocols:
  Admin mode     : no
  Interval       : 1 minute
  Error threshold: 2

  Rate-limit short window:
    Event count    : 10
    Window duration: 1 hour

  Rate-limit medium window:
    Event count    : 100
    Window duration: 1 day

  Rate-limit long window:
    Event count    : 600
    Window duration: 7 days
```

Related Commands	
Notes	

show logging events source-counters

show logging events [interfaces | protocols] source-counters

Displays set of counters for sampling.

Syntax Description	interfaces | protocols	Logical groups with specified set of counters
Default	N/A	
Configuration Mode	Any command mode	
History	3.6.6000	
Role	admin	

Example	`switch (config) # show logging events interfaces source-counters`
	
	`interfaces:`
	`  Counters: Rx discard packets, Rx error packets, Rx fcs errors, Rx undersize packets, Rx oversize packets, Rx unknown control opcode, Rx symbol errors, Rx discard packets by Storm Control, Tx discard packets, Tx error packets, Tx hoq discard packets`	

Related Commands		
Notes		

4.7 Link Diagnostic Per Port

4.7.1 General

When debugging a system, it is important to be able to quickly identify the root of a problem. The Diagnostic commands enables an insight into the physical layer components where the user is able to see information such as a cable status (plugged/unplugged) or if Auto-Negotiation has failed.

4.7.2 List of Possible Output Messages

```
No issue was observed
Closed by command
Negotiation failure
Link training failure
Speed logical mismatch
Remote faults detected
Cable speed not enabled
Bad signal integrity
Other issues
Speed degradation
Information unavailable
Cable is unplugged
Unsupported cable
I2C bus is stuck
Module memory invalid
Module overheated
Module short circuit
Power budget exceeded
Management forced down
```

4.7.3 Commands

show interfaces ib link-diagnostics

show interfaces ib [device/port] link-diagnostics

Displays a specific InfiniBand module/port or all InfiniBand ports.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.4000
Role	admin
Example	

```
switch (config) # show interfaces ib link-diagnostics
------------------------------------------------------------------------
Interface          Code          Status
------------------------------------------------------------------------
IB1/1              0             The port is Active.
IB1/2              0             The port is Active.
IB1/3              1024          Cable unplugged
IB1/4              1024          Cable unplugged
IB1/5              1024          Cable unplugged
IB1/6              1024          Cable unplugged
IB1/7              1024          Cable unplugged
IB1/8              1024          Cable unplugged
IB1/9              1024          Cable unplugged
IB1/10             1024          Cable unplugged
IB1/11             1024          Cable unplugged
IB1/12             1024          Cable unplugged
IB1/13             1024          Cable unplugged
IB1/14             1024          Cable unplugged
IB1/15             1024          Cable unplugged
IB1/16             1024          Cable unplugged
IB1/17             1024          Cable unplugged
IB1/18             1024          Cable unplugged
IB1/19             1024          Cable unplugged
IB1/20             1024          Cable unplugged
IB1/21             1024          Cable unplugged
IB1/22             1024          Cable unplugged
IB1/23             1024          Cable unplugged
IB1/24             1024          Cable unplugged
IB1/25             1024          Cable unplugged
IB1/26             1024          Cable unplugged
IB1/27             1024          Cable unplugged
IB1/28             1024          Cable unplugged
IB1/29             1024          Cable unplugged
IB1/30             1024          Cable unplugged
IB1/31             1024          Cable unplugged
IB1/32             1024          Cable unplugged
IB1/33             1024          Cable unplugged
IB1/34             1024          Cable unplugged
IB1/35             1             The port is closed by command.
IB1/36             2             Auto-Negotiation failure..
```

Related Commands
Notes

show interfaces ib internal leaf link-diagnostics

show interfaces ib internal leaf <module/port> link-diagnostics

Displays a specific InfiniBand internal leaf module/port.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.4000
Role	admin

Example	`switch (config) # show interfaces ib internal leaf 1 link-diagnostics`
	`----------------------------------------------------------------------`
	`Interface Code Status`
	`----------------------------------------------------------------------`
	`IB1/1/19 0 No issue was observed`
	`IB1/1/20 0 No issue was observed`
	`IB1/1/21 0 No issue was observed`
	`IB1/1/22 0 No issue was observed`
	`IB1/1/23 0 No issue was observed`
	`IB1/1/24 0 No issue was observed`
	`IB1/1/25 0 No issue was observed`
	`IB1/1/26 0 No issue was observed`
	`IB1/1/27 0 No issue was observed`
	`IB1/1/28 0 No issue was observed`
	`IB1/1/29 0 No issue was observed`
	`IB1/1/30 0 No issue was observed`

Related Commands	
Notes	

show interfaces ib internal spine link-diagnostics

show interfaces ib internal spine <module/port> link-diagnostics

Displays a specific InfiniBand internal spine module/port.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.4000
Role	admin

Example	`switch (config) # show interfaces ib internal spine 3/1/1 link-diagnostics`
	`---------------------------------------------------------------------`
	`Interface Code Status`
	`---------------------------------------------------------------------`
	`IB3/1/1 0 No issue was observed`

Related Commands	
Notes	

4.8 Signal Degradation Monitoring

A system can monitor the Bit Error Rate (BER) in order to ensure a quality of the link. As long as BER observed by the LRH layer is low enough, the rate of packet loss is low enough to allow successful operation of the applications running on top of the network.

The system continuously monitors the link BER and compares it to BER limits, when limits are crossed the system can generate an event indicating that link quality is degraded to the network operator that can take preemptive actions or even disable the low quality link.

When Forward Error Correction (FEC) is enabled a network operator can choose to monitor an amount of corrected errors by using the pre-FEC mode, or the amount of errors which the FEC failed to correct (uncorrectable errors) by using the post-FEC mode, when FEC is used then every error detected by the PHY will be monitored.

When link is disabled the system will keep it in shutdown state until either the port is explicitly enabled or the port's module is reinserted.

4.8.1 Effective-BER Monitoring

Effective-BER is the BER that the LRH/Application layer observe. Errors monitored by the Effective-BER may directly result in a packet drop. For links with no error correction, the Effective BER is the BER received by port, and it is monitored based on the received Phy symbols. For links with FEC, the Effective BER represents the rate of errors that the FEC decoder did not manage to correct and were passed to the LRH layer. The Effective BER for FEC links is monitored using the FEC decoder uncorrectable codewords data.

4.8.2 Configuring Signal Degradation Monitoring

Step 1. Enable signal degradation monitoring. Run:

```
switch (config) # ib 1/3 signal-degrade
```

If not indicated, the interface is disabled in case of signal degradation.

Step 2. (Optional) To prevent the interface from shutting down in case of signal degradation, run:

```
switch (config) # ib 1/3 signal-degrade no-shutdown
```

Step 3. (Optional) Enable SNMP notifications on signal degradation events. Run:

```
switch (config) # snmp notify event health-module-status
```

Please refer to Section 4.17.1.7, "Configuring an SNMP Notification," on page 494 for a general explanation on how to enable SNMP notifications for specific events.

Step 4. (Optional) Enable email notifications on signal degradation events. Run:

```
switch (config) # email notify event health-module-status
```

Please refer to Section 4.9.4, "Email Notifications," on page 301 for a general explanation on how to enable email notifications for specific events.

4.8.3 Commands

ib signal-degrade

ib <slot>/<port> signal-degrade [no-shutdown]
no ib <slot>/<port> signal-degrade [no-shutdown]

Enables signal degradation operation per interface.

Syntax Description	no-shutdown	Does not shutdown an affected interface
Default	Disabled	
Configuration Mode	config	
History	3.6.6102	
Role	admin	
Example	`switch (config) #ib 1/1 signal-degrade`	
Related Commands		
Notes		

show interfaces ib signal-degrade

show interfaces ib [<slot>/<port>] signal-degrade

Displays signal degradation information.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.6102
Role	admin

Example	`switch (config) # show interfaces ib signal-degrade`
	`---------------------------------------------------------------------------------------`
	`Interface  Physical port state  Monitoring  Action  FEC type`
	`---------------------------------------------------------------------------------------`
	`IB1/1  LinkUp  Disabled  Shutdown  no-fec/post-fec`
	`IB1/2  LinkUp  Enabled  Shutdown  no-fec/post-fec`
	`IB1/3  Polling  Disabled  Shutdown  no-fec/post-fec`
	`IB1/4  Polling  Disabled  Shutdown  no-fec/post-fec`
	`IB1/5  Polling  Disabled  Shutdown  no-fec/post-fec`
	`IB1/6  Polling  Disabled  Shutdown  no-fec/post-fec`
	`IB1/7  Polling  Disabled  Shutdown  no-fec/post-fec`
	`...`

Related Commands	
Notes	This command is relevant only for 1U switch systems

4.9 Event Notifications

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

4.9.1 Supported Events

Table 25 presents the supported events and maps them to their relevant MIB OID.

Table 25 - 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	N/A
dcbx-ets-port-admin-state-trap	DCBX ETS port admin state trap	MELLANOX-DCB-TRAPS-MIB: mellanoxETSPortAdminStateTrap	N/A
dcbx-ets-port-oper-state-trap	DCBX ETS port oper state trap	MELLANOX-DCB-TRAPS-MIB: mellanoxETSPortOperStateTrap	N/A
dcbx-ets-port-peer-state-trap	DCBX ETS port peer state trap	MELLANOX-DCB-TRAPS-MIB: mellanoxETSPortPeerStateTrap	N/A
dcbx-pfc-module-state-change	DCBX PFC module state change	MELLANOX-DCB-TRAPS-MIB: mellanoxPFCModuleStateTrap	N/A
dcbx-pfc-port-admin-state-trap	DCBX PFC port admin state trap	MELLANOX-DCB-TRAPS-MIB: mellanoxPFCPortAdminStateTrap	N/A
dcbx-pfc-port-oper-state-trap	DCBX PFC port oper state trap	MELLANOX-DCB-TRAPS-MIB: mellanoxPFCPortOperStateTrap	N/A
dcbx-pfc-port-peer-state-trap	DCBX PFC port peer state trap	MELLANOX-DCB-TRAPS-MIB: mellanoxPFCPortPeerStateTrap	N/A
disk-space-low	File system free space has fallen too low	Mellanox-EFM-MIB: diskSpaceLow	N/A
health-module-status	Health module status changed	Mellanox-EFM-MIB: systemHealthStatus	N/A
insufficient-fans	Insufficient amount of fans in system	Mellanox-EFM-MIB: insufficientFans	N/A
insufficient-fans-recover	Insufficient amount of fans in system recovered	Mellanox-EFM-MIB: insufficientFansRecover	N/A
insufficient-power	Insufficient power supply	Mellanox-EFM-MIB: insufficientPower	N/A

Table 25 - Supported Event Notifications and MIB Mapping

Event Name	Event Description	MIB OID	Comments
interface-down	An interface's link state has changed to DOWN	RFC1213: linkdown (SNMPv1)	Supported for 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 InfiniBand and management interfaces for 1U and blade systems
internal-bus-error	Internal bus (I^2C) error	Mellanox-EFM-MIB: internalBusError	N/A
internal-link-speed-mismatch	There is a mismatch in the speeds of the internal links between spine and leaf modules	Mellanox-EFM-MIB: internalSpeedMismatch	Supported only for director switches
liveness-failure	A process in the system is detected as hung	Not implemented	N/A
low-power	Low power supply	Mellanox-EFM-MIB: lowPower	N/A
low-power-recover	Low power supply recover	Mellanox-EFM-MIB: lowPowerRecover	N/A
mstp-new-bridge-root	The bridge become the root bridge root of a MSTI	MELLANOX-MSTP-MIB: mstpRootBridgeChange	N/A
mstp-new-root-port	The root port of a MSTI changed	MELLANOX-MSTP-MIB: mstpRootPortChange	N/A
mstp-topology-change	Port in MSTI become forwarding of blocking	MELLANOX-MSTP-MIB: mstpTopologyChange	N/A
N/A	Reset occurred due to over-heating of ASIC	Mellanox-EFM-MIB: asicOverTempReset	Not supported
ospf-auth-fail	OSPF authentication failure	OSPF-TRAP-MIB: ospfIfAuthFailure	N/A
ospf-config-error	OSPF config error	OSPF-TRAP-MIB: ospfIfConfigError	N/A
ospf-if-rx-bad-packet	Bad OSPF packet received	OSPF-TRAP-MIB: ospfIfRxBadPacket	N/A
ospf-if-state-change	OSPF interface state change	OSPF-TRAP-MIB: ospfIfStateChange	N/A
ospf-lsdb-approaching-overflow	OSPF LSDB is approaching overflow	OSPF-TRAP-MIB: ospfLsdbApproachingOverflow	Not supported

Table 25 - Supported Event Notifications and MIB Mapping

Event Name	Event Description	MIB OID	Comments
ospf-lsdb-overflow	OSPF LSDB overflow	OSPF-TRAP-MIB: ospfLsdbOverflow	Not supported
ospf-nbr-state-change	OSPF neighbor state change	OSPF-TRAP-MIB: ospfNbrStateChange	N/A
paging-high	Paging activity has risen too high	N/A	Not supported
power-redundancy-mismatch	Power redundancy mis-match	Mellanox-EFM-MIB: powerRedundancyMismatch	Supported only for director switches
process-crash	A process in the system has crashed	Mellanox-EFM-MIB: procCrash	N/A
process-exit	A process in the system unexpectedly exited	Mellanox-EFM-MIB: procUnexpectedExit	N/A
send-test	Send a test notification	testTrap	Run CLI command # snmp-server notify send-test
snmp-authtrap	An SNMPv3 request has failed authentica-tion	Not implemented	N/A
temperature-too-high	Temperature is too high	Mellanox-EFM-MIB: asicOverTemp	N/A
unexpected-shutdown	Unexpected system shutdown	Mellanox-EFM-MIB: unexpectedShutdown	N/A
xstp-new-root-bridge	The bridge became the root bridge of STI	MELLANOX-XSTP-MIB: mellanoxXstpRootBridgeChange	N/A
xstp-root-port-change	XSTP root port changed	MELLANOX-XSTP-MIB: mellanoxXstpRootPortChange	N/A
xstp-topology-change	Port in pvrst become forwarding of blocking	MELLANOX-XSTP-MIB: mellanoxXstpTopologyChange	N/A

4.9.2 SNMP Trap Notifications

To set SNMP notification see Section 4.17.1.7, “Configuring an SNMP Notification,” on page 494.

4.9.3 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) #
```

4.9.4 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.
```

4.9.5 Commands

4.9.5.1 Email Notification

email autosupport enable

	email autosupport enable **no email autosupport enable** Sends automatic support notifications via email. The no form of the command stops sending automatic support notifications via email.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.2.3000
Role	admin
Example	`switch (config) # email autosupport enable`
Related Commands	N/A
Notes	

email autosupport event

email autosupport event <event>
no email autosupport event

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

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

	• asic-chip-down – ASIC (chip) down • internal-bus-error – internal bus (I^2C) error • internal-link-speed-mismatch – internal links speed mismatch
Default	N/A
Configuration Mode	config
History	3.2.3000
Role	admin
Example	`switch (config) # email autosupport event process-crash`
Related Commands	N/A
Notes	

email autosupport ssl mode

email autosupport ssl mode {none | tls | tls-none}
no email autosupport ssl mode

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

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

email autosupport ssl cert-verify

	email autosupport ssl cert-verify **no email autosupport ssl cert-verify** Verifies server certificates. The no form of the command does not verify server certificates.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.2.3000
Role	admin
Example	`switch (config) # email autosupport ssl cert-verify`
Related Commands	N/A
Notes	

email autosupport ssl ca-list

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

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

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

email dead-letter

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

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

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

email domain

email domain <hostname or IP address>
no email domain

Sets the domain name from which the emails will appear to come from (provided that the return address is not already fully-qualified). This is used in conjunction with the system hostname to form the full name of the host from which the email appears to come.
The no form of the command clears email domain override.

Syntax Description	hostname or IP address IP address.
Default	No email domain
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # email domain mellanox`
	`switch (config) # show email`
	`Mail hub: 10.0.8.11`
	`Mail hub port: 125`
	`Domain: mellanox`
	`Return address: do-not-reply`
	`Include hostname in return address: yes`
	`...`
	`switch (config) #`

Related Commands	show emails
Notes	

email mailhub

email mailhub <hostname or IP address>
no email mailhub

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

Syntax Description	hostname or IP address Hostname or IP address.
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # email mailhub 10.0.8.11`
	`switch (config) # show email`
	`Mail hub: 10.0.8.11`
	`Mail hub port: 25`
	`Domain: (not specified)`
	`Return address: do-not-reply`
	`Include hostname in return address: yes`
	`...`
	`switch (config) #`

Related Commands	show email [events]
Notes	

email autosupport mailhub

email autosupport mailhub <hostname or IP address>
no email autosupport mailhub

Sets the mail relay to be used for sending autosupport notification emails. The no form of the command clears the mail relay to be used for sending autosupport notification emails.

Syntax Description	<Hostname or IP address> The mail hub Hostname or IP address.
Default	N/A
Configuration Mode	config
History	3.7.10xx
Role	Admin

Example	`switch (config) # email autosupport mailhub 10.10.10.1`
	`switch (config) # show email`
	
	`Autosupport emails`
	`  Enabled:  no`
	`  Recipient:`
	`  Mail hub:  10.10.10.1`
	`  Security mode:  tls-none`
	`  Verify server cert:  yes`
	`  Supplemental CA list: default-ca-list`

Related Commands	show email
Notes	

email autosupport recipient

email autosupport recipient <email addr>
no email autosupport recipient

Sets the recipient for autosupport emails.
The no form of the command clears the configured autosupport recipient.

Syntax Description	<email addr>	The autosupport recipient email address.
Default	N/A	
Configuration Mode	config	
History	3.7.10xx	
Role	Admin	

Example	`switch (config) # email autosupport recipient user@example.com`
	`switch (config) # show email`
	
	`Autosupport emails`
	`  Enabled:  no`
	`  Recipient:  user@example.com`
	`  Mail hub:`
	`  Security mode:  tls-none`
	`  Verify server cert:  yes`
	`  Supplemental CA list: default-ca-list`	

Related Commands	show email	
Notes		

email mailhub-port

email mailhub-port <hostname or IP address>
no email mailhub-port

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

Syntax Description	hostname or IP address hostname or IP address.
Default	25
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # email mailhub-port 125`
	`switch (config) # show email`
	`Mail hub: 10.0.8.11`
	`Mail hub port: 125`
	`Domain: (system domain name)`
	`Return address: do-not-reply`
	`Include hostname in return address: yes`
	`...`
	`switch (config) #`

Related Commands	show email
Notes	

email notify event

email notify event <event name>
no email notify event <event name>

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

Syntax Description	event name	Example event names would include “process-crash” and “cpu-util-high”.
Default	No events are enabled	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # email notify event process-crash`
	`switch (config) # show email events`
	`Failure events for which emails will be sent:`
	`process-crash: A process in the system has crashed`
	`unexpected-shutdown: Unexpected system shutdown`
	
	`Informational events for which emails will be sent:`
	`liveness-failure: A process in the system was detected as hung`
	`process-exit: A process in the system unexpectedly exited`
	`cpu-util-ok: CPU utilization has fallen back to normal levels`
	`cpu-util-high: CPU utilization has risen too high`
	`disk-io-ok: Disk I/O per second has fallen back to acceptable levels`
	`...`
	`temperature-too-high: Temperature has risen too high`
	
	`All events for which autosupport emails will be sent:`
	`process-crash: A process in the system has crashed`
	`liveness-failure: A process in the system was detected as hungswitch`
	`(config) #`
	`switch (config) #`	

Related Commands	show email	
Notes	This does not affect auto-support emails. Auto-support can be disabled overall, but if it is enabled, all auto-support events are sent as emails.	

email notify recipient

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

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

Syntax Description	email addr	Email address of intended recipient.
	class	Specifies which types of events are sent to this recipient.
	info	Sends informational events to this recipient.
	failure	Sends failure events to this recipient.
	detail	Sends detailed event emails to this recipient.
Default	No recipients are added	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # email notify recipient user2@autosupport.mellanox.com`
	`switch (config) # show email`
	`Mail hub:`
	`Mail hub port: 25`
	`Domain: (not specified)`
	`Return address: user1`
	`Include hostname in return address: no`
	`Dead letter settings:`
	`Save dead.letter files: yes`
	`Dead letter max age: (none)`
	`Email notification recipients:`
	`user2@autosupport.mellanox.com (all events, in detail)`
	`Autosupport emails`
	`Enabled: no`
	`Recipient: autosupport@autosupport.mellanox.com`
	`Mail hub: autosupport.mellanox.com`
	`switch (config) #`	

Related Commands	show email	
Notes		

email return-addr

email return-addr <username>
no email domain

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

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

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

Syntax Description	username	Username.
Default	do-not-reply	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # email return-addr user1`
	`switch (config) # show email`
	`Mail hub:`
	`Mail hub port: 25`
	`Domain: (not specified)`
	`Return address: user1`
	`Include hostname in return address: yes`
	`...`
	`switch (config) #`	

Related Commands	show email	
Notes		

email return-host

	email return-host **no email return-host** Includes the hostname in the return address for emails. The no form of the command does not include the hostname in the return address for emails.
Syntax Description	N/A
Default	No return host
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # no email return-host`
	`switch (config) # show email`
	`Mail hub:`
	`Mail hub port:    25`
	`Domain:           (system domain name)`
	`Return address:   my-address`
	`Include hostname in return address: no`
	
	`Current reply address: host@localdomain`
	
	`Dead letter settings:`
	`  Save dead.letter files: yes`
	`  Dead letter max age:    5 days`
	
	`No recipients configured.`
	
	`Autosupport emails`
	`  Enabled:      no`
	`  Recipient:    autosupport@autosupport.mellanox.com`
	`  Mail hub:     autosupport.mellanox.com`
	`switch (config) #`

Related Commands	show email
Notes	This only takes effect if the return address does not contain an “@” character.

email send-test

	email send-test Sends test-email to all configured event and failure recipients.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # email send-test`
Related Commands	show email [events]
Notes	

email ssl mode

email ssl mode {none | tls | tls-none}
no email ssl mode

Sets the security mode(s) to try for sending email.
The no form of the command resets the email SSL mode to its default.

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

email ssl cert-verify

	email ssl cert-verify **no email ssl cert-verify** Enables verification of SSL/TLS server certificates for email. The no form of the command disables verification of SSL/TLS server certificates for email.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.2.3000
Role	admin
Example	`switch (config) # email ssl cert-verify`
Related Commands	N/A
Notes	This command has no impact unless TLS is used.

email ssl ca-list

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

Specifies the list of supplemental certificates of authority (CA) from the certificate configuration database that is to be used for verification of server certificates when sending email using TLS, if any.
The no form of the command uses no list of supplemental certificates.

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

show email

show email [events]

Displays 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	3.7.10xx	
Role	admin	

Example	`switch (config) # show email`
	
	`Autosupport emails`
	`  Enabled:  no`
	`  Recipient:`
	`  Mail hub:  10.10.10.1`
	`  Security mode:  tls-none`
	`  Verify server cert:  yes`
	`  Supplemental CA list: default-ca-list`	

Related Commands	show email	
Notes		

4.10 Telemetry

As it is becoming increasingly complex to manage networks, and network administrators need more tools to understand network behavior, it is necessary to provide basic information about network performance, identify network bottlenecks, and provide information for the purposes of network optimization and future planning.

Therefore, network administrators are required to constantly review network port behavior, record port buffer consumption, and identify shortage in buffer resources and record flows which lead to the excessive buffer consumption.

MLNX-OS provides the following mechanisms to perform these tasks:

- Sampling (histograms) – a network administrator can enable a sampling of the port buffer occupancy, record occupancy changes over time, and provide information for different levels of buffer occupancy, and amount of time the buffer has been occupied during the observation period.
- Thresholds – thresholds may be enabled per port to record the network time when port buffer occupancy crosses the defined threshold and when buffer occupancy drops below it.
- Flow recording – a record of the most active flows which cause an excessive usage of the port buffers may be kept. Once enabled, the system may identify flow patterns and present a user with a list of flows, based on which a network administrator can rearrange distribution of the data flows in the network and minimize data loss.

4.10.1 Commands

protocol telemetry

protocol telemetry
no protocol telemetry

Unhides telemetry config CLIs.
The no form of the command hides telemetry config CLIs.

Syntax Description	N/A
Default	Disabled.
Configuration Mode	config
History	3.6.3004
Role	admin
Example	`switch (config) # protocol telemetry` `switch (config) # no protocol telemetry`
Related Commands	
Notes	

telemetry shutdown

	telemetry shutdown **no telemetry shutdown** Disables the telemetry protocol, threshold detection, and histogram fetching for all sampling enabled interfaces without changing any internal configuration. The no form of the command enables telemetry protocol.
Syntax Description	N/A
Default	Disabled
Configuration Mode	config
History	3.6.3004
Role	admin
Example	`switch (config) # telemetry shutdown` `switch (config) # no telemetry shutdown`
Related Commands	
Notes	

telemetry sampling

	interface ib <slot>/<port> telemetry sampling **no interface ib <slot>/<port> telemetry sampling** Enables sampling (histogram fetching) for a specific InfiniBand interface. The no form of the command disables sampling (histogram fetching).
Syntax Description	N/A
Default	N/A
Configuration Mode	config interface ib
History	3.6.3004
Role	admin
Example	`switch (config interface ib 1/1) # telemetry sampling`
Related Commands	
Notes	

telemetry sampling log

telemetry sampling log <time>
no telemetry sampling log <time>

Enables the log interval value (histogram fetching) from device.
The no form of the command disables the log interval value.

Syntax Description	time	Input Range: 100 msec - 1 min
Default	1000 msec.	
Configuration Mode	config	
History	3.6.3004	
Role	admin	
Example	`switch (config) # telemetry sampling log 1000` `switch (config) # no telemetry sampling log`	
Related Commands		
Notes		

telemetry threshold

	telemetry threshold **no telemetry threshold** Enables telemetry threshold on hardware. The no form of the command disables threshold.
Syntax Description	N/A
Default	false
Configuration Mode	config interface ib
History	3.6.4006
Role	admin
Example	`switch (config interface ib 1/1) # telemetry threshold`
Related Commands	
Notes	

telemetry threshold level

	telemetry threshold level **no telemetry threshold level** Configures threshold level in hardware per port. The no form of the command resets threshold to default value.	
Syntax Description	Level	Input range: 96-1000000 (in bytes and in increments of 96)
Default	69984	
Configuration Mode	config interface ib	
History	3.6.4006	
Role	admin	
Example	`switch (config interface ib 1/1) # telemetry threshold level 288`	
Related Commands		
Notes		

telemetry threshold log

	telemetry threshold log **no telemetry threshold log** Enables logging of threshold events in syslog. The no form of the command disable logging.
Syntax Description	N/A
Default	false
Configuration Mode	config
History	3.6.4006
Role	admin
Example	`switch (config) # telemetry threshold log` `switch (config) # no telemetry threshold log`
Related Commands	
Notes	

telemetry threshold record

	telemetry threshold record **no telemetry threshold record** Enables top talker configuration. The no form of the command disables top talker configuration.
Syntax Description	N/A
Default	Disabled
Configuration Mode	config interface ib
History	3.6.6105 3.6.8100 Updated notes
Role	admin
Example	`switch (config interfaces ib 1/2) # telemetry threshold record`
Related Commands	clear telemetry threshold record show telemetry threshold record
Notes	• When top talker is enabled, the minimal threshold window supported is 20 msecs. • Due to event timing issues, very short threshold events may not gather sufficient traffic samples to allow top-talker analysis. As a result, top-talkers may not be fully displayed in the relevant show command.

telemetry threshold syslog

telemetry threshold syslog <time>
no telemetry threshold syslog <time>

The command sets threshold events logging rate on per hour basis.
The no form of the command sets the logging rate back to default.

Syntax Description	time	Max rate per hour. Input range: 1-3600
Default	100	
Configuration Mode	config	
History	3.6.4006	
Role	admin	
Example	`switch (config) # telemetry threshold syslog 400`	
Related Commands		
Notes		

clear telemetry

clear telemetry {threshold | sampling} [interface <type> <port-id>]]

Clears telemetry data.

Syntax Description	type	Possible values: ib
Default	N/A	
Configuration Mode	config interface ib	
History	3.6.5000	
Role	admin	
Example	`switch (config ib 1/12) # clear telemetry threshold level 288`	
Related Commands		
Notes		

clear telemetry threshold

clear telemetry threshold [interface <type> <if>]

Clears threshold and top talker data.

Syntax Description	type	Possible values: ib
Default	N/A	
Configuration Mode	config	
History	3.6.6105	
Role	admin	
Example	`switch (config) # clear telemetry threshold interface ib 1/34-1/36`	
Related Commands		
Notes		

clear telemetry threshold record

clear telemetry threshold record [interface ib <if>]

Clears top talker data.

Syntax Description	type	Possible values: ib
Default	N/A	
Configuration Mode	config	
History	3.6.6105	
Role	admin	
Example	`switch (config) # clear telemetry threshold record interface ib 1/34-1/36`	
Related Commands	telemetry threshold record show telemetry threshold record	
Notes		

stats export csv telemetry

stats export csv telemetry <slot>/<port>[/<subport>] [filename *] [after * *] [before * *]

Exports histograms collected by stats to a csv file.

Syntax Description	slot/port	Port number
	subport	Sub-port number to be used in case of split port
Default	N/A	
Configuration Mode	Any command mode	
History	3.6.3004	
Role	admin	
Example	`switch (config) # stats export csv telemetry 1/1` `Generated report file: telemetry-20170119-102715.csv`	
Related Commands		
Notes		

file stats telemetry delete

	file stats telemetry delete <filename> Deletes the given .csv file created by “stats export” command to user directory.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.3004
Role	admin
Example	`switch (config) # file stats telemetry delete telemetry-20171006-102158.csv`
Related Commands	
Notes	

file stats telemetry upload

	file stats telemetry upload <filename> <upload-url> Uploads .csv file created by “stats export” command to user directory.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.3004
Role	admin
Example	`switch (config) # file stats telemetry upload telemetry-20170119-102715.csv scp://username:password@server//directory` `Password (if required): ******`
Related Commands	
Notes	

show telemetry

show telemetry

Displays the global configuration of telemetry properties.

Syntax Description	N/A
Default	
Configuration Mode	config
History	3.6.4000
Role	admin

Example

```
switch (config) # show telemetry
Telemetry Status                  : Enabled
H/W Sampling Interval(nsec)       : 512
S/W Sampling Interval(ms)         : 1000
Threshold Logging                 : Disabled
Threshold Logging(rate per hour)  : 100

-------------------------------------------------------------------------------------------
Interface          Sampling           Threshold          Record             Level (bytes)
-------------------------------------------------------------------------------------------
IB1/1              Disabled           Enabled            Enabled            100 (96)
IB1/2              Disabled           Enabled            Enabled            100 (96)
IB1/3              Disabled           Disabled           Disabled           N/A
IB1/4              Disabled           Disabled           Disabled           N/A
IB1/5              Disabled           Disabled           Disabled           N/A
IB1/6              Disabled           Disabled           Disabled           N/A
IB1/7              Disabled           Disabled           Disabled           N/A
...
IB1/36             Disabled           Disabled           Disabled           N/A
```

Related Commands	
Notes	

show telemetry threshold record

	show telemetry threshold record [interface ib <interface-id> | <interface-id-range>] Displays top talker events for all configured ports.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.4006 3.6.6105 Updated Example 3.6.8100 Updated Example
Role	admin

Example

```
switch (config) # show telemetry threshold record interface ib 1/11-1/12
-------------------------------------------------------------------------------------------------------------
Event-id  Date      Time      Port      Level   Duration(100 usec)   Repeated   DestQP   DLID   SLID   Percent(%)
-------------------------------------------------------------------------------------------------------------
1         07/10/18  14:00:31  IB 1/11   69984   48749.77             1          2741     29     32     62.30
2         07/10/18  14:01:47  IB 1/11   69984   63936.16             1          2745     29     32     54.55
```

Related Commands	clear telemetry threshold
Notes	• The values displayed of the SLID, DLID, and QP fields are in decimal • The command supports displaying up to 1000 threshold events. As a result, if more than 1000 thresholds configured in total, some interfaces may not be displayed. Therefore, to query thresholds for a specific interface, please use “show telemetry threshold interface ib <interface>”.

show telemetry sampling interface ib

show telemetry sampling interface ib <slot>/<port>

Displays telemetry histogram samples for a specific ib interface.

Syntax Description	slot/port	Infiniband port number
Default	N/A	
Configuration Mode	Any command mode	
History	3.6.3004	
Role	admin	

Example

```
switch (config) # show telemetry sampling interface ib 1/32
-------------------------------------------------------------------------------------------------------------------------
Telemetry histogram: IB1/32
System-time                                        Bin sizes (128 nsec tx buffer was occupied in bytes range)
-------------------------------------------------------------------------------------------------------------------------
02/09/17        <2976       35744       68512       101280      134048      166816      199584      232352      265120      265120<
12:19:03.41948  1883        8538        7802080     0           0           0           0           0           0           0
12:19:04.42107  830         9001        7802670     0           0           0           0           0           0           0
12:19:05.42249  96          9705        7802700     0           0           0           0           0           0           0
12:19:06.42388  32          9035        7803434     0           0           0           0           0           0           0
12:19:07.42573  80          9461        7802960     0           0           0           0           0           0           0
12:19:08.42761  160         9302        7803040     0           0           0           0           0           0           0
12:19:09.42915  304         9369        7802829     0           0           0           0           0           0           0
12:19:10.43071  96          8906        7803500     0           0           0           0           0           0           0
12:19:11.43215  463         8907        7803132     0           0           0           0           0           0           0
12:19:12.43369  256         8571        7803675     0           0           0           0           0           0           0
```

Related Commands	
Notes	In case requested entries are more than what the DB contains it will print the amount in the table.

show telemetry sampling interface ib last

show telemetry sampling interface ib <slot>/<port> last <num_of_entries>

Displays fetched unicast histogram details for tc_id of an Ethernet interface.

Syntax Description	slot/port	Infiniband port number
	num_of_entries	
Default	N/A	
Configuration Mode	Any command mode	
History	3.6.3004	
Role	admin	

Example

```
switch (config) # show telemetry sampling interface ib 1/36 last 20
Legend:
       2976    bytes - between 0       - 2976    of tx bytes buffer consumed
       35744   bytes - between 2977    - 35744   of tx bytes buffer consumed
-------------------------------------------------------------------------------------------------------------------------------
Telemetry histogram: IB1/36
System-time                                          Bin sizes (128 nsec tx buffer was occupied in bytes range)
-------------------------------------------------------------------------------------------------------------------------------
02/09/17          <2976       35744       68512       101280      134048      166816      199584      232352      265120      265120<
12:19:03.41948    1883        8538        7802080     0           0           0           0           0           0           0
12:19:04.42107    830         9001        7802670     0           0           0           0           0           0           0
12:19:05.42249    96          9705        7802700     0           0           0           0           0           0           0
12:19:06.42388    32          9035        7803434     0           0           0           0           0           0           0
12:19:07.42573    80          9461        7802960     0           0           0           0           0           0           0
```

Related Commands	
Notes	If requested entries are more than what the DB contains, it prints the amount in the table.

show files stats telemetry

show files stats telemetry [filename]

Displays all files created by the command “stats export csv telemetry”.

Syntax Description	filename	Displays stats for the specified file
Default	N/A	
Configuration Mode	Any command mode	
History	3.6.3004	
	3.6.8008	Updated Example
Role	admin	

Example	`switch (config) # show files stats telemetry telemetry-20180527-102715.csv`
	`Hostname :test-switch`
	`Report :telemetry histogram`
	`Time lower bound(UTC) :2018/05/28 05:58:10`
	`Time upper bound(UTC) :2018/05/28 05:58:25`
	`Export time(UTC) :2018/05/28 06:00:06`
	`Time lower bound :2018/05/28 08:58:10 +0300`
	`Time upper bound :2018/05/28 08:58:25 +0300`
	`Export time :2018/05/28 09:00:06 +0300`
	`System version :X86_64 sys_test 2018-05-15 04:02:13 x86_64`	

Related Commands	stats export csv telemetry	
Notes		

4.11 mDNS

Multicast DNS (mDNS) protocol is used by the SM HA to deliver control information between the InfiniBand nodes via the management interface. To block sending mDNS traffic from the management interface run the command `no ha dns enable`.

4.11.1 Commands

ha dns enable

	ha dns enable **no ha dns enable** Allows mDNS traffic. The no form of the command blocks mDNS traffic from being sent from mgmt0.
Syntax Description	N/A
Default	Enabled.
Configuration Mode	config
History	3.3.4000
Role	admin
Example	`switch (config) # no ha dns enable` `switch (config) #`
Related Commands	
Notes	

4.12 User Management and Security

4.12.1 User Accounts

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

Table 26 - User Roles (Accounts) and Default Passwords

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

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

4.12.2 Authentication, Authorization and Accounting (AAA)

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

4.12.2.1 User Re-authentication

Re-authentication prevents users from accessing resources or perform tasks for which they do not have authorization. If credential information (e.g. AAA server information like IP address, key, port number etc.) that has been previously used to authenticate a user is modified, that user gets immediately logged out of the switch and asked to re-authenticate.

4.12.2.2 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

4.12.2.3 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

4.12.2.4 LDAP

LDAP (Lightweight Directory Access Protocol) is an authentication protocol that allows a remote access server to forward a user's log-on 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
```

4.12.3 System Secure Mode

System secure mode is a state that configures the switch system to run secure algorithms in compliance with FIPS 140-2 requirements. In this mode, unsecure algorithms are disabled and unsecure feature configurations are disallowed.

In this mode the system supports Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules, which is a NIST (National Institute of Standards and Technology) publication that specifies the requirement for system cypher functionality.

When this mode is activated, all the modules which are used by the system are verified to work in compliance with the secure mode.

Note that if system fails to load in secure mode it is loaded in non-secure mode.

Prerequisites:

Step 1. Disable SNMPv1 and v2. Run:

```
switch (config) # no snmp-server enable communities
```

Step 2. Only allow SNMPv3 users with sha and aes-128. Run:

```
switch (config) # snmp-server user <username> v3 auth sha <password1> priv aes-128
<password2>
```

Step 3. Only allow SNMPv3 traps with sha and aes-128. Run:

```
switch (config) # snmp-server host <ip-address> informs version 3 user <username> auth
sha <password1> priv aes-128 <password2>
```

Step 4. Only allow SSHv2. Run:

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

Step 5. Enable SSH server strict security mode. Run:

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

Step 6. Disable HTTP access. Run:

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

Step 7. Enable HTTPS strict cyphers. Run:

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

Step 8. Disable router BGP neighbor password configuration. Run:

```
switch (config) # no router bgp <as-number> neighbor <ip-address> password
```

Step 9. Disable router BGP peer group password configuration. Run:

```
switch (config) # no router bgp <as-number> peer-group <peer-group-name> password
```

Step 10. Disable BGP password configuration. Run:

```
switch (config) # no neighbor <ip-address> password
```

Step 11. Disable MD5 password hashing on for users. Run:

```
switch (config) # username <username> password <password>
```

If a necessary prerequisite is not fulfilled the system does not activate secure mode and issues an advisory message accordingly.

Secure mode is not supported on director switch systems.

- ***To activate secure mode:***

```
switch (config) # system secure-mode enable

Warning! Configuration is about to be saved and the system will be reloaded.
  Type 'YES' to confirm the change in secure mode: YES
```

- ***To deactivate secure mode:***

```
switch (config) # no system secure-mode enable

Warning! Configuration is about to be saved and the system will be reloaded.
  Type 'YES' to confirm the change in secure mode: YES
```

- ***To verify secure mode configuration and state:***

```
switch (config)# show system secure-mode

Secure mode configured: yes
Secure mode enabled: yes
  switch (config) #
```

4.12.4 Commands

4.12.4.1 User Accounts

username

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

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

Syntax Description	username	Specifies a username and creates a user account. New users are created initially with admin privileges but is disabled.
	capability <cap>	Defines user capabilities. • admin - full administrative capabilities • monitor - read only capabilities, can not change the running configuration • unpriv – can only query the most basic information, and cannot take any actions or change any configuration • v_admin – basic administrator capabilities
	disable [login | password]	• Disable - disable this account • Disable login - disable all logins to this account • Disable password - disable login to this account using a local password
	disconnect	Logs out the specified user from the system
	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	
	3.4.0000	Updated Example

	3.4.1100	Updated Example
	3.6.2002	Added “disconnect” parameter

Role

admin

Example

```
switch (config) # username monitor full-name smith
switch (config) # show usernames
USERNAME    FULL NAME               CAPABILITY  ACCOUNT STATUS
USERID      System Administrator    admin       Password set
admin       System Administrator    admin       Password set
monitor     smith                   monitor     Password set (SHA512)
xmladmin    XML Admin User          admin       Password set (SHA512)
xmluser     XML Monitor User        monitor     Password set (SHA512)
switch (config) #
```

Related Commands

show usernames
show users

Notes

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

show usernames

	show usernames Displays list of users and their capabilities.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

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

Related Commands	username show users
Notes	

show users

show users [history]

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

Syntax Description	history	Displays current and historical sessions.
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show users`
	`USERNAME  FULL NAME  LINE  HOST  IDLE`
	`admin  System Administrator  pts/0  172.22.237.174  0d0h34m4s`
	`admin  System Administrator  pts/1  172.30.0.127  1d3h30m49s`
	`admin  System Administrator  pts/3  172.22.237.34  0d0h0m0s`
	`switch (config) #show users history`
	`admin  pts/3 172.22.237.34  Wed Feb  1 11:56  still logged in`
	`admin  pts/3 172.22.237.34  Wed Feb  1 11:42 - 11:46  (00:04)`
	
	`wtmp begins Wed Feb  1 11:38:10 2012`
	`switch (config) #`	

Related Commands	username show usernames	
Notes		

show whoami

	show whoami Displays username and capabilities of user currently logged in.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

Example	`switch (config) # show whoami`
	`Current user: admin`
	`Capabilities: admin`
	`switch (config) #`

Related Commands	username show usernames show users
Notes	

4.12.4.2 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 3.2.3000 Removed ‘time’ parameter from the command.
Role	admin

Example	`switch (config) # aaa accounting changes default stop-only tacacs+`
	`switch (config) # show aaa`
	`AAA authorization:`
	`  Default User: admin`
	`  Map Order: local-only`
	`Authentication method(s):`
	`  local`
	`  radius`
	`  tacacs+`
	`  ldap`
	`Accounting method(s):`
	`  tacacs+`
	`switch (config) #`

Related Commands	show aaa
Notes	• TACACS+ is presently the only accounting service method supported • Change accounting covers both configuration changes and system actions that are visible under audit logging, however this feature operates independently of audit logging, so it is unaffected by the “logging level audit mgmt” or “configuration audit” commands • Configured TACACS+ servers are contacted in the order in which they appear in the configuration until one accepts the accounting data, or the server list is exhausted • Despite the name of the “stop-only” keyword, which indicates that this feature logs a TACACS+ accounting “stop” message, and in contrast to configuration change accounting, which happens after configuration database changes, system actions are logged when the action is started, not when the action has completed

aaa authentication login

	aaa authentication login default <auth method> [<auth method> [<auth method> [<auth method> [<auth method>]]]] **no aaa authentication login** Sets a sequence of authentication methods. Up to four methods can be configured. The no form of the command resets the configuration to its default.	
Syntax Description	auth-method	• local • radius • tacacs+ • ldap
Default	local	
Configuration Mode	Any command mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # aaa authentication login default local radius tacacs+ ldap`
	`switch (config) # show aaa`
	`AAA authorization:`
	`  Default User: admin`
	`  Map Order: local-only`
	`Authentication method(s):`
	`  local`
	`  radius`
	`  tacacs+`
	`  ldap`
	`Accounting method(s):`
	`  tacacs+`
	`switch (config) #`	

Related Commands	show aaa	
Notes	The order in which the methods are specified is the order in which the authentication is attempted. It is required that “local” is one of the methods selected. It is recommended that “local” be listed first to avoid potential problems logging in to local accounts in the face of network or remote server issues.	

aaa authentication attempts fail-delay

aaa authentication attempts fail-delay <time>
no aaa authentication attempts fail-delay

Configures delay for a specific period of time after every authentication failure. The no form of the command resets the fail-delay to its default value.

Syntax Description	time	Range: 0-60 seconds
Default	0	
Configuration Mode	config	
History	3.5.0200	
Role	admin	
Example	`switch (config) # aaa authentication attempts fail-delay 1`	
Related Commands	N/A	
Notes		

aaa authentication attempts track

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

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

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

aaa authentication attempts lockout

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

Configures lockout of accounts based on failed authentication attempts.
The no form of the command clears configuration for lockout of accounts based on failed authentication attempts.

Syntax Description	enable	Enables locking out of user accounts based on authentication failures. This both suspends enforcement of any existing lockouts, and prevents any new lockouts from being recorded. If lockouts are later re-enabled, any lockouts that had been recorded previously resume being enforced; but accounts which have passed the max-fail limit in the meantime are NOT automatically locked at this time. They would be permitted one more attempt, and then locked, because of how the locking is done: lockouts are applied after an authentication failure, if the user has surpassed the threshold at that time. Lockouts only work if tracking is enabled. Enabling lockouts automatically enables tracking. Disabling tracking automatically disables lockouts.
	lock-time	Sets maximum permitted consecutive authentication failures before locking out users. Unlike the “max-fail” setting, this does take effect immediately for all accounts If both unlock-time and lock-time are set, the unlock-time must be greater than the lock-time This is not based on the number of consecutive failures, and is therefore divorced from most of the rest of the tally feature, except for the tracking of the last login failure
	max-fail	Sets maximum permitted consecutive authentication failures before locking out users. This setting only impacts what lockouts are imposed while the setting is active; it is not retroactive to previous logins. So if max-fail is disabled or changed, this does not immediately cause any users to be changed from locked to unlocked or vice-versa.
	unlock-time	Enables the auto-unlock of an account after a specified number of seconds if a user account is locked due to authentication failures, counting from the last valid login attempt. Unlike the “max-fail” setting, this does take effect immediately for all accounts. If both unlock-time and lock-time are set, the unlock-time must be greater than the lock-time. Careful with disabling the unlock-time, particularly if you have max-fail set to something, and have not overridden the behavior for the admin (i.e. they are subject to lockouts also). If the admin account gets locked out, and there are no other administrators who can aid, the user may be forced to boot single-user and use the pam_tallybyname command-line utility to unlock your account manually. Even if one is careful not to incur this many authentication failures, it makes the system more subject to DOS attacks.

Default	N/A
Configuration Mode	config
History	3.2.3000
Role	admin
Example	`switch (config) # aaa authentication attempts lockout enable`
Related Commands	N/A
Notes	

aaa authentication attempts class-override

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

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

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

aaa authentication attempts reset

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

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

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

clear aaa authentication attempts

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

Clears the authentication history for and/or unlocks specified users

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

aaa authorization

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

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+ or LDAP) and does not have a local account. If the username is local, this mapping is ignored.
	order <policy>	Sets the user mapping behavior when authenticating users via RADIUS or TACACS+ or LDAP 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: • 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. • 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.
	fallback	Sets the authenticating fallback behavior via RADIUS or TACACS+ or LDAP. This option attempts to authenticate username through the next authentication method listed in case of an error. • server-err – performs fallback if an error occurs while connecting to remote AAA server (e.g. server is down, not responding, etc)
Default	Default user – admin Map order – remote-first Order fallback – server-err	
Configuration Mode	config	
History	3.1.0000	
	3.7.00xx	Added "fallback" parameter

	3.7.10xx	Updated syntax
Role	admin	
Example	`switch (config) # aaa authorization map default-user admin` `switch (config) #`	
Related Commands	show aaa username	
Notes	• If, for example, the user is locally defined to have admin permission, but in a remote server such as RADIUS the user is authenticated as monitor and the order is remote-first, then the user is given monitor permissions. • If AAA authorization order policy is configured to remote-only, then when upgrading to 3.4.3000 or later from an older MLNX-OS version, this policy is changed to remote-first. • The user must be careful when disabling AAA authorization map fallback server-err, because if the remote server stops working then the user may lock themselves out.	

show aaa

	show aaa Displays the AAA configuration.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.7.0020 Example updated
Role	admin

Example	`switch (config) # show aaa`
	`AAA authorization:`
	`  Default User: admin`
	`  Map Order: remote-first`
	`  Fallback on server-err: yes`
	`Authentication method(s):`
	`  local`
	`Accounting method(s):`
	`  tacacs+`
	`switch (config) #`

Related Commands	aaa accounting aaa authentication aaa authorization show aaa show usernames username
Notes	

show aaa authentication attempts

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

Shows the current authentication, authorization and accounting settings.

Syntax Description	authentication attempts	Displays configuration and history of authentication failures.
	configured	Displays configuration of authentication failure tracking.
	status user	Displays status of authentication failure tracking and lockouts for specific user.
Default	N/A	
Configuration Mode	Any command mode	
History	3.2.1000	
	3.5.0200	Updated Example
Role	admin	

Example

```
switch (config) # show aaa authentication attempts
Configuration for authentication failure tracking and locking:
   Track authentication failures:                    yes
   Lock accounts based on authentication failures:   yes
   Override treatment of 'admin' user:               (none)
   Override treatment of unknown usernames:          hash-usernames
   Convert usernames to lowercase for tracking:      no
   Delay after each auth failure (fail delay):       none


Configuration for lockouts based on authentication failures:
   Lock account after consecutive auth failures:    5
   Allow retry on locked accounts (unlock time):    after 15 second(s)
   Temp lock after each auth failure (lock time):   none

Username                              Known  Locked  Failures  Last fail time        Last fail from
--------                              -----  ------  --------  -------------        -------------
0Q72B43EHBKT8CB5AF5PGRX3U3B3TUL4CYJP93N(*) no     no         1     2012/08/20 14:29:19   ttyS0

(*) Hashed for security reasons
switch-627d3c [standalone: master] (config) #
switch (config) #
```

Related Commands	N/A
Notes	

4.12.4.3 RADIUS

radius-server

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

Sets global RADIUS server attributes.
The no form of the command resets the attributes to their default values.

Syntax Description	secret	Sets a secret key (shared hidden text string), known to the system and to the RADIUS server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry (1-60).
Default	3 seconds, 1 retry	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # radius-server retransmit 3`	
Related Commands	aaa authorization radius-server host show radius	
Notes	Each RADIUS server can override those global parameters using the command “radius-server host”.	

radius-server host

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

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

Syntax Description	IP address	RADIUS server IP address
	enable	Administrative enable of the RADIUS server
	auth-port	Configures authentication port to use with this RADIUS server
	port	RADIUS server UDP port number
	key	Configures shared secret to use with this RADIUS server
	prompt-key	Prompt for key, rather than entering on command line
	retransmit	Configures retransmit count to use with this RADIUS server
	retries	Number of retries (0-5) before exhausting from the authentication
	timeout	Configures timeout between each try
	seconds	Timeout in seconds between each retry (1-60)
Default	3 seconds, 1 retry Default UDP port is 1812	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # radius-server host 40.40.40.40`	
Related Commands	aaa authorization radius-server show radius	
Notes	• RADIUS servers are tried in the order they are configured • If you do not specify a parameter for this configured RADIUS server, the configuration will be taken from the global RADIUS server configuration. Refer to “radius-server” command.	

show radius

	show radius Displays RADIUS configurations.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show radius`
	`RADIUS defaults:`
	`  Key       : ********`
	`  Timeout   : 3`
	`  Retransmit: 1`
	
	`RADIUS servers:`
	`  1.1.1.1:1812:`
	`    Enabled   : yes`
	`    Key       : ********`
	`    Timeout   : 3 (default)`
	`    Retransmit: 1 (default)`

Related Commands	aaa authorization radius-server radius-server host
Notes	

4.12.4.4 TACACS+

tacacs-server

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

Sets global TACACS+ server attributes.
The no form of the command resets the attributes to default values.

Syntax Description	secret	Set a secret key (shared hidden text string), known to the system and to the TACACS+ server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry (1-60).
Default	3 seconds, 1 retry	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # tacacs-server retransmit 3`	
Related Commands	aaa authorization show radius show tacacs tacacs-server host	
Notes	Each TACACS+ server can override those global parameters using the command “tacacs-server host”.	

tacacs-server host

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

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

Syntax Description	IP address	TACACS+ server IP address
	enable	Administrative enable for the TACACS+ server
	auth-port	Configures authentication port to use with this TACACS+ server
	port	TACACS+ server UDP port number
	auth-type	Configures authentication type to use with this TACACS+ server
	type	Authentication type. Possible values are: • ASCII • PAP (Password Authentication Protocol)
	key	Configures shared secret to use with this TACACS+ server
	secret	Sets a secret key (shared hidden text string), known to the system and to the TACACS+ server
	prompt-key	Prompts for key, rather than entering key on command line
	retransmit	Configures retransmit count to use with this TACACS+ server
	retries	Number of retries (0-5) before exhausting from the authentication
	timeout	Configures timeout to use with this TACACS+ server
	seconds	Timeout in seconds between each retry (1-60)
Default	3 seconds, 1 retry Default TCP port is 49 Default auth-type is PAP	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # tacacs-server host 40.40.40.40`
Related Commands	aaa authorization show tacacs tacacs-server
Notes	• TACACS+ servers are tried in the order they are configured • A PAP auth-type similar to an ASCII login, except that the username and password arrive at the network access server in a PAP protocol packet instead of being typed in by the user, so the user is not prompted • If the user does not specify a parameter for this configured TACACS+ server, the configuration will be taken from the global TACACS+ server configuration. Refer to “tacacs-server” command.

show tacacs

	show tacacs Displays TACACS+ configurations.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show tacacs`
	`TACACS+ defaults:`
	`  Key       :  ********`
	`  Timeout   :  3`
	`  Retransmit:  1`
	
	`TACACS+ servers:`
	`  1.1.1.1:49:`
	`    Enabled   : yes`
	`    Auth Type : pap`
	`    Key       : ********`
	`    Timeout   : 3 (default)`
	`    Retransmit: 1 (default)`

Related Commands	aaa authorization tacacs-server tacacs-server host
Notes	

4.12.4.5 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	
	3.4.0000	Updated Example
Role	admin	
Example	`switch (config) # ldap base-dn ou=department,dc=example,dc=com`	
Related Commands	show ldap	
Notes		

ldap bind-dn/bind-password

ldap {bind-dn | bind-password} <string>
no ldap {bind-dn | bind-password}

Gives the distinguished name or password to bind to on the LDAP server. This can be left empty for anonymous login (the default).
The no form of the command resets the attribute to its default values.

Syntax Description	string	A case-sensitive string that specifies distinguished name or password to bind to on the LDAP server.
Default	“”	
Configuration Mode	config	
History	3.1.0000	
	3.4.0000	Updated Example
Role	admin	
Example	`switch (config) # ldap bind-dn my-dn` `switch (config) # ldap bind-password my-password`	
Related Commands	show ldap	
Notes	For anonymous login, bind-dn and bind-password should be empty strings “”.	

ldap group-attribute/group-dn

ldap {group-attribute {<group-att> |member | uniqueMember} | group-dn <group-dn>}
no ldap {group-attribute | group-dn}

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

Syntax Description	group-att	Specifies a custom attribute name.
	member	groupOfNames or group membership attribute.
	uniqueMember	groupOfUniqueNames membership attribute.
	group-dn	DN of group required for authorization.
Default	group-att: member group-dn: “”	
Configuration Mode	config	
History	3.1.0000	
	3.4.0000	Updated Example
Role	admin	
Example	`switch (config) # ldap group-attribute member` `switch (config) # ldap group-dn my-group-dn`	
Related Commands	show ldap	
Notes	• The user’s distinguished name must be listed as one of the values of this attribute, or the user will not be authorized to log in • After login authentication, if the group-dn is set, a user must be a member of this group or the user will not be authorized to log in. If the group is not set (“” - the default) no authorization checks are done.	

ldap host

ldap host <IP Address> [order <number> last]
no ldap host <IP Address>

Adds an LDAP server to the set of servers used for authentication.
The no form of the command deletes the LDAP host.

Syntax Description	IP Address	IPv4 or IPv6 address.
	number	The order of the LDAP server.
	last	The LDAP server will be added in the last location.
Default	No hosts configured	
Configuration Mode	config	
History	3.1.0000	
	3.4.0000	Updated Example
Role	admin	
Example	`switch (config) # ldap host 10.10.10.10`	
Related Commands	show aaa show ldap	
Notes	• The system will select the LDAP host to try according to its order • New servers are by default added at the end of the list of servers	

ldap hostname-check enable

	ldap hostname-check enable **no ldap hostname-check enable** Enables LDAP hostname check. The no form of the command disables LDAP hostname check.
Syntax Description	N/A
Default	No hosts configured
Configuration Mode	config
History	3.6.8008
Role	admin
Example	`switch (config) # ldap hostname-check enable`
Related Commands	show aaa show ldap
Notes	

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	
	3.4.0000	Updated Example
Role	admin	
Example	`switch (config) # ldap login-attribute uid`	
Related Commands	show aaa show ldap	
Notes		

ldap port

ldap port <port>
no ldap port

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

Syntax Description	port	TCP port number.
Default	389	
Configuration Mode	config	
History	3.1.0000	
	3.4.0000	Updated Example
Role	admin	
Example	`switch (config) # ldap port 1111`	
Related Commands	show aaa show ldap	
Notes		

ldap referrals

	ldap referrals **no ldap referrals** Enables LDAP referrals. The no form of the command disables LDAP referrals.
Syntax Description	N/A
Default	LDAP referrals are enabled
Configuration Mode	config
History	3.1.0000 3.4.0000 Updated Example
Role	admin
Example	`switch (config) # no ldap referrals`
Related Commands	show aaa show ldap
Notes	Referral is the process by which an LDAP server, instead of returning a result, will return a referral (a reference) to another LDAP server which may contain further information.

ldap scope

	ldap scope <scope> **no ldap scope** Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request. The no form of the command resets the attribute to its default value.	
Syntax Description	scope	• one-level - searches the immediate children of the base dn • subtree - searches at the base DN and all its children
Default	subtree	
Configuration Mode	config	
History	3.1.0000	
	3.4.0000	Updated Example
Role	admin	
Example	`switch (config) # ldap scope subtree`	
Related Commands	show aaa show ldap	
Notes		

ldap ssl

ldap ssl {ca-list <options> | cert-verify | ciphers {all | TLS1.2} | crl-check {enable | file fetch <path>} | mode <mode> | port <port-number>}
no ldap ssl {cert-verify | ciphers | crl-check enable | 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.
	crl-check enable	Enables LDAP CRL check
	crl-check file fetch	Fetches CRL from remote server. CRL must be a valid PEM file unless a proper message shown. Supported formats: SCP, HTTP, HTTPS, FTP, and FTPS.
	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	
	3.2.3000	Added ca-list argument.
	3.4.0000	Added “ssl ciphers” parameter and updated Example
	3.6.8008	Added the parameter “crl-check”
Role	admin	

Example	`switch (config) # ldap ssl crl-check file fetch scp://root:pass@1.1.1.1/etc/pki/crl.pem`
	
	`100.0%`
	`[##########################################################################]`	

Related Commands	show aaa show ldap	
Notes	• If available, the TLS mode is recommended, as it is standardized, and may also be of higher security • The port number is used only for SSL mode. In case the mode is TLS, the LDAP port number will be used.	

ldap timeout

ldap {timeout-bind | timeout-search} <seconds>
no ldap {timeout-bind | timeout-search}

Sets a global communication timeout in seconds for all LDAP servers to specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.
The no form of the command resets the attribute to its default value.

Syntax Description	timeout-bind	Sets the global LDAP bind timeout for all LDAP servers.
	timeout-search	Sets the global LDAP search timeout for all LDAP servers.
	seconds	Range: 1-60 seconds.
Default	5 seconds	
Configuration Mode	config	
History	3.1.0000	
	3.4.0000	Updated Example
Role	admin	
Example	`switch (config) # ldap timeout-bind 10`	
Related Commands	show aaa show ldap	
Notes		

ldap version

ldap version <version>
no ldap version

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

Syntax Description	version	Sets the LDAP version. Values: 2 and 3.
Default	3	
Configuration Mode	config	
History	3.1.0000	
	3.4.0000	Updated Example
Role	admin	
Example	`switch (config) # ldap version 3`	
Related Commands	show aaa show ldap	
Notes		

show ldap

	show ldap Displays LDAP configurations.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.4.0000 Updated Example 3.6.8008 Updated Example
Role	admin

Example	`switch (config) # show ldap`
	
	`User base DN : ou=users,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`
	`Server Hostname check: no`
	`SSL mode : none`
	`Server SSL port : 636 (not active)`
	`SSL ciphers : all (not active)`
	`SSL cert verify : yes`
	`SSL ca-list : default-ca-list`
	`SSL CRL check : no`

Related Commands	show aaa show ldap
Notes	

show ldap crl

	show ldap crl Displays current CRL configured by the user.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.8008
Role	admin

Example	`switch (config) # show ldap crl`
	`-----BEGIN CERTIFICATE-----`
	`MIIDVzCSd……`
	`-----END CERTIFICATE-----`

Related Commands	show aaa show ldap
Notes	

4.12.4.6 System Secure Mode

system secure-mode enable

system secure-mode enable
no system secure-mode enable

Enables secure mode on the switch.
The no form of the command disables secure mode.

Syntax Description	N/A
Default	Disabled
Configuration Mode	config
History	3.5.0200
Role	admin

Example	`switch (config) # system secure-mode enable`
	
	`Warning! Configuration is about to be saved and the system will be reloaded.`
	`Type 'YES' to confirm the change in secure mode: YES`

Related Commands	user <username> password <password> ssh server min-version ssh server security strict snmp-server user no neighbor <ip-address> password ntp server disable ntp server keyID router bgp neighbor password router bgp peer-group password
Notes	Before enabling secure mode, the command performs the following configuration checks: • NTP Key ID cannot be MD5 when secure mode is enabled • SSH min-version cannot be 1 when enabling secure mode • SSH security must be set to strict security • SNMPv3 user auth cannot be md5 when enabling secure mode • SNMPv3 user priv cannot be des when enabling secure mode • SNMPv3 trap auth cannot be md5 when enabling secure mode • SNMPv3 trap priv cannot be des when enabling secure mode • Router BGP neighbor password cannot be set when enabling secure mode • Router BGP peer-group password cannot be set when enabling with secure mode • User password hash cannot be MD5 when secure mode is enabled Only if the check passes, secure mode is enabled on the switch system.

show system secure-mode

	show system secure-mode Displays the security mode of the switch system.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.4.2300
Role	admin

Example	`switch (config) # show system secure-mode`
	
	`Secure mode configured: yes`
	`Secure mode enabled : yes`
	`switch (config) #`

Related Commands	system secure-mode enable
Notes	“Secure mode configuration” describes the user configuration “Secure mode enabled” describes the system state

4.13 Cryptographic (X.509, IPSec) and Encryption

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.

4.13.1 System File Encryption

This feature encrypts all sensitive data on Mellanox systems including logs certificates, keys, etc.

➢ ***To activate encryption on the switch:***

Step 1. Enable encryption and configure key location as USB (if you are using a USB device). Run:

```
switch (config)# crypto encrypt-data key-location usb key mypassword

Warning! All sensitive files are about to be encrypted
- System will perform reset factory, configuration files will be preserved
- System will be rebooted
- Active configuration will be preserved
- Do not power-off, wait for the system to boot

Type 'YES' to confirm this action: YES
```

IMPORTANT NOTE
Encryption and decryption perform “reset factory keep-config” on the switch system once configured. This means that sysdumps, logs, and images are deleted.

The key may be saved locally as well by using the parameter “local” instead of “usb” but that configuration is less secure.

Step 2. After the system reboots, verify configuration. Run:

```
switch (config)# show crypto encrypt-data
Sensitive files encryption:
   Status:          enabled
   Key location:    usb
   Cipher:          aes256
```

Once encryption is enabled, reverting back to an older version while encrypted is not possible. The command “no crypto encrypt-data” must be run before attempting to downgrade to an older MLNX-OS version.

If encryption is enabled, upgrading to a new MLNX-OS version maintains the encryption configuration.

4.13.1.1 Commands

crypto encrypt-data

crypto encrypt-data key-location <local | usb> key <password>
no crypto encrypt-data

Enables and configures system file encryption.
The no form of the command decrypts sensitive information on the system.

Syntax Description	key-location	Configures where to store the encryption key: • local – Stores the key locally • usb – Stores the key on a USB device
	key	Configures a key
Default	N/A	
Configuration Mode	config	
History	3.6.1002	
Role	admin	

Example	`switch (config)# crypto encrypt-data key-location usb key mypassword`
	
	`Warning! All sensitive files are about to be encrypted`
	`- System will perform reset factory, configuration files will be preserved`
	`- System will be rebooted`
	`- Do not power-off, wait for the system to boot`
	
	`Type 'YES' to confirm this action: YES`	

Related Commands		
Notes	• It is recommended to store the encryption password on a USB device rather than locally • Enabling encryption may slightly slow system performance • If the key is stored on the USB, it must be plugged into the switch in order for the switch to boot. After the switch has booted, the USB key is no longer required and, for security purposes, it is recommended to remove it after running “usb eject”. The USB key may be needed again if the switch is rebooted or if the switch needs to be decrypted.	

crypto ipsec ike

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

Manage the IKE (ISAKMP) process or database state

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

crypto ipsec peer local

crypto ipsec peer <IPv4 or IPv6 address> local <IPv4 or IPv6 address> {enable | keying {ike [auth {hmac-md5 | hmac-sha1 | hmac-sha256 | null} | dh-group | disable | encrypt | exchange-mode | lifetime | local | mode | peer-identity | pfs-group | preshared-key | prompt-preshared-key | transform-set] | manual [auth | disable | encrypt | local-spi | mode | remote-spi]}}

Configures ipsec in the system.

Syntax Description	enable	Enables IPSec peering.
	ike	Configures IPSec peering using IKE ISAKMP to manage SA keys. It has the following optional parameters: • auth: Configures the authentication algorithm for IPSec peering • dh-group: Configures the phase1 Diffie-Hellman group proposed for secure IKE key exchange • disable: Configures this IPSec peering administratively disabled • encrypt: Configures the encryption algorithm for IPSec peering • exchange-mode: Configures the IKE key exchange mode to propose for peering • lifetime: Configures the SA lifetime to propose for this IPSec peering • local-identity: Configures the ISAKMP payload identification value to send as local endpoint's identity • mode: Configures the peering mode for this IPSec peering • peer-identity: Configures the identification value to match against the peer's ISAKMP payload identification • pfs-group: Configures the phase2 PFS (Perfect Forwarding Secrecy) group to propose for Diffie-Hellman exchange for this IPSec peering • preshared-key: Configures the IKE pre-shared key for the IPSec peering • prompt-preshared-key: Prompts for the pre-shared key, rather than entering it on the command line • transform-set: Configures transform proposal parameters
	keying	Configures key management for this IPSec peering: • auth: Configures the authentication algorithm for this IPSec peering • disable: Configures this IPSec peering administratively disabled • encrypt: Configures the encryption algorithm for this IPSec peering • local-spi: Configures the local SPI for this manual IPSec peering • mode: Configures the peering mode for this IPSec peering • remote-spi: Configures the remote SPI for this manual IPSec peering
	manual	Configures IPSec peering using manual keys.
Default	N/A	

Configuration Mode	config
History	3.2.3000
Role	admin
Example	`switch (config)# crypto ipsec peer 10.10.10.10 local 10.7.34.139 enable` `switch (config)#`
Related Commands	N/A
Notes	

crypto certificate ca-list

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

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

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

crypto certificate default-cert

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

Designates the named certificate as the global default certificate role for authentication of this system to clients.
The no form of the command reverts the default-cert name to “system-self-signed” (the “cert-name” value is optional and ignored).

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

crypto certificate generation

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

Configures default values for certificate generation.

Syntax Description	country-code	Configures the default certificate value for country code with a two-alphanumeric-character code or -- for none.
	days-valid	Configures the default certificate valid days. Default value: 365 days.
	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	
	3.3.4350	Added “hash-algorithm” parameter
	3.6.4000	Added “days-valid” parameter
Role	admin	
Example	`switch (config) # crypto certificate generation default hash-algorithm sha256`	
Related Commands	N/A	
Notes	The default hashing algorithm used is sha1.	

crypto certificate name

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

Configures default values for certificate generation.
The no form of the command clears/deletes certain certificate settings.

Syntax Description	cert-name	Unique name by which the certificate is identified.
	comment	Specifies a certificate comment.
	generate self-signed	Generates certificates. This option has the following parameters which may be entered sequentially in any order: • comment: Specifies a certificate comment (free string) • common-name: Specifies the common name of the issuer and subject (e.g. a domain name) • country-code: Specifies the country codwo-alpha-numeric-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. Default value is SHA256. • 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	
	3.3.4402	Added "hash-algorithm" parameter
	3.6.4000	Added "hash-algorithm" parameter
Role	admin	
Example	`switch (config) # crypto certificate name system-self-signed generate self-signed hash-algorithm sha256`	

Related Commands	N/A
Notes	

crypto certificate system-self-signed

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

Configures default values for certificate generation.

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

show crypto certificate

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

Displays information about all certificates in the certificate database.

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

Example

```
switch (config)# show crypto certificate
Certificate with name 'system-self-signed' (default-cert)
    Comment:                        system-generated self-signed certif-
icate
    Private Key:                    present
    Serial Number:                  0x546c935511bcafc21ac0e8249fbe0844
    SHA-1 Fingerprint:              fe6df38dd26801971cb2d44f62d-
be492b6063c5f

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

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

    Issuer:
        Common Name:                IBM-DEV-Bay4
        Country:                    IS
        State or Province:
        Locality:
        Organization:
        Organizational Unit:
        E-mail Address:
switch (config)#
```

Related Commands N/A

Notes

show crypto encrypt-data

	show encrypt-data Displays sensitive data encryption information.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.1002
Role	admin

Example	`switch (config)# show crypto encrypt-data`
	`Sensitive files encryption:`
	`  Status:  enabled`
	`  Key location:  usb`
	`  Cipher:  aes256`
	`switch (config)#`

Related Commands	N/A
Notes	

show crypto ipsec

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

Displays information ipsec configuration.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.2.1000
Role	admin

Example	`switch (config)# show crypto ipsec`
	`IPSec Summary`
	`-------------`
	`Crypto IKE is using pluto (Openswan) daemon.`
	`Daemon process state is stopped.`
	
	`No IPSec peers configured.`
	
	`IPSec IKE Peering State`
	`----------------------`
	`Crypto IKE is using pluto (Openswan) daemon.`
	`Daemon process state is stopped.`
	
	`No active IPSec IKE peers.`
	
	`IPSec Policy State`
	`------------------`
	`No active IPSec policies.`
	
	`IPSec Security Association State`
	`-------------------------------`
	`No active IPSec security associations.`
	`switch (config)#`

Related Commands	N/A
Notes	

4.14 Scheduled Jobs

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

4.14.1 Commands

job

job <job ID>
no job <job ID>

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

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

command

command <sequence #> | <command>
no command <sequence #>

Adds a CLI command to the job.
The no form of the command deletes the command from the job.

Syntax Description	sequence #	An integer that controls the order the command is executed relative to other commands in this job. The commands are executed in an ascending order.
	command	A CLI command.
Default	N/A	
Configuration Mode	config job	
History	3.1.0000	
Role	admin	

Example	`switch (config)# job 100`
	`switch (config job 100) # command 10 “show power”`
	`switch (config job 100) #`	

Related Commands	show jobs	
Notes	• The command must be defined with inverted commas (“”) • The command must be added as it was executed from the “config” mode. For example, in order to change the interface description you need to add the command: “interface <type> <number> description my-description”.	

comment

comment <comment>
no comment

Adds a comment to the job.
The no form of the command deletes the comment.

Syntax Description	comment	The comment to be added (string).
Default	“”	
Configuration Mode	config job	
History	3.1.0000	
Role	admin	

Example	`switch (config)# job 100`
	`switch (config job 100) # comment Job_for_example`
	`switch (config job 100) #`	

Related Commands	show jobs	
Notes		

enable

	enable **no enable** Enables the specified job. The no form of the command disables the specified job.
Syntax Description	N/A
Default	N/A
Configuration Mode	config job
History	3.1.0000
Role	admin

Example	`switch (config)# job 100`
	`switch (config job 100) # enable`
	`switch (config job 100) #`

Related Commands	show jobs
Notes	If a job is disabled, it will not be executed automatically according to its schedule; nor can it be executed manually.

execute

	execute Forces an immediate execution of the job.
Syntax Description	N/A
Default	N/A
Configuration Mode	config job
History	3.1.0000
Role	admin

Example	`switch (config)# job 100`
	`switch (config job 100) # execute`
	`switch (config job 100) #`

Related Commands	show jobs
Notes	• The job timer (if set) is not canceled and the job state is not changed: i.e. the time of the next automatic execution is not affected • The job will not be run if not currently enabled

fail-continue

	fail-continue **no fail-continue** Continues the job execution regardless of any job failures. The no form of the command returns fail-continue to its default.
Syntax Description	N/A
Default	A job will halt execution as soon as any of its commands fails
Configuration Mode	config job
History	3.1.0000
Role	admin

Example	`switch (config)# job 100`
	`switch (config job 100) # fail-continue`
	`switch (config job 100) #`

Related Commands	show jobs
Notes	

name

name <job name>
no name

Configures a name for this job.
The no form of the command resets the name to its default.

Syntax Description	name	Specifies a name for the job (string).
Default	“”.	
Configuration Mode	config job	
History	3.1.0000	
Role	admin	

Example	`switch (config)# job 100`
	`switch (config job 100) # name my-job`
	`switch (config job 100) #`	

Related Commands	show jobs	
Notes		

schedule type

schedule type <recurrence type>
no schedule type

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

Syntax Description	recurrence type	The available schedule types are: • daily - the job is executed every day at a specified time • weekly - the job is executed on a weekly basis • monthly - the job is executed every month on a specified day of the month • once - the job is executed once at a single specified date and time • periodic - the job is executed on a specified fixed time interval, starting from a fixed point in time.
Default	once	
Configuration Mode	config job	
History	3.1.0000	
Role	admin	

Example	`switch (config)# job 100`
	`switch (config job 100) # schedule type once`
	`switch (config job 100) #`	

Related Commands	show jobs	
Notes	A schedule type is essentially a structure for specifying one or more future dates and times for a job to execute.	

schedule <recurrence type>

schedule <recurrence type> <interval and date>
no schedule

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

Syntax Description	recurrence type	The available schedule types are: • daily - the job is executed every day at a specified time • weekly - the job is executed on a weekly basis • monthly - the job is executed every month on a specified day of the month • once - the job is executed once at a single specified date and time • periodic - the job is executed on a specified fixed time interval, starting from a fixed point in time.
	interval and date	Interval and date, per recurrence type.
Default	once	
Configuration Mode	config job	
History	3.1.0000	
Role	admin	

Example	`switch (config)# job 100`
	`switch (config job 100) # schedule monthly interval 10`
	`switch (config job 100) #`	

Related Commands	show jobs	
Notes	A schedule type is essentially a structure for specifying one or more future dates and times for a job to execute.	

show jobs

show jobs [<job-id>]

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

Syntax Description	job-id Job ID.
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show jobs 10`
	`Job 10:`
	`  Status: inactive`
	`  Enabled: yes`
	`  Continue on failure: no`
	`  Schedule Type: once`
	`  Time and date: 1970/01/01 00:00:00 +0000`
	`  Last Exec Time: Thu 2012/04/05 13:11:42 +0000`
	`  Next Exec Time: N/A`
	`  Commands:`
	`  Command 10: show power`
	`  Last Output:`
	`==========`
	`Module Status`
	`==========`
	`PS1 OK`
	`PS2 NOT PRESENT`
	
	`switch (config) #`

Related Commands	show jobs
Notes	

4.15 Statistics and Alarms

4.15.1 Commands

stats alarm <alarm-id> clear

stats alarm <alarm ID> clear

Clears alarm state.

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

stats alarm <alarm-id> enable

	stats alarm <alarm-id> enable **no stats alarm <alarm-id> enable** Enables the alarm. The no form of the command disables the alarm, notifications will not be received.	
Syntax Description	alarm ID	Alarms supported by the system, for example: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
Default	The default is different per alarm-id	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # stats alarm cpu_util_indiv enable` `switch (config) #`	
Related Commands	show stats alarm	
Notes		

stats alarm <alarm-id> event-repeat

stats alarm <alarm ID> event-repeat {single | while-not-cleared}
no stats alarm <alarm ID> event-repeat

Configures repetition of events from this alarm.

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

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

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

Configure alarms thresholds.

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

stats alarm <alarm-id> rate-limit

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

Configures alarms rate limit.

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

stats chd <chd-id> clear

stats chd <CHD ID> clear

Clears CHD counters.

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

Related Commands	show stats chd
Notes	

stats chd <chd-id> enable

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

Enables the CHD.
The no form of the command disables the CHD.

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

Related Commands	show stats chd
Notes	

stats chd <chd-id> compute time

stats chd <CHD ID> compute time {interval | range} <number of seconds>

Sets parameters for when this CHD is computed.

Syntax Description	CHD ID	Possible IDs: • cpu_util - CPU utilization: percentage of time spent • cpu_util_ave - CPU utilization average: percentage of time spent • cpu_util_day - CPU utilization average: percentage of time spent • disk_device_io_hour - Storage device I/O read/ write statistics for the last hour: bytes • disk_io - Operating system aggregate disk I/O average: KB/sec • eth_day • eth_hour • fs_mnt_day - Filesystem system usage average: bytes • fs_mnt_month - Filesystem system usage average: bytes • fs_mnt_week - Filesystem system usage average: bytes • ib_day • ib_hour • intf_day - Network interface statistics aggregation: bytes • intf_hour - Network interface statistics (same as “interface” sample) • intf_util - Aggregate network utilization across all interfaces • memory_day - Average physical memory usage: bytes • memory_pct - Average physical memory usage • paging - Paging activity: page faults • paging_day - Paging activity: page faults
	interval	Specifies calculation interval (how often to do a new calculation) in number of seconds.
	range	Specifies calculation range, in number of seconds.
	number of seconds	Number of seconds.
Default	Different per CHD	
Configuration Mode	config	
History	3.1.0000	
Role	monitor/admin	

Example	`switch (config) # stats chd memory_day compute time interval 120`
	`switch (config) # show stats chd memory_day`
	`CHD "memory_day" (Average physical memory usage: bytes):`
	`Source dataset: sample "memory"`
	`Computation basis: time`
	`Interval: 120 second(s)`
	`Range: 1800 second(s)`
	`switch (config) #`

Related Commands	show stats chd
Notes	

stats sample <sample-id> clear

stats sample <sample ID> clear

Clears sample history.

Syntax Description	sample ID	Possible sample IDs are: • congested • cpu_util - CPU utilization: milliseconds of time spent • disk_device_io - Storage device I/O statistics • disk_io - Operating system aggregate disk I/O: KB/sec • eth • eth-abs • eth_ip • fan - Fan speed • fs_mnt_bytes - Filesystem usage: bytes • fs_mnt_inodes - Filesystem usage: inodes • ib • interface - Network interface statistics • intf_util - Network interface utilization: bytes • memory - System memory utilization: bytes • paging - Paging activity: page faults • power - Power supply usage • power-consumption • temperature - Modules temperature
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # stats sample temperature clear` `switch (config) #`	
Related Commands	show stats sample	
Notes		

stats sample <sample-id> enable

stats sample <sample-id> enable
no states sample <sample-id> enable

Enables the sample.
The no form of the command disables the sample.

Syntax Description	sample-id	Possible sample IDs are: • congested • cpu_util - CPU utilization: milliseconds of time spent • disk_device_io - Storage device I/O statistics • disk_io - Operating system aggregate disk I/O: KB/sec • eth • fan - Fan speed • fs_mnt_bytes - Filesystem usage: bytes • fs_mnt_inodes - Filesystem usage: inodes • ib • interface - Network interface statistics • intf_util - Network interface utilization: bytes • memory - System memory utilization: bytes • paging - Paging activity: page faults • power - Power supply usage • power-consumption • temperature - Modules temperature
Default	Enabled	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # stats sample temperature enable` `switch (config) #`	
Related Commands	show stats sample	
Notes		

stats sample <sample-id> interval

stats sample <sample ID> interval <number of seconds>

Sets the amount of time between samples for the specified group of sample data.

Syntax Description	sample ID	Possible sample IDs are: • congested • cpu_util - CPU utilization: milliseconds of time spent • disk_device_io - Storage device I/O statistics • disk_io - Operating system aggregate disk I/O: KB/sec • eth • fan - Fan speed • fs_mnt_bytes - Filesystem usage: bytes • fs_mnt_inodes - Filesystem usage: inodes • ib • interface - Network interface statistics • intf_util - Network interface utilization: bytes • memory - System memory utilization: bytes • paging - Paging activity: page faults • power - Power supply usage • power-consumption • temperature - Modules temperature
	number of seconds	Interval in seconds.
Default	Different per sample	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # stats sample temperature interval 1`
	`switch (config) # show stats sample temperature`
	`Sample "temperature" (Modules temperature):`
	`  Enabled:  yes`
	`  Sampling interval: 1 second`
	`switch (config) #`	

Related Commands	show stats sample	
Notes		

stats clear-all

	stats clear all Clears data for all samples, CHDs, and status for all alarms.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # stats clear-all` `switch (config) #`
Related Commands	N/A
Notes	

stats export

stats export <format> <report name> [{after | before} <yyyy/mm/dd> <hh:mm:ss>] [filename <filename>]

Exports statistics to a file.

Syntax Description	format	Currently the only supported value for <format> is "csv" (comma-separated value).
	report name	Determines dataset to be exported. Possible report names are: • memory - Memory utilization • paging - Paging I/O • cpu_util - CPU utilization
	after | before	Only includes stats collected after or before a specific time.
	yyyy/mm/dd	Date: It must be between 1970/01/01 and 2038/01/19.
	hh:mm:ss	Time: It must be between 00:00:00 and 03:14:07 UTC and is treated as local time.
	filename	Specifies filename to give new report. If a filename is specified, the stats will be exported to a file of that name; otherwise a name will be chosen automatically and will contain the name of the report and the time and date of the export. Any automatically-chosen name will be given a .csv extension.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # stats export csv memory filename mellanoxexample before 2000/08/14 15:59:50 after 2000/08/14 15:01:50`
	`Generated report file: mellanoxexample.csv`
	`switch (config) # show files stats`
	`mellanoxexample.csv`
	`switch (config) #`	

Related Commands	show files stats	
Notes		

show stats alarm

show stats alarm [<Alarm ID> [rate-limit]]

Displays status of all alarms or the specified alarm.

Syntax Description	Alarm ID	May be: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
	rate-limit	Displays rate limit parameters.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show stats alarm`
	`Alarm cpu_util_indiv (Average CPU utilization too high):  ok`
	`Alarm disk_io (Operating System Disk I/O per second too high): (disabled)`
	`Alarm fs_mnt (Free filesystem space too low):  ok`
	`Alarm intf_util (Network utilization too high):  (disabled)`
	`Alarm memory_pct_used (Too much memory in use):  (disabled)`
	`Alarm paging (Paging activity too high):  ok`
	`Alarm temperature (Temperature is too high):  ok`
	`switch (config) #`	

Related Commands	stats alarm	
Notes		

show stats chd

show stats chd [<CHD ID>]

Displays configuration of all statistics CHDs.

Syntax Description	CHD ID	May be: • cpu_util_indiv - Average CPU utilization too high: percent utilization • disk_io - Operating System Disk I/O per second too high: kilobytes per second • fs_mnt - Free filesystem space too low: percent of disk space free • intf_util - Network utilization too high: bytes per second • memory_pct_used - Too much memory in use: percent of physical memory used • paging - Paging activity too high: page faults • temperature - Temperature is too high: degrees
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show stats chd disk_device_io_hour`
	
	`CHD "disk_device_io_hour" (Storage device I/O read/write statistics for the last`
	`hour: bytes):`
	`Enabled: yes`
	`Source dataset: sample "disk_device_io"`
	`Computation basis: data points`
	`Interval: 1 data point(s)`
	`Range: 1 data point(s)`
	`switch (config) #`	

Related Commands	stats chd	
Notes		

show stats cpu

	show stats cpu Displays some basic stats about CPU utilization: • the current level • the peak over the past hour • the average over the past hour
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show stats cpu`
	
	`CPU 0`
	`  Utilization:                6%`
	`  Peak Utilization Last Hour: 16% at 2012/02/28 08:47:32`
	`  Avg. Utilization Last Hour: 8%`
	`switch (config) #`

Related Commands	N/A
Notes	

show stats sample

show stats sample [<sample ID>]

Displays sampling interval for all samples, or the specified one.

Syntax Description	sample ID	Possible sample IDs are: • congested • cpu_util - CPU utilization: milliseconds of time spent • disk_device_io - Storage device I/O statistics • disk_io - Operating system aggregate disk I/O: KB/sec • eth • fan - Fan speed • fs_mnt_bytes - Filesystem usage: bytes • fs_mnt_inodes - Filesystem usage: inodes • ib • interface - Network interface statistics • intf_util - Network interface utilization: bytes • memory - System memory utilization: bytes • paging - Paging activity: page faults • power - Power supply usage • power-consumption • temperature - Modules temperature
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show stats sample fan`
	`Sample "fan" (Fan speed):`
	`  Enabled:  yes`
	`  Sampling interval: 1 minute 11 seconds`
	`switch (config) #`	

Related Commands	N/A	
Notes		

4.16 Chassis Management

The chassis manager provides the user access to the following information:

Table 27 - Chassis Manager Information

Accessible Parameters	Description
switch temperatures	Displays system's temperature
power supply voltages	Displays power supplies' voltage levels
fan unit	Displays system fans' status
power unit	Displays system power consumers
Flash memory	Displays information about system memory utilization.

Additionally, it monitors:

- AC power to the PSUs
- DC power out from the PSUs
- Chassis failures

4.16.1 System Health Monitor

The system health monitor scans the system to decide whether or not the system is healthy. When the monitor discovers that one of the system's modules (leaf, spine, fan, or power supply) is in an unhealthy state or returned from an unhealthy state, it notifies the users through the following methods:

- System logs – accessible to the user at any time as they are saved permanently on the system
- Status LEDs – changed by the system health monitor when an error is found in the system and is resolved
- email/SNMP traps – notification on any error found in the system and resolved

4.16.1.1 Re-Notification on Errors

When the system is in an unhealthy state, the system health monitor notifies the user about the current unresolved issue every X seconds. The user can configure the re-notification gap by running the "health notif-cntr <counter>" command.

4.16.1.2 System Health Monitor Alerts Scenarios

- System Health Monitor sends notification alerts in the following cases:

Table 28 - System Health Monitor Alerts Scenarios (Sheet 1 of 2)

Alert Message	Scenario	Notification Indicator	Recovery Action	Recovery Message
<fan_name> speed is below minimal range	A chassis fan speed is below minimal threshold: 15% of maximum speed	Email, fan LED and system status LED set red, log alert, SNMP.	Check the fan and replace it if required	"<fan_name> has been restored to its normal state"
Fan <fan_number> speed in spine number <spine_number> is below minimal range	A spine fan speed is below minimal threshold: 30% of maximum speed	Email, fan LED and system status LED set red, log alert, SNMP	Check the fan and replace it if required	"Fan speed <fan_number> in spine number <spine_number> has been restored to its normal state"
<fan_name> is unresponsive	A chassis fan is not responsive on MLNX-OS systems	Email, fan LED and system status LED set red, log alert, SNMP	Check fan connectivity and replace it if required	"<fan_name> has been restored to its normal state"
Fan <fan_number> in spine number <spine_number> is unresponsive	A spine fan is not responsive on MLNX-OS systems	Email, fan LED and system status LED set red, log alert, SNMP	Check fan connectivity and replace it if required	"Fan <fan_number> in spine number <spine_number> has been restored to its normal state"
<fan_name> is not present	A chassis fan is missing	Email, fan LED and system status LED set red, log alert, SNMP	Insert a fan unit	"<fan_name> has been restored to its normal state"
Fan <fan_number> in spine number <spine_number> is not present.	A spine fan is missing	Email, fan LED and system status LED set red, log alert, SNMP	Insert a fan unit	"Fan <fan_number> in spine number <spine_number> has been restored to its normal state"
Insufficient number of working fans in the system	Insufficient number of working fans in the system	Email, fan LED and system status LED set red, log alert, SNMP	Plug in additional fans or change faulty fans	"The system currently has sufficient number of working fans"
Power Supply <ps_number> voltage is out of range	The power supply voltage is out of range.	Email, power supply LED and system status LED set red, log alert, SNMP	Check the power connection of the PS	"Power Supply <ps_number> voltage is in range"

Table 28 - System Health Monitor Alerts Scenarios (Sheet 2 of 2)

Alert Message	Scenario	Notification Indicator	Recovery Action	Recovery Message
Power supply <ps_number> temperature is too hot	A power supply unit temperature is higher than the maximum threshold of 70 Celsius on MLNX-OS systems	Email, power supply LED and system status LED set red, log alert, SNMP	Check chassis fans connections. On MLNX-OS systems, check system fan connections.	"Power supply <ps_number> temperature is back to normal"
Power Supply <number> is unresponsive	A power supply is malfunctioning or disconnected	Email, system status LED set red, log alert, SNMP	Connect power cable or replace malfunctioning PS	"Power supply has been removed" or "PS has been restored to its normal state"
Unit/leaf/spine <leaf/spine number> is unresponsive	A leaf/spine is not responsive	Email, system status LED set red, log alert, SNMP	Check leaf/spine connectivity and replace it if required	"Leaf/spine number <leaf/spine number> has been restored to its normal state"
Unit/leaf/spine voltage is out of range	One of the voltages in a MLNX-OS unit is below minimal threshold or higher than the maximum threshold - both thresholds are 15% of the expected voltage	Email, system status LED set red, log alert, SNMP	Check leaf connectivity	"Unit voltage is in range"
ASIC temperature is too hot	A ASIC unit temperature is higher than the maximum threshold of 105 Celsius on MLNX-OS systems.	Email, system status LED set red, log alert, SNMP	Check the fans system	"ASIC temperature is back to normal"

4.16.2 Power Management

4.16.2.1 Power Supply Options

MLNX-OS offers power redundancy configurations and monitoring for director switch systems. Director switch systems have the following redundancy configuration modes:

- "combined" – no power supply is reserved, the redundancy is not enabled.
- "ps-redundant" – one power supply unit is redundant to the rest. The system can work with one less power supply unit.
- "grid-redundant" – the power supplies are split into two logical power supply grids, first half of the PSUs belongs to grid A and the second half to grid B. The systems can work with only one grid. When using grid-redundancy mode the power budget is calculated according to the minimum power budget between the grids. This mode is available on CS75xx chassis systems. During switch initialization, or hot-plugging of switch compo-

nents, MLNX-OS enables and/or disables switch components according to the available power budget.

MLNX-OS may send power alarms (via SNMP or email) as follow:

- If the available budget is insufficient for all the system components an `insufficient-Power` event is generated. In this mode several switch components may be disabled.
- If the total power of the system is insufficient for redundancy, a `lowPower` event is generated.
- If a connected power supply provides below 1.6K Watts or grid-redundancy mode is configured and a power supply is connected to a 110V grid, then a `powerRedundancy-Mismatch` event is generated, where grid redundancy can not be achieved in such configuration.

In case of an insufficient-power mode, the order in which the FRUs are turned ON is first spines (1,2,3...max) and then the leafs (1,2,3...max), while the order of the FRUs in case of turning them OFF is first the spines (max...3) and then the leafs (max...1). The management modules are not affected.

For the trap OID, please refer to the Mellanox-MIB file.

Power cycle is needed after changing power redundancy mode on a director switch system.

4.16.2.2 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 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 459.

Table 29 - 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

4.16.2.3 Managing Chassis Power

It is possible to shut down or power up modules in a chassis by using the commands "`power enable`" and "`no power enable`".

Step 1. Change to Config mode. Run:

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

Step 2. Run the command "`show power`" to get a list of modules that are available to power up or down.

Step 3. To power down a module run the command "`no power enable`" followed by a module.

```
switch (config) # no power enable ps1
```

Step 4. To power up a module run the command "`power enable`" followed by a module.

```
switch (config) # power enable ps1
```

Using the `show power` command it is possible to see the power consumption of the system and also the power consumption by power supply unit.

4.16.3 Monitoring Environmental Conditions

Step 1. Display module's temperature. Run:

```
switch (config) # show temperature
-------------------------------------------------------
Module      Component              Reg  CurTemp    Status
                                        (Celsius)
-------------------------------------------------------
MGMT        SIB                    T1   33.00      OK
MGMT        Board AMB temp         T1   24.50      OK
MGMT        Ports AMB temp         T1   27.00      OK
MGMT        CPU package Sensor     T1   29.00      OK
MGMT        CPU Core Sensor        T1   28.00      OK
MGMT        CPU Core Sensor        T2   24.00      OK
PS1         power-mon              T1   22.00      OK
PS2         power-mon              T1   23.00      OK
```

Step 2. Display measured voltage levels of power supplies. Run:

```
switch (config) # show voltage
-------------------------------------------------------------------------------------------
Module   Power Meter          Reg              Expected  Actual   Status  High   Low
                                                Voltage   Voltage          Range  Range
-------------------------------------------------------------------------------------------
MGMT     acdc-monitor1        DDR3 0.675V      0.68      0.67     OK      0.78   0.57
MGMT     acdc-monitor1        CPU 0.9V         0.90      0.86     OK      1.03   0.77
MGMT     acdc-monitor1        SYS 3.3V         3.30      3.36     OK      3.79   2.80
MGMT     acdc-monitor1        CPU 1.8V         1.80      1.82     OK      2.07   1.53
MGMT     acdc-monitor1        CPU/PCH 1.05V    1.05      1.06     OK      1.21   0.89
MGMT     acdc-monitor1        CPU 1.05V        1.05      1.06     OK      1.21   0.89
MGMT     acdc-monitor1        DDR3 1.35V       1.35      1.35     OK      1.55   1.15
MGMT     acdc-monitor1        USB 5V           5.00      5.04     OK      5.75   4.25
MGMT     acdc-monitor1        1.05V LAN        1.50      1.51     OK      1.72   1.27
MGMT     ASICVoltMonitor1     Asic 1.2V        1.20      1.21     OK      1.38   1.02
MGMT     ASICVoltMonitor1     Asic 3.3V        3.30      3.31     OK      3.79   2.80
MGMT     ASICVoltMonitor2     Vcore SX         0.95      0.96     OK      1.09   0.81
MGMT     ASICVoltMonitor2     Asic 1.8V        1.80      1.81     OK      2.07   1.53
MGMT     acdc-monitor2        3.3V Switch IB   3.30      3.36     OK      3.79   2.80
PS1      power-mon            vout 12V         12.00     12.07    OK      13.80  10.20
```

Step 3. Display the fan speed and status. Run:

```
switch (config) # show fan
-------------------------------------------------
Module          Device          Fan  Speed     Status
                                     (RPM)
-------------------------------------------------
FAN1            FAN             F1   6297.00   OK
FAN1            FAN             F2   5421.00   OK
FAN2            FAN             F1   6355.00   OK
FAN2            FAN             F2   5378.00   OK
FAN3            FAN             F1   6183.00   OK
FAN3            FAN             F2   5421.00   OK
FAN4            FAN             F1   6268.00   OK
FAN4            FAN             F2   5399.00   OK
PS1             FAN             F1   10336.00  OK
PS2             FAN             -    -         NOT PRESENT
```

Step 4. Display the voltage current and status of each module in the system. Run:

```
switch (config) # show power consumers
-------------------------------------------------------------------
Module  Device           Sensor  Power   Voltage  Current  Status
                                 [Watts] [Volts]  [Amp]
-------------------------------------------------------------------
PS1     power-mon        input   39.94   12.07    3.31     OK
MGMT    acdc-monitor1    input   2.11    12.00    0.18     OK

Total power used : 42.05 Watts
```

4.16.4 USB Access

MLNX-OS can access USB devices attached to switch systems. USB devices are automatically recognized and mounted upon insertion. To access a USB device for reading or writing a file, you need to provide the path to the file on the mounted USB device in the following format:

```
scp://username:password@hostname/var/mnt/usb1/<file name>
```

While username and password are the admin username and password and hostname is the IP of the switch.

Examples:

- ***To fetch an image from a USB device, run the command:***

```
switch (config) # “image fetch scp://admin:admin@127.0.0.1/var/mnt/usb1/image.img
```

- ***To save log file ‘my-logfile’ to a USB device under the name*** `test_logfile` ***using the*** `logging files` ***command, run (in Enable or Config mode):***

```
switch (config) # logging files upload my-logfile scp://username:password@hostname/var/
mnt/usb1/test_logfile
```

- ***To safely remove the USB and to flush the cache, after writing (log files, for example) to a USB, use the*** `usb eject` ***command (in Enable or Config mode).***

```
switch (config) # usb eject
```

4.16.5 Unit Identification LED

The unit identification (UID) LED is a hardware feature used as a means of locating a specific switch system in a server room.

- ***To activate the UID LED on a switch system, run:***

```
switch (config) # led MGMT uid on
```

- ***To verify the LED status, run:***

```
switch (config) # show leds
Module   LED           Status
------------------------------------------------------------------------
MGMT     STATUS        Green
MGMT     FAN1          Green
MGMT     FAN2          Green
MGMT     FAN3          Green
MGMT     FAN4          Green
MGMT     PS_STATUS     Green
MGMT     PS1           Green
MGMT     PS2           Green
MGMT     UID           Blue
```

- ***To deactivate the UID LED on a switch system, run:***

```
switch (config) # led MGMT uid off
```

4.16.6 High Availability (HA)

Mellanox high end management director switch systems support redundant management modules. Chassis HA reduces downtime as it assures continuity of the work even when a management module dies. Chassis HA management allows the systems administrator to associate a single IP address with the appliance. Connecting to that IP address allows the user to change and review the system’s chassis parameters regardless of the active management module.

4.16.6.1 Chassis High Availability Nodes Roles

Every node in the Chassis HA has one of the following roles/modes:

- Master – the node that manages chassis configurations and services the chassis IP addresses
- Slave – the node that replaces the Master node and takes over its responsibilities once the Master node is down.

The master node is the only node that has access to chassis components such as temperature, inventory and firmware.

The CPU role of the current management node can be recognized by the following methods:

- Run the `show chassis ha` command.

```
switch (config) # show chassis ha
2-node HA state:
  Box management IP: 172.30.1.200/16
          interface: mgmt0

       local role: master
       local slot: 1
      other state: ready
      reset count: 0

switch (config) #
```

- Check the LEDs in the management modules as displayed in the figure below.
- Go to the WebUI => System => Modules page and see the information on the LEDs.

4.16.6.2 Malfunctioned CPU Behavior

When a CPU in not responding to an internal communication with the other CPU, the non responding CPU will be reset by the other CPU. Each time a CPU resets, a counter is incremented. After 5 resets a CPU is considered malfunctioned and will be shut down.

To verify how many times a CPU is reset, run the following command:

```
switch [default: master] (config) # show chassis ha
2-node HA state:
  Box management IP: 172.30.1.200/16
          interface: mgmt0

       local role: master
       local slot: 1
      other state: ready
      reset count: 1

switch-11a14e [default: master] (config) #
```

To verify if a CPU has been shut down, either run the following command:

```
switch [default: master] (config) # show chassis ha
2-node HA state:
  Box management IP: 172.30.1.200/16
          interface: mgmt0

       local role: master
       local slot: 1
      other state: powered-off
      reset count: 5

switch-11a14e [default: master] (config) #
```

Or check the system page in the WebUI, the management figure will be grayed out.

To enable the malfunctioned CPU, first replace it and run `chassis ha reset other`.

4.16.6.3 Box IP Centralized Location

Box IP (BIP) centralized management infrastructure enables you to configure and monitor the system. The BIP continues to function even if one of the management blades dies. Box IP is defined by running the chassis ha bip <board IP address> command. The created BIP is used as the master IP's alias.

Example:

```
switch [standalone: master] (config) # chassis ha bip 192.168.10.100 255.255.255.0
switch [standalone: master] (config) #
```

4.16.6.4 System Configuration

System configuration changes should be performed by the master using the BIP otherwise they are overridden by the master configuration.

Chassis HA is based on database replication enabling the entire master configuration to be replicated to the slave. Data such as chassis configuration is replicated. However, run time information such as time, logs, active user lists, is not copied. Additionally, node specific configuration information such as host name and IP address is not copied..

Chassis HA requires connectivity of both management modules (mgmt0, mgmt1) in the same broadcast domain.

4.16.6.5 Takeover Functionally

Management CPU functional takeover takes up to 20-30 seconds. However, when plugging in a module, you need to wait for approximately 3 minutes before making any other hardware change. During the takeover process, the Master LED status is differentiated by a color scheme. To verify the system's status, run the "show chassis ha" command on both managements.

In case of CPU malfunction the system tries to reset it 5 times to solve the issue. If the CPU is not activated after resetting, the system powers it off as well as its attached spine. Once the CPU is

powered off, the user should replace the malfunctioned CPU module. To power on the CPU and the attached spine, plug the module in, log into the Master CPU and run the “chassis ha power enable other” command.

Although the LEDs are functional during the takeover, wait for approximately 3 minutes before making any other hardware change.

Master example:

```
switch [default: master] (config) # show chassis ha
2-node HA state:
  Box management IP: 172.30.1.200/16
          interface: mgmt0

      local role: master
      local slot: 1
     other state: ready
     reset count: 1

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

Slave example:

```
switch [default: master] (config) # show chassis ha
2-node HA state:
  Box management IP: 172.30.1.200/16
          interface: mgmt0

      local role: slave
      local slot: 2
     other state: ready
     reset count: 0

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

Not following these instructions may result in some errors in the log. These errors may be safely ignored.

4.16.7 System Reboot

4.16.7.1 Rebooting 1U Switches

➢ ***To reboot a 1U switch system:***

Step 1. Enter Enable or Config mode. Run:

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

Step 2. Reboot the system. Run:

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

4.16.7.2 Rebooting Director Switches

Mellanox high end management director switch systems support redundant management modules. Chassis HA reduces downtime as it assures continuity of the work even when a management module dies. Chassis HA management allows the systems administrator to associate a single IP address with the appliance. Connecting to that IP address allows the user to change and review the system's chassis parameters regardless of the active management module.

➢ ***To reboot director switches:***

Step 1. Connect to BIP. Please refer to Section 4.16.6.3, "Box IP Centralized Location," on page 452 for more information.

Step 2. Enter Config mode. Run:

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

Step 3. Reboot the slave management. Run:

```
switch [default: master] (config) # chassis ha reset other
switch [default: master] (config) #
```

Step 4. Reboot the master management. Run:

```
switch [default: master] (config) # reload
```

4.16.8 Commands

4.16.8.1 Chassis Management

clear counters

clear counters [all | interface <type> <number>] [ethernet | port-channel]

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	
History	3.2.3000	
	3.6.4000	Added note
Role	admin	
Example	`switch (config) # clear counters`	
Related Commands		
Notes	The command also clears storm-control counters.	

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. Range: 10-2048.
	re-notif-cntr <counter>	Health control changes notification counter, in seconds. Range: 120-7200 seconds.
	report-clear	Clears the health report.
Default	max-report-len: 50 re-notif-cntr:	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # health re-notif-cntr 125` `switch (config) #`	
Related Commands	show health-report	
Notes		

led uid

led <module> uid <on | off>

Configures the UID LED.

Syntax Description	module	Specifies the module whose UID LED to configure
	on	Turns on UID LED
	off	Turns off UID LED
Default	N/A	
Configuration Mode	config	
History	3.6.1002	
	3.6.2002	Added director switch support
Role	admin	
Example	`switch (config) # led MGMT uid on` `switch (config) #`	
Related Commands	N/A	
Notes	• On 1U switch systems, the module parameter can only be MGMT • On director switch systems, the module parameter may be MGMT#, L#, S# (e.g. MGMT1, L01, S01)	

power enable

power enable <module name>
no power enable <module name>

Powers on the module.
The no form of the command shuts down the module.

Syntax Description	module name Enables power for selected module.
Default	Power is enabled on all modules.
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # power enable L01` `switch (config) #`
Related Commands	show power show power consumers
Notes	• This command is not applicable on 1U systems • It is recommended to run this command prior to extracting a module from the switch system, else errors are printed in the log

power-management width

power-management width {auto | force}
no power-management width

Sets the width of the interface to be automatically adjusted.
The no form of the command disables power-saving.

Syntax Description	auto	Allows the system to automatically decide whether to work in power-saving mode or not.
	force	Forces power-saving mode on the port.
Default	Disabled	
Configuration Mode	config interface ib	
History	3.3.4000	
Role	admin	
Example	`switch (config interface ib 1/1) # power-management width auto`	
Related Commands	show interface	
Notes		

power redundancy-mode

power redundancy-mode [combined | grid-redundant | ps-redundant]

Controls the power supply redundancy mode.

Syntax Description	combined	No redundancy - no alarm threshold.
	grid-redundant	N+N – the alarm threshold will be set to a level, indicating when the power availability falls below power that can support N+N scheme
	ps-redundant	N+1 – the alarm threshold will be set to a level, indicating when the power availability falls below power that can support N+1 scheme
Default	N/A	
Configuration Mode	config	
History	3.1.0000, 3.2.0000	
Role	admin	
Example	`switch (config) # power redundancy-mode combined` `switch (config) #`	
Related Commands	N/A	
Notes	• The difference between the modes sets the threshold for power supply redundancy failure. It does not change any power supply configuration. • This command is not applicable for 1U or blade systems.	

system profile

system profile {ib-single-switch | ib-no-adaptive-routing-single-switch | ib [split-ready] [num-of-swids <swid-num>] [no-adaptive-routing] [ib-router] [adaptive-routing-groups <value>]} [force]

Sets the profile of the system to InfiniBand with various parameters

Syntax Description	ib-single-switch	Enables InfiniBand switch profile All network interfaces link protocol set to InfiniBand
	ib-no-adaptive-routing-single-switch	Enables InfiniBand switch profile without adaptive routing capabilities All network interfaces link protocol set to InfiniBand with disabled adaptive routing
	split-ready	Enables the system to reboot in split enable mode with capability to configure 2x the number of ports exposed to IB utilities. **Note:** This parameter is available only on Quantum-based systems.
	ib-router	Enables IB Routing capability on the system
	num-of-swids	Enables IB Router Multiple switch IDs are configurable • adaptive routing – enables adaptive routing • ib-router – enables IB router **Note:** If num-of-swids is not defined then it is set to 1 by default.
	adaptive-routing-groups	Sets adaptive routing groups. Range: 128-4096 (must be multiples of 128) **Note:** Allowed only when adaptive routing is enabled.
Default	The default system profile depends on the system: SB7780 system has “IB Router” and 2 SWIDs as default	
Configuration Mode	config	
History	3.1.0000	
	3.2.1100	Added “vpi-single-switch” option
	3.6.1002	Added system profile “ib num-of-swids”
	3.6.6162	Added system profile “num of adaptive routing”
	3.7.0020	Added system profile “ib split-ready”
Role	admin	
Example	`switch (config) # system profileib-single-switch` `switch (config) #`	

Related Commands	port type show system profile show ports type
Notes	• This command requires a license. Refer to “Licenses” section in the *MLNX-OS SwitchX User Manual* • This command requires approval because reboot is performed and all configuration is removed • This command deletes all switch configuration (keeping IP connectivity) and resets the system • System profile “ib-no-adaptive-routing-single-switch profile” is the default profile for InfiniBand switches • The parameter “adaptive-routing-groups” is only available when “adaptive-routing” is configured • Refer to the ‘port type’ command in order to change the link protocol • System profile “ib split-ready” must run together with num-of-swids <count> • IB router and adaptive routing are enabled only if specified but cannot be enabled at the same time • IB router only works when adaptive routing is disabled.

usb eject

	usb eject Gracefully turns off the USB interface.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # usb eject` `switch (config) #`
Related Commands	N/A
Notes	Applicable only for systems with USB interface.

show asic-version

	show asic-version Displays firmware ASIC version.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.4.2008 Updated Example 3.4.3050 Updated Example 3.6.1002 Updated Example
Role	admin

Example	`switch (config) # show asic-version`
	`==================================================`
	`Module Device Version`
	`==================================================`
	`L05 SIB2-1 15.0200.0092`
	`L05 SIB2-2 15.0200.0092`

Related Commands	N/A
Notes	

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	`switch (config) # show bios`
	`BIOS version : 4.6.5`
	`BIOS subversion : Official AMI Release`
	`BIOS release date : 07/02/2013`
	`switch (config) #`

Related Commands	
Notes	

show cpld

	show cpld Displays status of all CPLDs in the system.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.3.4302 Updated example
Role	admin

Example	`switch (config) # show cpld`
	`==================================`
	`Name Type Version`
	`==================================`
	`Cpld1 CPLD_TOR 4`
	`Cpld2 CPLD_PORT1 2`
	`Cpld3 CPLD_PORT2 2`
	`Cpld4 CPLD_MEZZ 3`
	`switch (config) #`

Related Commands	N/A
Notes	

show fan

	show fan Displays fans status.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

Example	`switch (config) # show fan`
	`switch (config) # show fan`
	`==================================================`
	`Module  Device  Fan  Speed  Status`
	`(RPM)`
	`==================================================`
	`FAN  FAN  F1  5340.00  OK`
	`FAN  FAN  F2  5340.00  OK`
	`FAN  FAN  F3  5640.00  OK`
	`FAN  FAN  F4  5640.00  OK`
	`PS1  FAN  F1  5730.00  OK`
	`PS2  FAN  -  -  NOT PRESENT`
	`switch (config) #`

Related Commands	N/A
Notes	

show health-report

	show health-report Displays health report.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.3.0000 Output update
Role	admin

Example	`switch (config) # show health-report`
	`=======================`
	`| ALERTS CONFIGURATION |`
	`=======================`
	`Re-notification counter (sec):[3600]`
	`Report max counter: [50]`
	`=======================`
	`| HEALTH REPORT |`
	`=======================`
	`No Health issues file`
	`switch (config) #`

Related Commands	N/A
Notes	

show inventory

	show inventory Displays system inventory.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.4.1604 Removed CPU module output from Example 3.5.1000 Removed Type column from Example 3.6.1002 Updated Example
Role	admin

Example	`switch (config) # show inventory`
	`----------------------------------------------------------------------`
	`Module Part Number Serial Number Asic Rev. HW Rev.`
	`----------------------------------------------------------------------`
	`CHASSIS MSB7800-ES2F MT1602X17464 N/A A1`
	`MGMT MSB7800-ES2F MT1602X17464 0 A1`
	`FAN1 MTEF-FANF-A MT1602X16943 N/A A3`
	`FAN2 MTEF-FANF-A MT1602X16944 N/A A3`
	`FAN3 MTEF-FANF-A MT1602X16956 N/A A3`
	`FAN4 MTEF-FANF-A MT1602X16957 N/A A3`
	`PS1 MTEF-PSF-AC-A MT1601X09908 N/A A3`

Related Commands	N/A
Notes	

show leds

show leds [<module>]

Displays the LED status of the switch system.

Syntax Description	module	Specifies the module whose LED status to display
Default	N/A	
Configuration Mode	config	
History	3.6.1002	
	3.6.2002	Updated Example
Role	admin	
Example		

```
switch (config) # show leds
Module       LED                       Status
-------------------------------------------
MGMT1        STATUS                    Green
MGMT1        REAR_FAN                  Green
MGMT1        PS                        Green
MGMT1        FRONT_FAN                 Green
MGMT1        MASTER/SLAVE              Green
L01          STATUS                    Green
L01          UID                       Blue
L02          STATUS                    Green
L02          UID                       Blue
L03          STATUS                    Green
L03          UID                       Off
L04          STATUS                    Green
L04          UID                       Off
L05          STATUS                    Green
L05          UID                       Off
L06          STATUS                    Green
L06          UID                       Off
S01          STATUS                    Green
S01          FAN                       Green
S02          STATUS                    Green
S02          FAN                       Green
S03          STATUS                    Green
S03          FAN                       Green
FAN1         STATUS                    Green
FAN2         STATUS                    Green
FAN3         STATUS                    Green
FAN4         STATUS                    Green
```

Related Commands	N/A
Notes	

show memory

	show memory Displays memory status.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.7.10xx Example updated
Role	admin

Example	`scorpion-167 [standalone: master] (config) # show memory`
	
	`----------------------------------------------------------------------`
	`Memory Space  Total       Used        Free        Used+B/C    Free-B/C`
	`----------------------------------------------------------------------`
	`Physical      15848 MB    2849 MB     12999 MB    3854 MB     11994 MB`
	`Swap          0 MB        0 MB        0 MB`
	
	`Physical Memory Borrowed for System Buffers and Cache:`
	`  Buffers            : 27 MB`
	`  Cache              : 910 MB`
	`  Total Buffers/Cache: 937 MB`

Related Commands	N/A
Notes	

show module

	show module Displays modules status.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.3.0000 Added “Is Fatal” column 3.4.2008 Updated command output 3.4.3000 Updated command output and added note
Role	admin

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

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

show 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 3.5.1000 Updated Example
Role	admin

Example	`switch (config) # show power`
	`---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------`
	`Module Device Sensor Power Voltage Current Capacity Feed Status`
	`[Watts] [Volts] [Amp] [Watts]`
	`---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------`
	`PS1 power-mon input 32.25 12.11 1.26 800.00 DC OK`
	`PS2 power-mon input 46.56 12.13 2.33 800.00 DC OK`
	`switch (config) #`

Related Commands	N/A
Notes	

show power consumers

	show power consumers Displays power consumption information.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.5.1000 Updated Example
Role	admin

Example	`switch (config) # show power consumers`
	`---------------------------------------------------------------------------`
	`Module  Device           Sensor  Power   Voltage  Current  Status`
	`                                  [Watts] [Volts]  [Amp]`
	`---------------------------------------------------------------------------`
	`MGMT    CURR_MONITOR     12V     52.96   11.71    4.52     OK`
	
	`Total power used : 52.96 Watts`
	`switch (config) #`

Related Commands	N/A
Notes	

show protocols

	show protocols Displays all protocols enabled in the system.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.2.3000 3.3.4550 Updated Example 3.6.1002 Updated Example
Role	admin

Example	`switch (config) # show protocols`
	
	`Infiniband enabled`
	`sm enabled`
	`router disabled`

Related Commands	N/A
Notes	

show resources

	show resources Displays system resources.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

Example	`switch (config) # show resources`
	`Total      Used      Free`
	`Physical  2027 MB    761 MB   1266 MB`
	`Swap         0 MB      0 MB      0 MB`
	
	`Number of CPUs:    1`
	`CPU load averages: 0.11 / 0.23 / 0.23`
	
	`CPU 1`
	`  Utilization:                5%`
	`  Peak Utilization Last Hour: 19% at 2012/02/15 13:26:19`
	`  Avg. Utilization Last Hour: 7%`
	`switch (config) #`

Related Commands	N/A
Notes	

show system capabilities

	show system capabilities Displays system capabilities.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.3.0000 Added gateway support 3.6.1002 Updated Example 3.7.00xx Updated Example
Role	admin

Example	`switch (config) # show system capabilities`
	`IB: Supported, L2, Adaptive Routing, Split Ready`
	`Max SM nodes: 648`
	`IB Max licensed speed: EDR`

Related Commands	show system profile
Notes	

show system profile

	show system profile Displays system profile.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.2.0000 3.7.00xx Updated Example
Role	admin

Example	`switch (config) # show system profile`
	
	`Profile : ib`
	`Number of SWIDs : 1`
	`Adaptive Routing : yes`
	`Adaptive Routing Groups : 2048`
	`IB Routing : no`

Related Commands	system profile
Notes	

show system profile detailed

	show system profile detailed Displays detailed system profile.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.6000
Role	admin

Example	`switch (config) # show system profile detailed`
	
	`Profile: eth-default`
	
	`----------------------------------------------`
	`Parameter Guaranteed Max Value`
	`----------------------------------------------`
	`FDB size 102400`
	`IPMC-L2 lists 10240`
	`IPMC-L3 lists 10240`
	`IPv4 MC/IGMP routes 10240`
	`IPv4 neighbors 51200`
	`IPv6 neighbors 8192`
	`IPv4 routes 100000`
	`IPv6 shorts 51200`
	`IPv6 routes 21504`
	`VRF 64`
	`RIF 999`

Related Commands	
Notes	

show system type

	show system type Displays system type.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.5.1000
Role	admin
Example	`switch (config) # show system type` `SB7700`
Related Commands	
Notes	

show temperature

	show temperature Displays system temperature sensors status.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

Example	`switch (config) # show temperature`
	`----------`
	`Module  Component  Reg  CurTemp  Status`
	`(Celsius)`
	`----------`
	`MGMT  SIB2  T1  32.00  OK`
	`MGMT  Board AMB temp  T1  23.50  OK`
	`MGMT  Ports AMB temp  T1  27.50  OK`
	`MGMT  CPU package Sensor  T1  27.00  OK`
	`MGMT  CPU Core Sensor  T1  18.00  OK`
	`MGMT  CPU Core Sensor  T2  27.00  OK`
	`PS1  power-mon  T1  22.50  OK`

Related Commands	N/A
Notes	

show version

show version

Displays version information for the currently running system image.

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

Example	`switch (config) # show version`
	`Product name:  MLNX-OS`
	`Product release:  3.6.8008`
	`Build ID:  #1-dev`
	`Build date:  2018-07-18 13:46:44`
	`Target arch:  x86_64`
	`Target hw:  x86_64`
	`Built by:  jenkins@c5de6027485e`
	`Version summary:  X86_64 3.6.8008 2018-07-18 13:46:44 x86_64`
	
	`Product model:  x86`
	`Host ID:  7CFE9058E01E`
	`System UUID:  03000200-0400-0500-0006-000700080009`
	
	`Uptime:  16h 50m 41.260s`
	`CPU load averages:  2.38 / 2.25 / 2.24`
	`Number of CPUs:  2`
	`System memory:  2860 MB used / 12988 MB free / 15848 MB total`
	`Swap:  0 MB used / 0 MB free / 0 MB total`

Related Commands	N/A
Notes	

show version concise

	show version concise Displays concise version information for the currently running system image.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin
Example	`switch (config) # show version concise` `X86_64 3.6.4006 2017-07-03 16:17:39 x86_64`
Related Commands	N/A
Notes	

show voltage

show voltage

Displays voltage level measurements on different sensors.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.3.5006 Updated Example
Role	admin
Example	
Related Commands	N/A
Notes	

```
switch (config) # show voltage
================================================================================================
Module  Power Meter          Reg                 Expected  Actual   Status  High   Low
                                                 Voltage   Voltage          Range  Range
================================================================================================
MGMT    BOARD_MONITOR        USB 5V sensor       5.00      5.15     OK      5.55   4.45
MGMT    BOARD_MONITOR        Asic I/O sensor     2.27      2.11     OK      2.55   1.99
MGMT    BOARD_MONITOR        1.8V sensor         1.80      1.79     OK      2.03   1.57
MGMT    BOARD_MONITOR        SYS 3.3V sensor     3.30      3.28     OK      3.68   2.92
MGMT    BOARD_MONITOR        CPU 0.9V sensor     0.90      0.93     OK      1.04   0.76
MGMT    BOARD_MONITOR        1.2V sensor         1.20      1.19     OK      1.37   1.03
MGMT    CPU_BOARD_MONITOR    12V sensor          12.00     11.67    OK      13.25  10.75
MGMT    CPU_BOARD_MONITOR    12V sensor          2.50      2.46     OK      2.80   2.20
MGMT    CPU_BOARD_MONITOR    2.5V sensor         3.30      3.26     OK      3.68   2.92
MGMT    CPU_BOARD_MONITOR    SYS 3.3V sensor     3.30      3.24     OK      3.68   2.92
MGMT    CPU_BOARD_MONITOR    SYS 3.3V sensor     1.80      1.79     OK      2.03   1.57
MGMT    CPU_BOARD_MONITOR    1.8V sensor         1.20      1.24     OK      1.37   1.03
switch (config) #
```

4.16.8.2 Chassis High Availability

chassis ha bip

chassis ha bip <board IP address>

Configures Chassis Board IP (BIP).

Syntax Description	board IP address	Sets the chassis virtual IP address.
Default	0.0.0.0	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # chassis ha bip 192.168.10.100` `switch (config) #`	
Related Commands	show chassis ha	
Notes	This command is applicable only for director switch systems.	

chassis ha

chassis ha reset other

Performs a reset to the other management card in the chassis.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # chassis ha reset other` `switch (config) #`
Related Commands	show chassis ha
Notes	This command is applicable only for director switch systems.

chassis ha power enable other

	chassis ha power enable other **no chassis ha power enable other** Enables the other management card in the chassis. The no form of the command disables the other management card in the chassis.
Syntax Description	N/A
Default	The other management card is enabled.
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # chassis ha power enable other` `switch (config) #`
Related Commands	show chassis ha
Notes	This command is applicable only for director switch systems.

show chassis ha

	show chassis ha Displays Chassis HA parameters and status.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show chassis ha`
	`2-node HA state:`
	`  Box management IP: 172.30.1.200/16`
	`          interface: mgmt0`
	
	`       local role: master`
	`       local slot: 1`
	`      other state: ready`
	`      reset count: 0`
	`switch (config) #`

Related Commands	chassis ha
Notes	This command is applicable only for director switch systems.

show chassis ha

	show chassis ha Displays Chassis HA parameters and status.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show chassis ha`
	`2-node HA state:`
	`  Box management IP: 172.30.1.200/16`
	`          interface: mgmt0`
	
	`       local role: master`
	`       local slot: 1`
	`      other state: ready`
	`      reset count: 0`
	`switch (config) #`

Related Commands	chassis ha
Notes	This command is applicable only for director switch systems.

4.17 Network Management Interfaces

4.17.1 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

4.17.1.1 Standard MIBs

Table 30 - 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 31 - Standard MIBs – Chassis and Switch

MIB	Standard	Comments
RFC1213-MIB	RFC 1213	
IF-MIB	RFC 2863	ifXTable only supported.
ENTITY-MIB	RFC 4133	
ENTITY-STATE-MIB	RFC 4268	Fan and temperature states
ENTITY-SENSOR-MIB	RFC 3433	• Port module transmit/receiver power sensors (for 1U systems only) • Fan and temperature sensors

4.17.1.2 Private MIB

Table 32 - Private MIBs Supported

MIB	Description
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	Partially 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-POWER-CYCLE	Allows rebooting the switch system
MELLANOX-SW-UPDATE-MIB	Allows viewing what SW images are installed, uploading and installing new SW images
MELLANOX-CONFIG-DB	Allows loading, uploading, or deleting configuration files
MELLANOX-ENTITY-STATE-MIB	Extension to support state change traps Note: Currently supported for power supply insertion and extraction only
MELLANOX-XSTP-MIB	Extension to support STP information
MELLANOX-DCB-TRAPS	Extension traps for ETC and PFC
MELLANOX-QOS	Proprietary QoS MIBs

Mellanox private MIBs can be downloaded from the Mellanox Support webpage.

4.17.1.3 Proprietary Traps

The following private traps are supported by MLNX-OS.

Table 33 - SNMP MELLANOX-EFM-MIB 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.

Table 33 - SNMP MELLANOX-EFM-MIB Traps

Trap	Action Required
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 25, “Supported Event Notifications and MIB Mapping,” on page 298.

Table 34 - SNMP MELLANOX-POWER-CYCLE Traps

Trap	Action Required
mellanoxPowerCyclePlannedReload	N/A

4.17.1.4 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 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
```

4.17.1.5 Resetting SNMPv3 Engine ID

Resetting SNMP engine ID is not supported on director switch systems.

Switch systems shipped with OS versions older than 3.6.6102 have all had the exact same SNMPv3 engine ID. Going forward, however, all switch systems will ship with a system-specific engine ID.

Upgrading the OS version to 3.6.6102 or higher does not automatically change the current engine ID. That can be done through one of the following methods after performing the software upgrade:

- Changing a switch system's profile
- Running "reset factory"
- Using the command "snmp-server engineID reset" (for more details, please see the procedure below)

➢ ***To reset SNMP engine ID using "snmp-server engineID reset":***

Prerequisites:

Step 1. If any of the following SNMP configurations exist, please delete/disable them and re-enable/reconfigure them only after SNMP engine ID reset is performed:

1. Make sure SNMP is disabled. Run:

```
switch (config) # no snmp-server enable
```

2. Make sure no SNMP trap host is configured. Run:

```
switch (config) # no snmp-server host <ip-address>
```

3. Make sure no SNMP users are configured. Run:

```
switch (config) # no snmp-server user <username> v3
```

Procedure:

Step 1. Check existing engine ID:

```
switch (config) # show snmp engineID
Local SNMP engineID: <current_key>
```

Step 2. Reset existing engine ID:

```
switch (config) # snmp-server engineID reset
```

Step 3. Verify new engine ID:

```
switch (config) # show snmp engineID
Local SNMP engineID: <new_key>
```

4.17.1.6 Configuring an SNMPv3 User

➢ ***To configure SNMPv3 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 or sha224 or sha256 or sha384 or sha512
- priv type – des or aes-128 or 3des or aes-192 or aes-256

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
```

4.17.1.7 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
```

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
```

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)
```

Step 4. Configure the desired event to be sent via SNMP. Run:

```
switch (config) # snmp-server notify event interface-up
```

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
```

To print event notifications to the terminal (SSH or CONSOLE) refer to Section 4.6.1, “Monitor,” on page 264.

4.17.1.8 SNMP SET Operations

MLNX-OS allows the user to use SET operations via SNMP interface. This is needed to configure a user/community supporting SET operations.

4.17.1.8.1 Enabling SNMP SET

➢ ***To allow SNMP SET operations using SNMPv1/v2:***

Step 1. Enable SNMP communities. Run:

```
switch (config) # snmp-server enable communities
```

Step 2. Configure a read-write community. Run:

```
switch (config) # snmp-server community my-community-name rw
```

Step 3. Make sure SNMP communities are enabled (they are enabled by default). Make sure “(DISABLED)” does not appear beside “Read-only communities” / “Read-write communities”. Run:

```
switch (config) # show snmp

SNMP enabled   : yes
SNMP port      : 161
System contact :
System location:

Read-only communities:
  public

Read-write communities:
  my-community-name

Interface listen enabled: yes

Listen Interfaces:
  Interface: mgmt0

switch (config) # show snmp
No Listen Interfaces.
```

Step 4. Configure this RW community in your MIB browser.

➢ ***To allow SNMP SET operations using SNMPv3:***

Step 1. Create an SNMPv3 user. Run:

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

It is possible to use other configuration options not specified in the example above. Please refer to the command "snmp-server user" on page 532 for more information.

Step 2. Make sure the username is enabled for SET access and has admin capability level. Run:

```
switch (config) # show snmp user
User name: myuser
   Enabled overall:         yes
   Authentication type:     sha
   Privacy type:            aes-128
   Authentication password: (set)
   Privacy password:        (set)
   Require privacy:         yes
   SET access:
      Enabled:              yes
      Capability level:     admin
```

MLNX-OS supports the OIDs for SET operation listed in Table 35 which are expanded upon in the following subsections.

Table 35 - Supported SET OIDs

MIB Name	OID Name	OID
MELLANOX-EFM-MIB	sendTestTrapSet	1.3.6.1.4.1.33049.2.1.1.1.6.0
SNMPv2-MIB	sysName	1.3.6.1.2.1.1.5.0
MELLANOX-CONFIG-DB	mellanoxConfigDBCmdExecute mellanoxConfigDBCmdFilename mellanoxConfigDBCmdStatus mellanoxConfigDBCmdStatusString mellanoxConfigDBCmdUri	1.3.6.1.4.1.33049.12.1.1.2.3.0 1.3.6.1.4.1.33049.12.1.1.2.2.0 1.3.6.1.4.1.33049.12.1.1.2.4.0 1.3.6.1.4.1.33049.12.1.1.2.5.0 1.3.6.1.4.1.33049.12.1.1.2.1.0
MELLANOX-POWER-CYCLE	mellanoxPowerCycleCmdExecute mellanoxPowerCycleCmdStatus mellanoxPowerCycleCmdStatusString	1.3.6.1.4.1.33049.10.1.1.2.1.0 1.3.6.1.4.1.33049.10.1.1.2.2.0 1.3.6.1.4.1.33049.10.1.1.2.3.0
MELLANOX-SW-UPDATE	mellanoxSWUpdateCmdSetNext mellanoxSWUpdateCmdUri mellanoxSWUpdateCmdExecute mellanoxSWUpdateCmdStatus mellanoxSWUpdateCmdStatusString mellanoxSWActivePartition mellanoxSWNextBootPartition	1.3.6.1.4.1.33049.11.1.1.2.1.0 1.3.6.1.4.1.33049.11.1.1.2.2.0 1.3.6.1.4.1.33049.11.1.1.2.3.0 1.3.6.1.4.1.33049.11.1.1.2.4.0 1.3.6.1.4.1.33049.11.1.1.2.5.0 1.3.6.1.4.1.33049.11.1.1.3.0.0 1.3.6.1.4.1.33049.11.1.1.4.0.0

4.17.1.8.2Sending a Test Trap SET Request

MLNX-OS allows the user to use test the notification mechanism via SNMP SET. Sending a SET request with the designated OID triggers a test trap.

Prerequisites:

1. Enable SET operations by following the instructions in Section 4.17.1.8.1, “Enabling SNMP SET,” on page 496.
2. Configure host to which to send SNMP notifications.
3. Set a trap receiver in the MIB browser.

➢ ***To send a test trap:***

Step 1. Send a SET request to the switch IP with the OID 1.3.6.1.4.1.33049.2.1.1.1.6.0.

Step 2. Make sure the test trap is received by the aforementioned trap receiver (OID: 1.3.6.1.4.1.33049.2.1.2.13).

4.17.1.8.3Setting Hostname with SNMP

Mellanox supports setting system hostname using an SNMP SET request as described in SNMPv2-MIB (sysName, OID: 1.3.6.1.2.1.1.5.0).

The restrictions on setting a hostname via CLI also apply to setting a hostname through SNMP. Refer to the command “hostname” on page 149 for more information.

4.17.1.8.4Power Cycle with SNMP

Mellanox supports power cycling its systems using an SNMP SET request as described in MELLANOX-POWER-CYCLE MIB.

Power cycle command is issued via the OID mellanoxPowerCycleCmdExecute. The following options are available:

- Reload – saves any unsaved configuration and reloads the switch
- Reload discard – reboots the system and discards of any unsaved changes
- Reload force – forces an expedited reload on the system even if it is busy without saving unsaved configuration (equals the CLI command `reload force`)
- Reload slave – reloads the slave management on dual management systems (must be executed from the master management module)

On dual management systems it is advised to connect via the BIP to make sure commands are executed from the master management.

4.17.1.8.5Changing Configuration with SNMP

Mellanox supports making configuration changes on its systems using SNMP SET requests. Configuration requests are performed by setting several values (arguments) and then executing a command by setting the value for the relevant operation.

It is possible to set the parameters and execute the commands on the same SNMP request or separate them to several SET operations. Upon executing a command, the values of its arguments remain and can be read using GET commands.

Once a command is executed there may be two types of errors:

- Immediate: This error results in a failure of the SNMP request. This means a critical error in the SNMP request has occurred or that a previous SET request is being executed
- Delayed: The SET request has been accepted by the switch but an error occurred during its execution.

For example, when performing a fetch (download) operation, an immediate error can occur when the given URL is invalid. A delayed error can occur if the download process fails due to network connectivity issues.

The following parameters are arguments are supported:

- Command URI – URI to fetch the configuration file from or upload the file to (for supported URI format please refer to the CLI command "configuration fetch" for more details)
- Config file name – filename to save the configuration file to or to upload to remote location

The following commands are supported:

- BinarySwitchTo – replaces the configuration file with a new binary configuration file. This option fetches the configuration file from the URI provided in the mellanoxConfigDBCmdUri and switches to that configuration file. This command should be preceded by a reload command in order for the new configuration to apply.
- TextApply – fetches a configuration file in human-readable format and applies its configuration upon the current configuration.
- BinaryUpload – uploads a binary format configuration file of the current running configuration or an existing configuration file on the switch to the URI in the mellanoxConfigDBCmdUri command. The filename parameter indicates what configuration file on the switch to upload.
- TextUpload – uploads a human-readable configuration file of the current running configuration of an existing configuration file on the switch to the URI in the mellanoxConfigDBCmdUri command. The filename parameter indicates what configuration file on the switch to upload (same as the CLI command `configuration text generate file <filename> upload`).
- ConfigWrite – saves active configuration to a filename on the switch as given in the filename parameter. In case filename is "active", active configuration is saved to the current saved configuration (same as the CLI command `configuration write`).
- BinaryDelete – deletes a binary based configuration file
- TextDelete – deletes a text based configuration file

4.17.1.8.6Upgrading MLNX-OS Software with SNMP

Mellanox supports upgrading MLNX-OS software using an SNMP SET request as described in MELLANOX-SW-UPDATE MIB.

The software upgrade command is issued via the OID mellanoxSWUpdateCmdExecute. The following options are available:

- Update – fetches the image from a specified URI (equivalent to the command “image fetch” followed by “image install”)

  The image to update from is defined by the OID mellanoxSWUpdateCmdUri. The restrictions on the URI are identical to what is supported in the CLI command “image fetch” on page 222.

- Set-Next – changes the image for the next boot equivalent to the CLI command “image boot”)

  The partition from which to boot is defined by the OID mellanoxSWUpdateCmdSetNext. The parameters for this OID are as follows:

  - 0 – no change
  - 1 – partition 1
  - 2 – partition 2
  - 3 – next partition (default)

Using the OIDs mellanoxSWUpdateCmdStatus and mellanoxSWUpdateCmdStatusString you may view the status of the latest operation performed from the aforementioned in either integer values, or human-readable forms, respectively. The integer values presented may be as follows:

- 0 – no operation
- 1-100 – progress in percentage
- 101 – success
- 200 – failure

4.17.1.9 IF-MIB and Interface Information

MLNX-OS supports displaying information of switch ports, LAG ports, MLAG ports and VLAN interfaces on all systems via SNMP interface. This feature is enabled by default. The interface information is available in the ifTables, ifXTable and mellanoxIfVPITable. Additionally, traps for interface up/down, and internal link suboptimal speed are enabled. The user has the ability to enable one or both of these traps.

Interface up/down traps are sent whenever there is a change in the interface’s operational state. These traps are suppressed for internal links when the internal link’s speed does not match the configured speed of the link (mismatch condition).

4.17.2 JSON API

JavaScript Object Notation (JSON) is a machine-to-machine data-interchange format which is supported in MLNX-OS CLI.

The JSON API allows executing CLI commands and receiving outputs in JSON format which can be easily parsed by the calling software.

4.17.2.1 Authentication

The JSON API protocol runs over HTTP/HTTPS and uses the existing web authentication mechanism.

In order to access the system via HTTP/HTTPS, an HTTP/HTTPS client is needed to send POST requests to the system.

HTTPS access to the web-based management console needs to be enabled using the command “web https enable” to allow POST requests.

The HTTPS client must first be authenticated by sending a POST request to the following URL:

```
https://<switch-ip-address>/admin/launch?script=rh&template=login&action=login
```

The POST request content should contain the following data:

```
"f_user_id=<user name>&f_password=<user password>"
```

After a successful login, a session id (cookie) is returned to be used for other HTTPS requests in the system.

See Section 4.17.2.6, “JSON Examples,” on page 506 for examples.

4.17.2.2 Sending the Request

After successful authentication, the HTTPS client can start sending JSON requests. All requests (POST and GET) should be sent to the following URL:

```
https://<switch-ip-address>/admin/launch?script=json
```

After the request is handled in the system the HTTPS client receives a JSON response with an indication of the request execution result. If there is data resulting from the request, it is returned as part of the response.

See Section 4.17.2.3, “JSON Request Format,” on page 501 for the CLI request format.

See Section 4.17.2.4, “JSON Response Format,” on page 503 for the reply format.

JSON requests may also be sent using the WebUI. For more information on using the WebUI with JSON, please refer to Section 4.17.2.7, “JSON Request Using WebUI,” on page 511.

4.17.2.3 JSON Request Format

4.17.2.3.1 JSON Execution Requests

JSON execution requests are HTTPS POST requests that contain CLI commands to be executed in the system.

Execution request can contain a single command or multiple commands to be executed.

Single command execution request format:

```
{
     "cmd": "<CLI command to execute>"
}
```

Example:

```
{
     "cmd": "show  1/1"
}
```

Multiple command execution request format:

```
{
     "commands":["<CLI cmd 1>", "<CLI cmd 2>", … , <CLI cmd n>]
}
```

Example:

```
{
     "commands":
     [
          "show  1/1",
          "show  1/2"
     ]
}
```

In case of a multiple command request, the execution of the commands is done in the order they appear in the execution list. Note that the execution of a multiple command request will be stopped upon first failure. That is, in case the execution of one of the commands fails, none of the remaining commands will be executed.

See Section 4.17.2.6, “JSON Examples,” on page 506 for examples.

Execution Types

Execution requests can be either synchronous (default) or asynchronous.

Synchronous requests will wait for a JSON response from the system. The synchronous request has a defined wait time after which the user will receive a timeout response. The timeout for a synchronous request is configurable by the user and is 30 seconds by default (see the CLI command “json-gw synchronous-request-timeout” on page 543).

Asynchronous requests will return immediately after sending the request with a reply containing a “job_id” key. The user can use the given job ID to later query for request status and execution results. Queries for asynchronous request results are guaranteed to be accessible up to 60 seconds after the request has been completed.

To specify the execution type, the user needs to add the following key to the JSON execution request:

```
"execution_type":"<async|sync>"
```

Example:

```
{
     "execution_type":"async",
     "cmd": "show  1/1"
}
```

See Section 4.17.2.6, “JSON Examples,” on page 506 for examples.

4.17.2.3.2JSON Query Requests

JSON Query requests are HTTPS GET requests that contain a job ID parameter. Using a query request, the user can get information on the current execution state of an ongoing request or the execution results of a completed request. To send a query request, the user should add the following parameters to the JSON URL:

```
job_id=<job number>
```

Example:

```
https://<switch-ip-address>/admin/launch?script=json&job_id=<job number>
```

See Section 4.17.2.6, “JSON Examples,” on page 506 for more examples.

4.17.2.4 JSON Response Format

Set commands normally do not return any data or output. If a set command does return an output, it will be displayed in the “status_message” field.

4.17.2.4.1Single Command Response Format

The HTTPS POST response format structure is a JSON object consisting of 4 name-value pairs as follows:

```
{
    "executed_command": "<CLI command that was executed>",
    "status" = "<OK|ERROR>",
    "status_message" = "<information on the status received>",
    "data" = {the information that was asked for in the request}
}
```

- executed_command – the CLI command that was executed in the request
- status – the result of the request execution:
  - “OK” if the execution is successful
  - “ERROR” in case of a problem with the execution

  The value type of this key is “string”.
- data – a JSON object containing the information requested. Returns an empty string if there is no data.
- status message – additional information on the received status. May be empty. The value type of this key is “string”.

Example:

```
{
    “executed_command”: “show  1/1
    "status": "OK",
    "status_message": "",
    "data":
    {
        "speed": "40GbE",
        "admin_state": "up"
    }
}
```

See Section 4.17.2.6, “JSON Examples,” on page 506 for more examples.

4.17.2.4.2Multiple Command Response Format

The HTTPS response format structure is a JSON object consisting of a list of JSON results. Each JSON structure in the list is structured the same as in the single command execution response (see the previous section).

However, the status field can contain in this case an additional value, “ABORTED”, in case a previous command failed. This status value indicates that the command has not been executed at all in the system.

```
{
    "results": [
    {
        "executed_command": "<…>",
        "status": "<OK|ERROR|ABORTED>",
        "status_message": "<…>",
        "data": {…}
     },
     {
        "executed_command": "<…>",
        "status": "<OK|ERROR|ABORTED>",
        "status_message": "<…>",
        "data": {…}
      },
…
      {
        "executed_command": "<…>",
        "status": "<OK|ERROR|ABORTED>",
        "status_message": "<…>",
        "data": {…}
       }
              ]
}
```

Example:

```
{
    "results": [
    {
        "executed_command": "show  1/1",
        "status": "OK",
        "status_message": ""
        "data": {"speed":"40GbE", "admin_state":"up"}
    },
    {
        "executed_command": "show  1/100",
        "status": "ERROR",
        "status_message": "wrong interface name",
        "data": ""
    },
    {
        "executed_command": "show  1/2",
        "status": "ABORTED",
        "status_message": "",
        "data": ""
    }
              ]
}
```

See Section 4.17.2.6, “JSON Examples,” on page 506 for more examples.

4.17.2.4.3Query Response Format

Response to a query request can be of two types. In case the request completes its execution, the response will be similar to the single/multiple command response format, depending on the format of the request, and will display the execution results.

In case the execution is not complete yet, the response format will be similar to the single command response format. However, the status field will contain in this case the value “PENDING” to indicate that the request is still in progress. In addition, the “executed_command” field will contain the current request command being handled by the system.

Example:

```
{
    "executed_command": "show  1/1",
    "status": "PENDING",
    "status_message": "",
    "data":""
}
```

See Section 4.17.2.6, “JSON Examples,” on page 506 for examples.

4.17.2.4.4Asynchronous Response Format

Response to an asynchronous request is similar to the HTTPS response format of the single command response. However, an additional unique field will be added, “job_id”, containing the job id number for querying the request later. The value of the job_id key is of type string.

Another difference is that the “executed_command” field will be empty.

Example:

```
{
    "executed_command": ""
    "status": "OK"
    "status_message": ""
    "data": ""
    "job_id": "2754930426"
}
```

See Section 4.17.2.6, “JSON Examples,” on page 506 for examples.

4.17.2.5 Supported Commands

4.17.2.5.1 Set Commands

All non-interactive CLI set commands are supported.

Interactive commands are commands which require user interaction to complete (e.g., type “yes” to confirm). These commands are not supported by the JSON API.

4.17.2.5.2 Show Commands

Not all CLI show commands are currently supported by the JSON API. Unsupported commands return an error indication.

Support for all show commands will be completed in future MLNX-OS releases.

For a list “show” commands not currently supported, please refer to Appendix B,“Show Commands Not Supported by JSON,” on page 1943.

4.17.2.6 JSON Examples

The following examples use curl (a common tool in Linux systems) to send HTTPS POST requests to the system.

4.17.2.6.1 Authentication Example

Before sending JSON HTTPS request, the user must first authenticate. Run the following from your server’s shell to create a login session ID in the file: /tmp/cookie.

```
curl -c /tmp/cookie -d "f_user_id=admin&f_password=admin"
"https://10.10.10.10/admin/launch?script=rh&template=login&action=login"
```

Upon a successful login, you will receive a reply similar to the following:

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://10.10.10.10/admin/launch?script=rh&amp;tem-
plate=home">here</a>.</p>
<hr>
<address>Apache Server at 10.10.10.10 Port 80</address>
</body></html>
```

The session id can now be used in all other JSON HTTPS requests to the system.

4.17.2.6.2 Synchronous Execution Request Example

Single Command

This example sends a request to query the system profile.

Request (save it to a file named req.json):

```
{"cmd": "show system profile"}
```

Send the request:

```
curl -b /tmp/cookie -X POST -d @req.json "https://10.10.10.10/admin/launch?script=json"
```

Response:

When the system finishes processing the request, the user will receive a response similar to the following:

```
{
    "status": "OK",
    "executed_command": "show system profile",
    "status_message": "",
    "data": {
        "Profile": "ib",
        "Adaptive Routing": "yes",
        "Number of SWIDs": "1"
    }
}
```

Multiple Commands

This example sends a request to change an interface description and then queries for its status.

Request (save it to a file named req.json):

```
{"commands": ["interface ib 1/1 description test description",
"show interfaces ib 1/1 status"]}
```

Send the request:

```
curl -b /tmp/cookie -X POST -d @req.json "https://10.10.10.10/admin/launch?script=json"
```

Response:

When the system finishes processing the request, the user will receive a response similar to the following:

```
{
    "results": [
        {
            "status": "OK",
            "executed_command": "interface ib 1/1 description test description",
            "status_message": "",
            "data": ""
        },
        {
            "status": "OK",
            "executed_command": "show interfaces ib 1/1 status",
            "status_message": "",
            "data": {
                "IB1/1": [
                    {
                        "Description": "test description",
                        "Speed": "fdr",
                        "Logical port state": "Initialize",
                        "Physical port state": "LinkUp",
                        "Current line rate": "56.0 Gbps",
                        "IB Subnet": "infiniband-default"
                    }
                ]
            }
        }
    ]
}
```

4.17.2.6.3Asynchronous Execution Request Example

This example sends an asynchronous request to change an interface description and then queries for its status.

Request (save it to a file named req.json):

```
{"execution_type":"async",
"commands": ["interface ib 1/1 description test description",
"show interfaces ib 1/1 status"]}
```

Send the request:

```
curl -b /tmp/cookie -X POST -d @req.json "https://10.10.10.10/admin/launch?script=json"
```

Response:

The system immediately returns a response similar to the following:

```
{
        "executed_command": "",
        "status": "OK",
        "status_message": "",
        "data": "",
        "job_id": "91329386"
}
```

4.17.2.6.4Query Request Example

This example sends a request to query for a job ID received from a previous execution request.

Request:

The request is a an HTTPS GET operation to the JSON URL with the “job_id” parameter.

Send the request:

```
curl -b /tmp/cookie -X GET "https://10.10.10.10/admin/
launch?script=json&job_id=91329386"
```

Response:

If the system is still processing the request, the user receives a response similar to the following:

```
{
        "executed_command": " interface ib 1/1 description test description ",
        "status": "PENDING",
        "status_message": "",
        "data": ""
}
```

If the system is done processing the request, the user receives a response similar to the following:

```
{
    "results": [
        {
            "status": "OK",
            "executed_command": "interface ib 1/1 description test description",
            "status_message": "",
            "data": ""
        },
        {
            "status": "OK",
            "executed_command": "show interfaces ib 1/1 status",
            "status_message": "",
            "data": {
                "IB1/1": [
                    {
                        "Description": "test description",
                        "Speed": "fdr",
                        "Logical port state": "Initialize",
                        "Physical port state": "LinkUp",
                        "Current line rate": "56.0 Gbps",
                        "IB Subnet": "infiniband-default"
                    }
                ]
            }
        }
    ]
}
```

4.17.2.6.5Error Response Example

General Error

This example sends a request with an illegal JSON structure.

Request - without closing bracket “]” (save it to a file named req.json):

```
{"commands": ["interface ib 1/1 description test description",
"show interfaces ib 1/1 status"}
```

Send the request:

```
curl -b /tmp/cookie -X POST -d @req.json "https://10.10.10.10/admin/launch?script=json"
```

Error response:

```
{
    "status": "ERROR",
    "executed_command": "",
    "status_message": "Handle request failed. Reason:\nIllegal JSON structure found in
given JSON data.\nExpecting , delimiter: line 1 column 95 (char 94)",
    "data": ""
}
```

Multiple Command Request Failure

This example sends a multiple command request where one command fails.

Request - with a non-existing interface (1/200) (save it to a file named req.json):

```
{
        "execution_type": "sync",
        "commands": [   "interface ib 1/1 speed sdr",
                        "interface ib 1/200 speed sdr",
                        "interface ib 1/3 speed sdr"]
}
```

Send the request:

```
curl -b /tmp/cookie -X POST -d @req.json "https://10.10.10.10/admin/launch?script=json"
```

Error response:

```
{
    "results": [
        {
            "status": "OK",
            "executed_command": "interface ib 1/1 speed sdr",
            "status_message": "",
            "data": ""
        },
        {
            "status": "ERROR",
            "executed_command": "interface ib 1/200 speed sdr",
            "status_message": "% 1st Interface does not exist",
            "data": ""
        },
        {
            "status": "ABORTED",
            "executed_command": "interface ib 1/3 speed sdr",
            "status_message": "",
            "data": ""
        }
    ]
}
```

4.17.2.7 JSON Request Using WebUI

The MLNX-OS WebUI also allows users to send JSON HTTPS POST and GET requests.

Log into the WebUI, go to the “Setup” tab, and select “JSON API” from the left side menu.

This section is displayed only if JSON API is enabled using the command “json-gw enable”.

4.17.2.7.1To Execute a JSON Request

Step 1. Choose “Execute JSON command”.

Step 2. Choose the “execution_type” from the drop down list.

Step 3. In the “commands” field, type the CLI command(s) to execute.

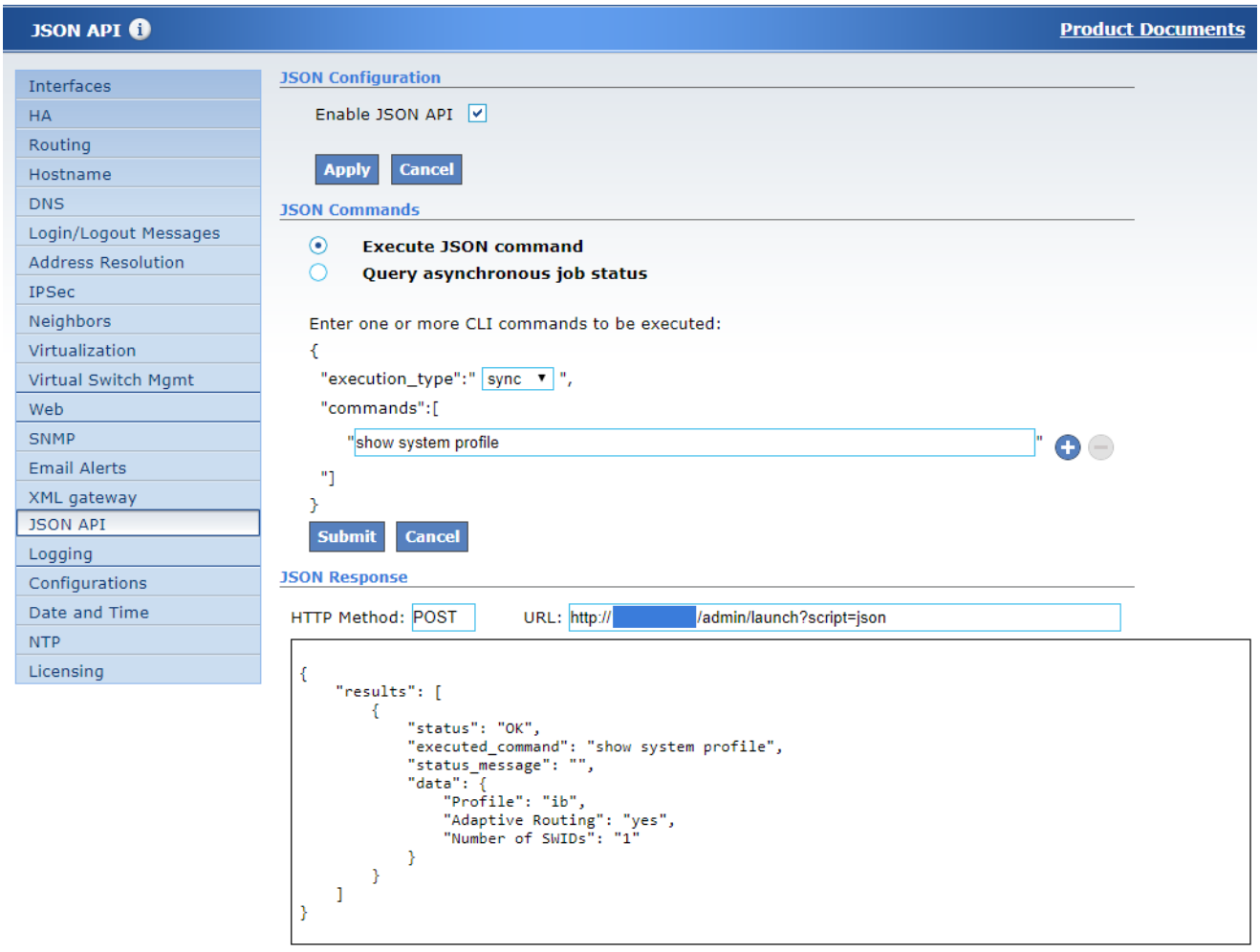
Use the “+” and “-” buttons to add or remove additional commands to the request.

Step 4. Click “Submit”.

The JSON response is then shown in the “JSON Response” box below.

The HTTPS method (HTTPS POST in this instance) and the URL used to send the request will be displayed next to the “HTTPS Method” and “URL” field respectively.

Figure 13: JSON API WebUI Example



4.17.2.7.2To Query an Asynchronous JSON Request

Step 1. Choose “Query asynchronous job status”.

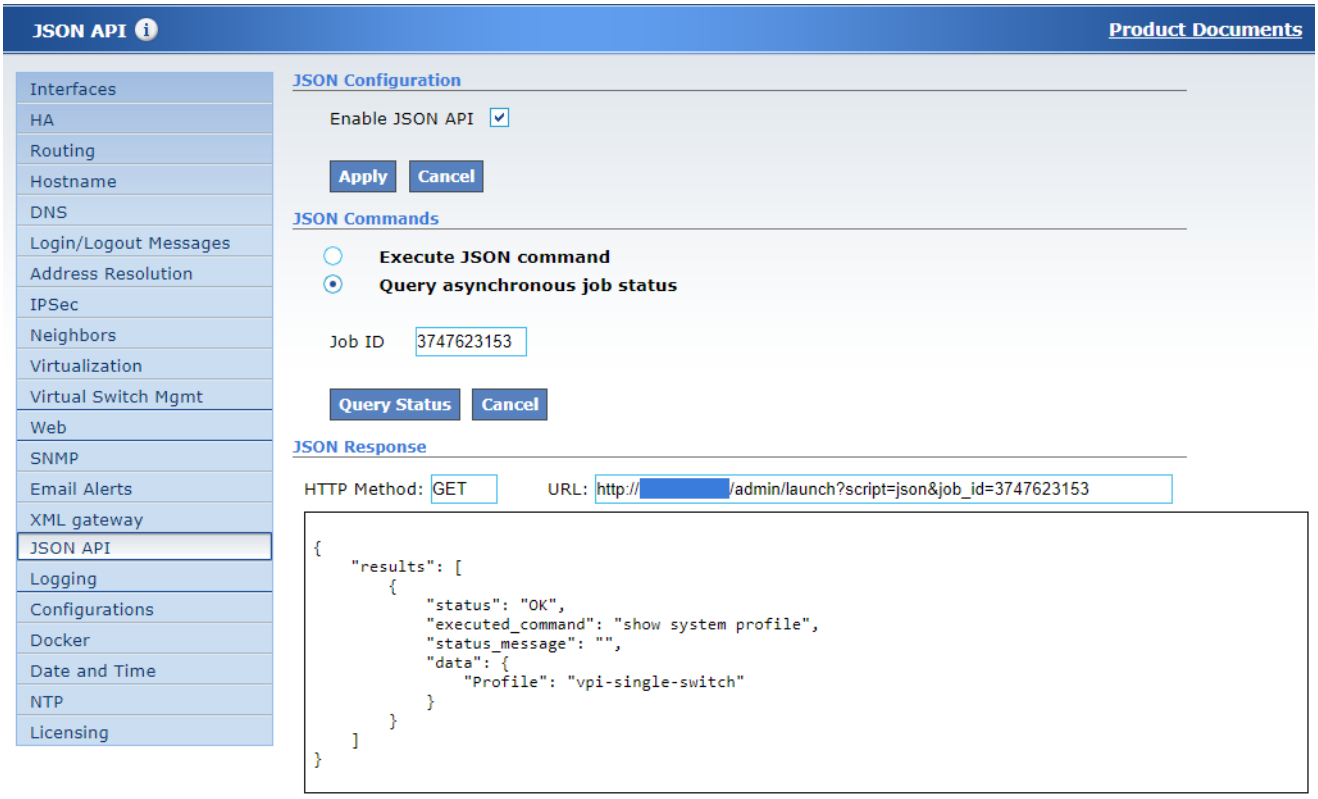
Step 2. Type the job ID in the “Job ID” text box.

Step 3. Press “Query Status”.

The JSON response is then shown in the “JSON Response” box below.

The HTTPS method (HTTPS GET in this instance) and the URL used to send the request will be displayed next to the “HTTPS Method” and “URL” field respectively.

Figure 14: JSON API Asynchronous Job WebUI Example



4.17.3 XML API

MLNX-OS XML API is documented in the *MLNX-OS XML API Reference Guide*.

4.17.4 Commands

4.17.4.1 SNMP Commands

The commands in this section are used to manage the SNMP server.

snmp-server auto-refresh

snmp-server auto-refresh {enable | interval <time>}
no snmp-server auto-refresh enable

Configures SNMPD refresh settings.
The no form of the command disables SNMPD refresh mechanism.

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

snmp-server cache enable

	[no] snmp-server cache enable Enables/disables snmp cache in case auto-refresh is disabled.
Syntax Description	If snmp cache is disabled, every snmp request will get updated data.
Default	Enabled
Configuration Mode	Configure terminal
History	3.7.00xx
Role	admin
Example	`scorpion2-75 [standalone: master] (config) # snmp-server cache enable`
Related Commands	show snmp auto-refresh [no] snmp-server auto-refresh enable
Notes	If snmp auto-refresh is enabled, the value of cache is meaningless

snmp-server community

snmp-server community <community> [ro | rw]
no snmp-server community <community>

Sets a community name for either read-only or read-write SNMP requests. The no form of the command sets the community string to default.

Syntax Description	community	Community name.
	ro	Sets the read-only community string.
	rw	Sets the read-write community string.
Default	Read-only community: “public” Read-write community: “”	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch(config) # snmp-server community private rw`
	`switch (config) # show snmp`
	`SNMP enabled: yes`
	`SNMP port: 161`
	`System contact:`
	`System location:`
	`Read-only community: public`
	`Read-write community: private`
	
	`Interface listen enabled: yes`
	`No Listen Interfaces.`
	
	`Traps enabled: yes`
	`Default trap community: public`
	`Default trap port: 162`
	
	`No trap sinks configured.`
	`switch(config) #`	

Related Commands	show snmp	
Notes	• If neither the “ro” or the “rw” parameters are specified, the read-only community is set as the default community • If the read-only community is specified, only queries can be performed • If the read-write community is specified, both queries and sets can be performed	

snmp-server contact

snmp-server contact <contact name>
no snmp-server contact

Sets a value for the sysContact variable in MIB-II.
The no form of the command resets the parameter to its default value.

Syntax Description	contact name	Contact name.
Default	“”	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # snmp-server contact my-name`	
Related Commands	show snmp	
Notes		

snmp-server enable

	snmp-server enable **no snmp-server enable** Enables SNMP-related functionality (SNMP engine, and traps) The no form of the command disables the SNMP server.
Syntax Description	N/A
Default	SNMP is enabled by default
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # snmp-server enable`
Related Commands	show snmp
Notes	

snmp-server enable

	snmp-server enable **no snmp-server enable** Enables SNMP-related functionality (SNMP engine, and traps) The no form of the command disables the SNMP server.
Syntax Description	N/A
Default	SNMP is enabled by default
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # snmp-server enable`
Related Commands	show snmp
Notes	

snmp-server engineID reset

	snmp-server engineID reset Resets the SNMPv3 engine ID to be node unique.
Syntax Description	N/A
Default	Default engineID is unchanged
Configuration Mode	config
History	3.6.6102
Role	admin
Example	`switch (config) # snmp-server engienID reset`
Related Commands	show snmp engineID
Notes	Changing system profile or performing “reset factory...” causes the engine ID to change to the new node-unique one.

snmp-server enable mult-communities

	snmp-server enable mult-communities **no snmp-server enable mult-communities** Enables multiple communities to be configured. The no form of the command disables multiple communities to be configured.
Syntax Description	N/A
Default	SNMP server multi-communities are disabled by default
Configuration Mode	config
History	N/A
Role	admin
Example	`switch (config) # snmp-server enable mult-communities`
Related Commands	show snmp
Notes	

snmp-server enable notify

	snmp-server enable notify **no snmp-server enable notify** Enables sending of SNMP traps and informs from this system. The no form of the command disables sending of SNMP traps and informs from this system.
Syntax Description	N/A
Default	SNMP notifies are enabled by default
Configuration Mode	config
History	N/A
Role	admin
Example	`switch (config) # snmp-server enable notify`
Related Commands	show snmp
Notes	SNMP traps are only sent if there are trap sinks configured with the “snmp-server host...” command, and if these trap sinks are themselves enabled.

snmp-server enable set-permission

	snmp-server enable set-permission <MIB-name> **no snmp-server enable set-permission <MIB-name>** Allows SNMP SET requests for items in a specified MIB. The no form of the command disallows SNMP SET requests for items in a specified MIB.
Syntax Description	N/A
Default	SNMP MIBs are all given permission for SET requests by default
Configuration Mode	config
History	3.6.3004
Role	admin
Example	`switch (config) # snmp-server enable set-permission MELLANOX-SW-UPDATE`
Related Commands	show snmp set-permission
Notes	

snmp-server host disable

	snmp-server host <ip-address> disable **no snmp-server host <ip-address> [disable]** Temporarily disables sending of all notifications to this host. The no form of the commands resumes sending of all notifications to this host
Syntax Description	IP address IPv4 or IPv6 address
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # snmp-server host 10.10.10.10 disable`
Related Commands	show snmp snmp-server enable
Notes	

snmp-server host informs

snmp-server host <ip-address> informs [<community> | port <port> | version 2c | version 3 {engineID <engineID> | user <name> {auth <hash-type> <auth-password> [priv <privacy-type> [<priv-password>]] | encrypted auth ... | prompt auth ...}}]
no snmp-server host <ip-address> informs port

Send SNMP v2c informs to this host with the default trap community.
The no form of the commands removes a host from which SNMP traps should be sent.

Syntax Description	IP address	IPv4 or IPv6 address
	community	Specifies trap community string
	port	Overrides default UDP port for this trap sink
	version	Specifies the SNMP version of traps to send to this host
	engineID	Specifies engine ID of this inform sink
	user	Specifies username for this inform sink
	auth	Configures SNMP v3 security parameters, specifying passwords in plaintext on the command line (passwords are always stored encrypted)
	hash-type	• MD5 • SHA
	auth-password	Plaintext password to use for authentication. If “priv” is not specified the default privacy algorithm is used with the same privacy password as that specified for authentication.
	priv	Specifies SNMPv3 privacy settings for this user
	privacy-type	• aes-128 – uses AES-128 encryption for privacy • des – uses DES encryption for privacy
	priv-password	Plaintext password to use for privacy. If not specified, then auth-password is used.
	encrypted	Configure SNMP v3 security parameters, specifying passwords in encrypted form
	prompt	Configure SNMP v3 security parameters, specifying passwords securely in follow-up prompts, rather than on the command line
Default	Default community is “public” Default UDP port is 162 Default SNMP version is 2	

Configuration Mode	config
History	3.2.1050
Role	admin
Example	`switch (config) # snmp-server host 1.1.1.1 informs version 3 engineID 0x800041da04643265363932653432303135 user test auth md5 password priv aes-128 password`
Related Commands	show snmp snmp-server enable snmp-server host informs version 3
Notes	

snmp-server host traps

snmp-server host <ip-address> traps [<community> | port <port> | version {1 | 2c} | version 3 {user <name> {auth <hash-type> <auth-password> [priv <privacy-type> [<priv-password>]] | encrypted auth ... | prompt auth ...}}]
no snmp-server host <ip-address> traps port

Send SNMP v2c traps to this host with the default trap community.
The no form of the commands removes a host from which SNMP traps should be sent.

Syntax Description	IP address	IPv4 or IPv6 address
	community	Specifies trap community string
	port	Overrides default UDP port for this trap sink
	version	Specifies the SNMP version of traps to send to this host
	user	Specifies username for this inform sink
	auth	Configures SNMP v3 security parameters, specifying passwords in plaintext on the command line (passwords are always stored encrypted)
	hash-type	• MD5 • SHA
	auth-password	Plaintext password to use for authentication. If “priv” is not specified the default privacy algorithm is used with the same privacy password as that specified for authentication.
	priv	Specifies SNMPv3 privacy settings for this user
	privacy-type	• aes-128 – uses AES-128 encryption for privacy • des – uses DES encryption for privacy
	priv-password	Plaintext password to use for privacy. If not specified, then auth-password is used.
	encrypted	Configure SNMP v3 security parameters, specifying passwords in encrypted form
	prompt	Configure SNMP v3 security parameters, specifying passwords securely in follow-up prompts, rather than on the command line
Default	Default community is “public” Default UDP port is 162 Default SNMP version is 2	
Configuration Mode	config	

History	3.1.0000
Role	admin
Example	`switch (config) # snmp-server host 1.1.1.1 informs version 3 user test auth md5 password priv aes-128 password`
Related Commands	show snmp snmp-server enable snmp-server host informs version 3
Notes	

snmp-server listen

snmp-server listen {enable | interface <ifName>}
no snmp-server listen {enable | interface <ifName>}

Configures SNMP server interface access restrictions.
The no form of the command disables the listen interface restricted list for SNMP server.

Syntax Description	enable	Enables SNMP interface restrictions on access to this system.
	ifName	Adds an interface to the “listen” list for SNMP server. For example: “mgmt0”, “mgmt1”.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # snmp listen enable`	
Related Commands	show snmp	
Notes	If enabled, and if at least one of the interfaces listed is eligible to be a listen interface, then SNMP requests will only be accepted on those interfaces. Otherwise, SNMP requests are accepted on any interface.	

snmp-server 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	
	3.2.1050	Changed traps to notify
Role	admin	
Example	`switch (config) # snmp-server community public`	
Related Commands	show snmp show snmp events	
Notes	• This setting is only meaningful if traps are enabled, though the list of hosts may still be edited if traps are disabled • Refer to Mellanox MIB file for the list of supported traps	

snmp-server port

snmp-server port <port>
no snmp-server port

Sets the UDP listening port for the SNMP agent.
The no form of the command resets the parameter to its default value.

Syntax Description	port	UDP port.
Default	161	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # snmp-server port 1000`	
Related Commands	show snmp	
Notes		

snmp-server user

snmp-server user {admin | <username>} v3 {[encrypted] auth <hash-type> <password> [priv <privacy-type> [<password>]] | capability <cap> | enable <sets> | prompt auth <hash-type> [priv <privacy-type>] | require-privacy}
no snmp-server user {admin | <username> } v3 {[encrypted] auth <hash-type> <password> [priv <privacy-type> [<password>]] | capability <cap> | enable <sets> | prompt auth <hash-type> [priv <privacy-type>]}

Specifies an existing username, or a new one to be added.
The no form of the command disables access via SNMP v3 for the specified user.

Syntax Description	v3	Configures SNMP v3 users
	auth	Configures SNMP v3 security parameters, specifying passwords in plaintext on the command line (note: passwords are always stored encrypted). Available hash-type options are: <md5|sha|sha224|sha256|sha384|sha512>.
	capability	Sets capability level for SET requests
	enable	Enables SNMP v3 access for this user
	encrypted	Configures SNMP v3 security parameters, specifying passwords in encrypted form
	prompt	Configures SNMP v3 security parameters, specifying passwords securely in follow-up prompts, rather than on the command line
	require-privacy	Requires privacy (encryption) for requests from this user
	priv	Configures SNMP v3 security parameters, specifying which protocol to use for traffic encryption. Available priv-type options: <des|3des|aes-128|aes-192|aes-256>.
Default	No SNMP v3 users defined	
Configuration Mode	config	
History	3.1.0000	
	3.7.00xx	
Role	admin	
Example	`switch (config) # snmp-server user admin v3 enable`	

Related Commands	show snmp user
Notes	• The username chosen here may be anything that is valid as a local UNIX username (alphanumeric, plus '-', '_', and '.'), but these usernames are unrelated to, and independent of, local user accounts. That is, they need not have the same capability level as a local user account of the same name. Note that these usernames should not be longer than 31 characters, or they will not work. • The hash algorithm specified is used both to create digests of the authentication and privacy passwords for storage in configuration, and also in HMAC form for the authentication protocol itself. • There are three variants of the command, which branch out after the “v3” keyword. If “auth” is used next, the passwords are specified in plaintext on the command line. If “encrypted” is used next, the passwords are specified encrypted (hashed) on the command line. If “prompt-pass” is used, the passwords are not specified on the command line the user is prompted for them when the command is executing. If “priv” is not specified, only the auth password is prompted for. If “priv” is specified, the privacy password is prompted for; entering an empty string for this prompt will result in using the same password specified for authentication. • AES privacy type encryption using the newest algorithm, which means we use aes-blumenthal. For more information see - http://www.snmp.com/eso/esoConsortiumMIB.txt • No more than 30 SNMP V3 users are allowed in the database.

show snmp

show snmp [events | host]

Displays SNMP-server configuration and status.

Syntax Description	events	SNMP events
	host	List of notification sinks
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
	3.6.8008	Updated Example
Role	admin	

Example	`switch (config) # show snmp`
	
	`SNMP enabled : no`
	`SNMP port : 161`
	`System contact : Test`
	`System location: Boston`
	
	`Read-only communities:`
	`public`
	
	`Read-write communities:`
	`good`
	
	`Interface listen enabled: yes`
	
	`Listen Interfaces:`
	`Interface: mgmt0`	

Related Commands	show snmp	
Notes		

show snmp auto-refresh

	show snmp auto-refresh Displays SNMPD refresh mechanism status.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000 3.6.6000 Updated Example 3.7.00xx Updated Example
Role	admin

Example	`switch (config) # show snmp auto-refresh`
	`SNMP auto refresh:`
	`Auto-refresh enabled: yes`
	`Refresh interval (sec): 60`
	`Cache enabled: yes`
	
	`Auto-Refreshed tables:`
	`ifTable`
	`ifXTable`
	`mellanoxIfVPITable`

Related Commands	snmp-server auto-refresh
Notes	

show snmp engineID

	show snmp engineID Displays SNMPv3 engine ID key.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.6102
Role	admin
Example	`switch (config) # show snmp engineID` `Local SNMP engineID: 0x80004f4db1dd435e80accf4a4d4d3031`
Related Commands	snmp-server engineID
Notes	

show snmp set-permission

show snmp set-permission

Displays SNMP SET permission settings.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.3004
Role	admin

Example	`switch (config) # show snmp set-permission`
	`---------------------------------------------`
	`MIB Name                              Set Enable`
	`---------------------------------------------`
	`MELLANOX-CONFIG-DB-MIB             yes`
	`MELLANOX-EFM-MIB                   yes`
	`MELLANOX-POWER-CYCLE               yes`
	`MELLANOX-SW-UPDATE                 no`
	`RFC1213-MIB                         no`

Related Commands	snmp-server enable set-permission
Notes	

show snmp user

	show snmp user Displays SNMP user information.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000 3.6.8008 Updated Example
Role	admin

Example	`switch (config) # show snmp user`
	`User name: Hendrix`
	`   Enabled overall:         yes`
	`   Authentication type:     sha`
	`   Privacy type:            des`
	`   Authentication password: (set)`
	`   Privacy password:        (set)`
	`   Require privacy: yes`
	`   SET access:`
	`      Enabled:              yes`
	`      Capability level:     admin`
	`switch (config) #`

Related Commands	show snmp
Notes	

show interfaces ib internal notification

	show interfaces ib internal notification Displays information about internal links notification.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.3.4318 3.4.3000 Updated Example
Role	admin

Example	`switch (config) # show interfaces ib internal notification`
	`==========================`
	`Internal links information`
	`==========================`
	`State change enabled : yes`
	`Speed mismatch enabled : yes`
	`Periodic notifications : 6 (hours)`

Related Commands	interfaces ib internal notification
Notes	

4.17.4.2 XML API Commands

xml-gw enable

xml-gw enable
no xml-gw enable

Enables the XML gateway.
The no form of the command disables the XML gateway.

Syntax Description	N/A
Default	XML Gateway is enabled
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # xml-gw enable`
	`switch (config) # show xml-gw`
	`XML Gateway enabled:  yes`
	`switch (config) #`

Related Commands	show xml-gw
Notes	

show xml-gw

	show xml-gw Displays the XML gateway setting.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

Example	`switch (config) # show xml-gw`
	`XML Gateway enabled:  yes`
	`switch (config) #`

Related Commands	xml-gw enable
Notes	

4.17.4.3 JSON API Commands

json-gw enable

	json-gw enable **no json-gw enable** Enables the JSON API. The no form of the command disables the JSON API.
Syntax Description	N/A
Default	JSON API is enabled
Configuration Mode	config
History	3.6.3004
Role	admin
Example	`switch (config) # json-gw enable`
Related Commands	show json-gw
Notes	

json-gw synchronous-request-timeout

	json-gw synchronous-request-timeout <time out value> **no json-gw synchronous-request-timeout** Defines a timeout value for synchronous JSON requests (in seconds). The no form of the command returns the timeout value to its default.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.3004 3.6.4000 Updated Example and Related Commands.
Role	admin

Example	`switch (config) # show json-gw`
	
	`JSON Gateway enabled:  yes`
	`Synchronous request timeout:  30`
	`JSON API version:  1.0`

Related Commands	json-gw enable json-gw synchronous-request-timeout <time out value> no json-gw synchronous-request-timeout
Notes	

show json-gw

	show json-gw Displays the JSON API setting.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.3004 3.6.4000 Updated Example and Related Commands.
Role	admin

Example	`switch (config) # show json-gw`
	
	`JSON Gateway enabled:  yes`
	`Synchronous request timeout:  30`
	`JSON API version:  1.0`

Related Commands	json-gw enable json-gw synchronous-request-timeout <time out value> no json-gw synchronous-request-timeout
Notes	

4.18 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.

4.18.1 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) #
```

4.18.2 Accepting the Switch Request

This is to be performed on the first run only.

➢ ***To accept the switch’s request:***

Option 1 – using Puppet CLI commands:

Step 1. Ensure the certificate request. Run:

```
# puppet cert list
"<switch>"
(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 15: Accepting an Agent Request through the Console

4.18.3 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.

4.18.4 Supported Configuration Capabilities

4.18.4.1 InfiniBand Interface Capabilities

Table 36 - Ethernet and Port-Channel 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

Table 36 - Ethernet and Port-Channel Interface Capabilities

Field	Description	Values	Example
admin	Disables/enables interface admin state.	up, down	admin => up
mtu	Configures the maximum transmission unit frame size for the interface.		mtu => 1520

4.18.4.2 SNMP Capabilities

Table 37 - Protocol Enable/Disable Capabilities

Field	Description	Values	Example
ensure	Enables/disables the protocol specified in the resource ID	present, absent	ensure => present

4.18.4.3 Fetched Image Capabilities

Table 38 - 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

4.18.4.4 Installed Image Capabilities

Table 39 - Installed 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

4.18.5 Supported Resources for Each Type

Table 40 - Fetched Image Capabilities

Resource Type	Puppet Type Name	Supported Resource IDS	Example
Network device	netdev_device	$hostname	netdev_device { $hostname: }
Fetched image	mlnx_fetched_img	The image file name	mlnx_fetched_image { 'image-X86_64-3.6.8008.img': ensure => present}
Installed image	mlnx_installed_img	The image version name	mlnx_installed_img { '3.3.4300': ensure => present}

4.18.6 Troubleshooting

This section presents common issues that may prevent the switch from connecting to the puppet server.

4.18.6.1 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 `ntpdate`).

4.18.6.2 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).

4.18.6.3 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 tracepath {<hostname> | <ip>}/8140).

4.18.7 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	
Notes	

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	`switch (config puppet-agent) # master-hostname my-puppet-server-host-name` `switch (config puppet-agent) #`	
Related Commands		
Notes		

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	
Notes	

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	
Notes		

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	
Notes	

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 Example with “Run interval” 3.7.00xx Updated Example with “Puppet agent: disabled”
Role	admin

Example	`switch (config puppet-agent) # show puppet-agent`
	`Puppet agent: disabled`
	`Puppet master hostname: puppet`
	`Run interval: 30m`
	`switch (config puppet-agent) #`

Related Commands	
Notes	

4.19 Control Plane Policing

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		
Related Commands		
Notes		

```
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) #
```

Control Plane Policing or Policies (CoPP) ensures the CPU and control plane are not over-utilized which is essential for the robustness of the switch. CoPP limits the number of control plane packets. MLNX-OS implements several CoPP mechanisms:

- ACLs may be used to limit the rate of packets or bytes of a certain type, including L3 control packets (L2 control packets are forwarded to the CPU before the ACL)
- Policers on traffic going to the CPU – these policers are configured by MLNX-OS and cannot be modified by the user
- IP filter tables limit the traffic to the CPU coming in from the management ports.

4.19.1 IP Table Filtering

IP table filtering is a mechanism that allows the user to apply actions to a specific control packet flow identified by a certain flow key.

This mechanism is used in order to protect switch control traffic against attacks. For example, it could allow traffic coming from a specific trusted management subnet only, block the SNMP UDP port from receiving traffic, and force ping rate to be lower than a specific threshold.

Each IP table rule is defined by key, priority, and action:

- Key – the key is a combination of physical port and layer 3 parameters (e.g. SIP, DIP, SPORT, DPORT, etc.), and other fields. Each part of the key, can be set to a specific value or masked.
- Priority – each rule in the IP table is assigned a priority, and the rule with the highest priority whose key matches the packet executes the action.
- Action – the action describes the behavior of packets which match the key. The action type may be drop, accept, rate limit, etc.

An IP table rule is bound to an IP interface that can be a management out-of-band interface, VLAN interface, or router port interface. Once bound, all traffic received (ingress rule) or transmitted (egress rule) in this direction is being verified with all bounded rules.

Once a match was found, the rule action is executed. If no match is found, the default policy of the chain shall apply.

IP table rules get a lower priority than ACL mechanism.

4.19.1.1 Configuring IP Table Filtering

Prerequisite for IPv6:

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

➢ ***To configure IPv4 table filtering:***

Step 1. Select the policy that applies to the input/output chain (default is “accept”). Run:

```
switch (config)# ip filter chain input policy drop
switch (config)# ip filter chain output policy accept
```

Step 2. Append filtering rules to the list or set a specific rule number, select a target, and (optional) any additional filter conditions. For example, run:

```
switch (config)# ip filter chain input rule append tail target rate-limit 2 protocol
udp
switch (config)# ip filter chain input rule set 2 target drop protocol icmp in-intf
mgmt1
switch (config)# ip filter chain output rule append tail target drop protocol icmp
```

Step 3. Enable IP table filtering. Run:

```
switch (config) # ip filter enable
```

Step 4. Verify IP table filtering configuration. Run:

```
switch (config) # show ip filter configured

Packet filtering for IPv4: enabled

IPv4 configuration:
  Chain 'input' Policy 'accept':
    Rule 1:
      Target      : rate-limit 2 pps
      Protocol    : udp
      Source      : all
      Destination : all
      Interface   : all
      State       : any
      Other Filter:  -

    Rule 2:
      Target      : drop
      Protocol    : icmp
      Source      : all
      Destination : all
      Interface   : mgmt1 (ingress)
      State       : any
      Other Filter:  -

  Chain 'output' Policy 'accept':
    Rule 1:
      Target      : drop
      Protocol    : icmp
      Source      : all
      Destination : all
      Interface   : all
      State       : any
      Other Filter: -
```

4.19.1.2 Modifying IP Table Filtering

- ***To modify IP table filtering configuration:***

```
switch (config) # ip filter chain input rule modify 3 target reject-with icmp6-adm-pro-
hibited source-addr 10::0 /126
```

- ***To delete an existing IP table filtering rule:***

```
switch (config) # no ip filter chain input rule 2
```

- ***To delete all existing IP table filtering rules:***

```
switch (config) # no ip filter chain output rule all
```

- ***To insert an IP table filtering rule in a chain:***

```
switch (config) # ip filter chain input rule 2 set target drop protocol tcp dest-port
22 in-intf mgmt1
```

4.19.1.3 Rate-limit Rule Configuration

Using a rate-limit target allows to create a rule to limit the rate of certain traffic types. The limit is specified in packets per second (pps) and can be anywhere between 1-1000 pps. When enabled, the system takes the user specified rate and converts it into units of 1/10000 of a second. Therefore, any value greater than 100 can have a slight difference when the rule is displayed using the show command.

Unlike other rules which are a match type of rule, limiting packets should be followed by a rule that drops additional packets of the same “type”. Alternatively, this can be implicitly achieved by setting the chain policy to “drop” so that it drops packets not processed by matching rules. Otherwise, no effect of the rule is observed as the remaining traffic simply gets accepted.

Rate-limit is implemented with an average rate and a burst-limit. Rate values are specified in pps and take a range from 1-1000 pps. For rate values in the range 1-100, the burst value is set equal to the rate value. For rate values in the range 101-1000, the burst limit is set to 100.

4.19.2 Commands

ip filter enable
ipv6 filter enable

{ip | ipv6} filter enable
no {ip | ipv6} filter enable

Enables IP filtering.
The no form of the command disables IP filtering.

Syntax Description	N/A
Default	Disabled
Configuration Mode	config
History	3.5.1000
Role	admin
Example	`switch (config) # ip filter enable` `switch (config) #`
Related Commands	N/A
Notes	It is recommended to run this command only after configuring all of the IP table filter parameters.

ip filter chain policy
ipv6 filter chain policy

{ip | ipv6} filter chain <chain_name> policy {accept | drop}
no {ip | ipv6} filter chain <chain_name> policy

Configures default policy for a specific chain (if no rule matches this default policy action shall apply).
The no form of the command resets default policy for a specific chain.

Syntax Description	chain_name	Selects a chain for which to add or modify a filter: • input – input chain or ingress interfaces • output – output chain or egress interfaces
	accept	Accepts all traffic by default for this chain
	drop	Drops all traffic by default for this chain
Default	Accept for input and output chains	
Configuration Mode	config	
History	3.5.1000	
Role	admin	
Example	`switch (config) # ipv6 filter chain input policy accept` `switch (config) #`	
Related Commands	N/A	
Notes		

ip filter chain rule target
ipv6 filter chain rule target

{ip | ipv6} filter chain <chain_name> rule <oper> target <target> [<param>]
no {ip | ipv6} filter chain <chain_name> rule {<number> | all}

Inserts rule before specified rule number.
The no form of the command deletes rule for a specific chain.

Syntax Description	chain_name	A chain to which to add or modify a filter: • input – input chain or ingress interfaces • output – output chain or egress interfaces
	rule	• append tail – appends operation to the bottom of operation list • insert <oper_num> – inserts operation at specified position (existing operation at that position moves back in the list) • modify <oper_num> – modifies existing operation at specified position. Only the parameters specified in this invocation are altered; everything else is left untouched. • move <oper_num1> to <oper_num2> – moves one operation to another place in the operation list • set <oper_num> – sets operation at specified position (overwrites existing)
	target	• accept – allows the packets that match the rule into the management plane • drop – drops packets that match the rule • rate-limit – allows with rate limiting in packets per sec (PPS) • reject-with – drops the packet and replies with an ICMP error message

param	• comment <text> – specifies description string for this rule (60 chars max) • dest-addr <ip> – IP matching a specific destination address or address range. A specific IPv4 address can be provided or an entire subnet by giving an address along with netmask in dot notation or as a CIDR notation (e.g. /24). • not-dest-addr <ip> – IP not matching a specific destination address range • dest-port <port(s)> – matching a specific destination port or port range • not-dest-port <port(s)> – port not matching a specific destination port or port range • dup-delete – deletes any preexisting duplicates of this rule • in-intf – interface matching a specific inbound interface • not-in-intf <if_name> – interface not matching a specific inbound interface • out-intf <if_name> – matches a specific outbound interface • not-out-intf <if_name> – interface not matching a specific outbound interface

param4 (cont.)	• protocol <if_name> – matches a specific protocol
	  • tcp
	  • udp
	  • icmp
	  • all
	• not-protocol <protocol> – does not match a specific protocol
	  • tcp
	  • udp
	  • icmp
	  • all
	• source-addr <ip> – matches a specific source address range
	• not-source-addr <ip> – does not match a specific source address range
	• source-port <port(s)> – matches a specific source port or port range
	• not-source-port <port(s)> – does not match a specific source port or port range
	• state – matches packets in a particular state. Possible values:
	  • established – packet associated with an established connection which has seen traffic in both directions
	  • related – packet that starts a new connection but is related to an existing connection
	  • new – packet that starts a new, unrelated connection
	  • A combination can be entered separated by commas

Default	N/A
Configuration Mode	config
History	3.5.1000
Role	admin
Example	`switch (config) # ipv6 filter enable chain input rule append tail target drop state related protocol all dup-delete` `switch (config) #`
Related Commands	N/A
Notes	• The source and destination ports may each be either a single number, or a range specified as “<low>-<high>”. For example: “10-20” would specify ports 10 through 20 (inclusive). • The port parameter only works in conjunction with TCP and UDP. • Setting a “positive” rule removes any corresponding “not-” rules, and vice-versa • The “state” parameter is a classification of the packet relative to existing connections • If TCP or UDP are selected for the “protocol” parameter, source and/or destination ports may be specified. If ICMP is selected, these options are either ignored, or an error is produced.

show ip filter

	show ip filter Displays IPv4 filtering state.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show ip filter`
	
	`Packet filtering for IPv4: enabled`
	
	`Active IPv4 filtering rules (omitting any not from configuration):`
	`  Chain 'input' Policy 'accept':`
	`    Rule 1:`
	`      Target      : accept`
	`      Protocol    : all`
	`      Source      : all`
	`      Destination : 1.1.1.0/24`
	`      Interface   : all`
	`      State       : any`
	`      Other Filter:  -`
	
	`  Chain 'output' Policy 'accept':`
	`    Rule 1:`
	`      Target      : reject-with icmp-net-unreachable`
	`      Protocol    : tcp`
	`      Source      : all`
	`      Destination : all`
	`      Interface   : all`
	`      State       : any`
	`      Other Filter: dest-port 1000`

Related Commands	N/A
Notes	N/A

show ip filter all

	show ip filter all Displays IPv4 filtering state (including un-configured rules).
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show ip filter all`
	
	`Packet filtering for IPv4: enabled`
	
	`All active IPv4 filtering rules:`
	`  Chain 'input' Policy 'accept':`
	`  Rule 1:`
	`  Target  : accept`
	`  Protocol  : all`
	`  Source  : all`
	`  Destination : 1.1.1.0/24`
	`  Interface  : all`
	`  State  : any`
	`  Other Filter:  -`
	
	`  Chain 'output' Policy 'accept':`
	`  Rule 1:`
	`  Target  : reject-with icmp-net-unreachable`
	`  Protocol  : tcp`
	`  Source  : all`
	`  Destination : all`
	`  Interface  : all`
	`  State  : any`
	`  Other Filter: dest-port 1000`

Related Commands	N/A
Notes	N/A

show ip filter configured

	show ip filter configured Displays IPv4 filtering configuration.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show ip filter configured`
	
	`Packet filtering for IPv4: enabled`
	
	`IPv4 configuration:`
	`  Chain 'input' Policy 'accept':`
	`    Rule 1:`
	`      Target      : accept`
	`      Protocol    : all`
	`      Source      : all`
	`      Destination : 1.1.1.0/24`
	`      Interface   : all`
	`      State       : any`
	`      Other Filter:  -`
	
	`  Chain 'output' Policy 'accept':`
	`    Rule 1:`
	`      Target      : reject-with icmp-net-unreachable`
	`      Protocol    : tcp`
	`      Source      : all`
	`      Destination : all`
	`      Interface   : all`
	`      State       : any`
	`      Other Filter: dest-port 1000`

Related Commands	N/A
Notes	N/A

show ipv6 filter

	show ipv6 filter Displays IPv6 filtering state.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show ipv6 filter`
	
	`Packet filtering for IPv6: enables`
	
	`Active IPv6 filtering rules (omitting any not from configuration):`
	`  Chain 'input' Policy 'accept':`
	`    Rule 1:`
	`      Target      : accept`
	`      Protocol    : all`
	`      Source      : all`
	`      Destination : 1.1.1.0/24`
	`      Interface   : all`
	`      State       : any`
	`      Other Filter:  -`
	
	`  Chain 'output' Policy 'accept':`
	`    Rule 1:`
	`      Target      : reject-with icmp-net-unreachable`
	`      Protocol    : tcp`
	`      Source      : all`
	`      Destination : all`
	`      Interface   : all`
	`      State       : any`
	`      Other Filter: dest-port 1000`

Related Commands	N/A
Notes	N/A

show ipv6 filter all

	show ipv6 filter all Displays IPv6 filtering state (including un-configured rules).
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show ipv6 filter all`
	
	`Packet filtering for IPv6: enables`
	
	`All active IPv6 filtering rules:`
	`  Chain 'input' Policy 'accept':`
	`    Rule 1:`
	`      Target      : accept`
	`      Protocol    : all`
	`      Source      : all`
	`      Destination : 1.1.1.0/24`
	`      Interface   : all`
	`      State       : any`
	`      Other Filter:  -`
	
	`  Chain 'output' Policy 'accept':`
	`    Rule 1:`
	`      Target      : reject-with icmp-net-unreachable`
	`      Protocol    : tcp`
	`      Source      : all`
	`      Destination : all`
	`      Interface   : all`
	`      State       : any`
	`      Other Filter: dest-port 1000`

Related Commands	N/A
Notes	N/A

show ipv6 filter configured

	show ipv6 filter configured Displays IPv6 filtering configuration.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show ipv6 filter configured`
	
	`Packet filtering for IPv6: enables`
	
	`IPv6 configuration:`
	`  Chain 'input' Policy 'accept':`
	`    Rule 1:`
	`      Target      : accept`
	`      Protocol    : all`
	`      Source      : all`
	`      Destination : 1.1.1.0/24`
	`      Interface   : all`
	`      State       : any`
	`      Other Filter:  -`
	
	`  Chain 'output' Policy 'accept':`
	`    Rule 1:`
	`      Target      : reject-with icmp-net-unreachable`
	`      Protocol    : tcp`
	`      Source      : all`
	`      Destination : all`
	`      Interface   : all`
	`      State       : any`
	`      Other Filter: dest-port 1000`

Related Commands	N/A
Notes	N/A

4.19.3

5 InfiniBand Switching

5.1 Node Name

5.1.1 Commands

ib nodename

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

Maps between GUID and node name.

Syntax Description	guid	System GUID
	name	User defined string
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

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

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

show ib nodename

	show ib nodename Maps between GUID and node name.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Role	admin

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

Related Commands	ib nodename
Notes	

5.2 Fabric

5.2.1 Commands

fabric zero-counters

	fabric zero-counters Clears the performance counters of the node.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	monitor/admin

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

Related Commands	
Notes	

show fabric

show fabric {pm | sm}

Displays InfiniBand fabric details.

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

Example	`switch (config) # show fabric sm`
	`% # This database file was automatically generated by IBDIAG`
	
	`ibdiagnet fabric SM report`
	
	`  SM - master`
	`    Port=0 lid=0x0005 guid=0x0002c903004a2980 dev=51000 priority:15`
	
	`  SM - standby`
	`    Port=0 lid=0x0001 guid=0x0000000000000111 dev=51000 priority:0`
	`switch (config) #`	

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

show guids

	show guids Displays GUIDs per ASIC in the chassis.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000 3.4.2008 Updated Example 3.6.1002 Updated Example
Role	admin

Example	`switch (config) # show guids`
	`============================================================`
	`Module  Device  IB Subnet  GUID`
	`============================================================`
	`SYSTEM  -  -  E4:1D:2D:03:00:2E:49:40`
	`MGMT  SIB  infiniband-default  E4:1D:2D:03:00:2E:49:40`
	`MGMT  SIB  infiniband-1  E4:1D:2D:03:00:2E:49:41`
	`MGMT  SIB  infiniband-2  E4:1D:2D:03:00:2E:49:42`
	`switch (config) #`

Related Commands	
Notes	

show system guid

	show {guids | system guid} Displays the system GUID.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

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

Related Commands	
Notes	

show lids

	show lids Displays the LIDs of each module in the switch system
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000 3.4.2008 Updated Example 3.6.1002 Updated Example
Role	admin/monitor

Example	`switch (config) # show lids`
	`==========================================`
	`Module  Device  IB Subnet  LID`
	`==========================================`
	`MGMT  SIB  infiniband-default  1`
	`MGMT  SIB  infiniband-1  8`
	`MGMT  SIB  infiniband-2  3`
	`switch (config) #`

Related Commands	
Notes	

5.3 IB Router

IB router provides the ability to send traffic between two or more IB subnets thereby potentially expanding the size of the network to over 40k end-ports, enabling separation and fault resilience between islands and IB subnets, and enabling connection to different topologies used by different subnets.

The forwarding between the InfiniBand subnets is performed using GRH (global route header) lookup.

IB router capabilities are supported only on SB7780 switch system which comes with the following default configuration:

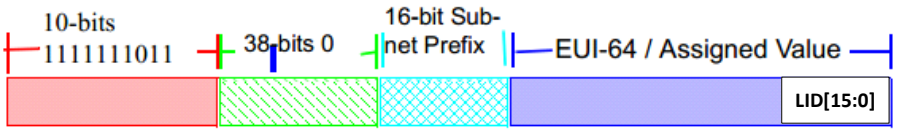
- L3 capabilities enabled
- 2 SWIDs, with interface 1/1 mapped to infiniband-default and interface 1/2 mapped to infiniband-1

The IB router's basic functionality includes:

- Removal of current L2 LRH (local routing header)
- Routing table lookup – using GID from GRH
- Building new LRH according to the destination and the routing table

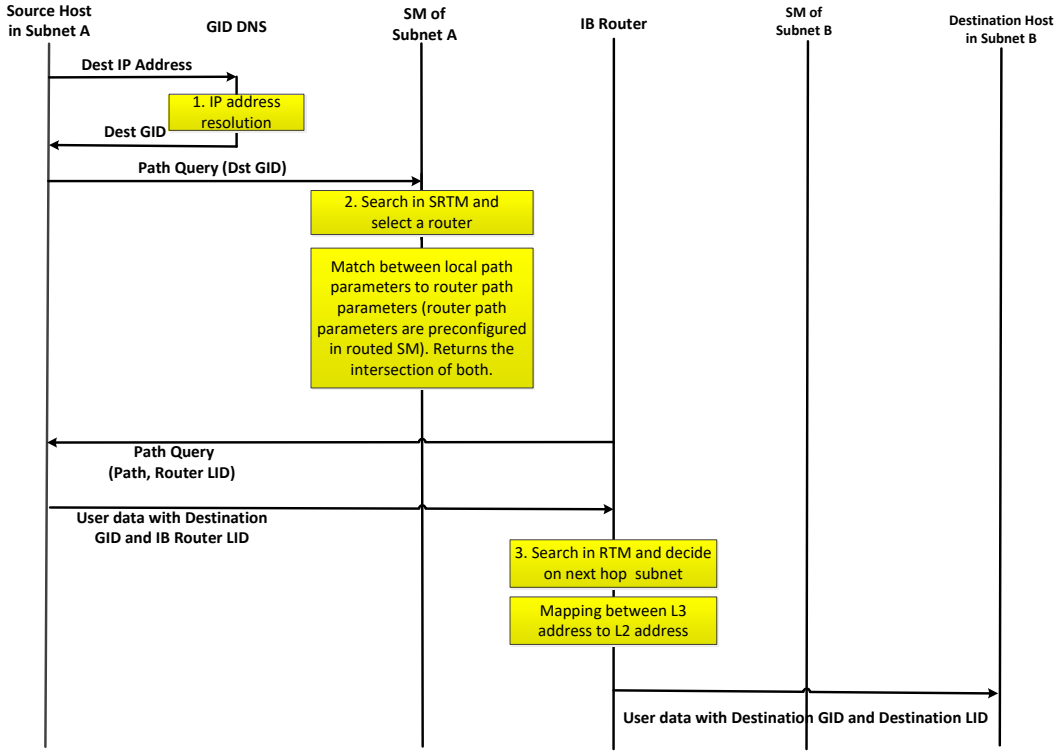
The DLID in the new LRH is built using simplified GID-to-LID mapping (where LID = 16 LSB bits of GID) thereby not requiring to send for ARP query/lookup.

Figure 16: Site-Local Unicast GID Format



For this to work, the SM allocates an alias GID for each host in the fabric where the alias GID = {subnet prefix[127:64], reserved[63:16], LID[15:0]}. Hosts should use alias GIDs in order to transmit traffic to peers on remote subnets.

Figure 17: Host-to-Host IB Router Unicast Flow



For more information on IB router architecture and functionality, please refer to the following Mellanox Community page: https://community.mellanox.com/docs/DOC-2384.

IB router requires HCA configuration such as SM, partition key, MPI, GID translation, and more. To learn more about these configurations, please refer to the following Mellanox Community page: https://community.mellanox.com/docs/DOC-2466.

5.3.1 Configuring IB Router

Prerequisites:

Step 1. Check system capabilities to make sure IB L3 is supported. Run:

```
switch (config) # show system capabilities
IB: Supported, L2, L3, Adaptive Routing
Max SM nodes: 2048
IB Max licensed speed: EDR
```

Step 2. Configure system profile to multi-switch with 2 SWIDs. Run:

```
switch (config) # system profile ib num-of-swids 2 no-adaptive-routing ib-router
```

Note that some of the interfaces may not be mapped to a SWID.

Step 3. Verify system profile configuration. Run:

```
switch (config) # show system profile
Profile:             ib
Number of SWIDs:     2
Adaptive Routing:    no
IB Routing:          yes
```

➢ ***To configure IB router:***

Step 1. Map an interface to a SWID. Run:

```
switch (config) # interface ib 1/1 switchport access subnet infiniband-default force
switch (config) # interface ib 1/2 switchport access subnet infiniband-1 force
```

Step 2. Verify SWID configuration. Run:

```
switch (config) # show interfaces ib status
Interface    Description    IB Subnet            Speed             Current line rate  Logical port state  Physical port state
---------    -----------    ---------            ---------         ----------------   ------------------  -------------------
IB1/1                       infiniband-default    -                 -                  Down                Polling
IB1/2                       infiniband-1          edr               100.0 Gbps         Initialize          LinkUp
IB1/3                       -                     -                 -                  -                   -
...
```

Step 3. Configure and enable IB router. Run:

```
switch (config) # ib router
switch (config) # no ib router shutdown
```

Step 4. Enable IB subnet interface. Run:

```
switch (config) # no interface ib-subnet infiniband-default shutdown
switch (config) # no interface ib-subnet infiniband-1 shutdown
```

Step 5. Verify configuration. Run:

```
switch (config) # show ib router
Routing state: enabled

IB subnet               Routing enabled
  infiniband-default      enabled
  infiniband-1            enabled
```

```
switch (config) # show interfaces ib-subnet infiniband-default
infiniband-default state:
  GUID                 : F4:52:14:03:00:6E:F2:8B
  Alias GID            : N/A
  LID                  : 10
  Subnet prefix        : FE:C0:00:00:00:00:00:08
  Physical state       : LinkUp
  Logical state        : Active
  L3 interface state   : Up
switch (config) #
```

For more advanced information on IB router configuration, please refer to the following Mellanox Community page: https://community.mellanox.com/docs/DOC-2466.

5.3.2 Subnet Prefix Checking

The SB7780 IB router expects the subnet prefix to be constructed according to some very specific rules. By default, the command which enables IB routers validates the subnet prefix prior to allowing the change.

The commands which affect subnet prefix checking are as follows:

- ib sm <name> enable – starts SM on this node or any node in cluster
- ib sm subnet-prefix <subnet-prefix> – configures the subnet prefix
- ib sm rtr-aguid-enable <1 | 2> – enables support for alias GIDs as needed by IB routers

When any of these commands is run, while the other two have already been issued, the value of the subnet prefix is checked. If it is not valid, the current commit is rejected and the OpenSM state does not change.

➢ ***To disable subnet prefix checking***

Step 1. Verify the status of subnet prefix override. Run:

```
switch (config) # show ib sm subnet-prefix-override
enable
```

Step 2. If enabled, disable subnet-prefix-override. Run:

```
switch (config) # ib sm subnet-prefix-override
```

Step 3. Verify configuration. Run:

```
switch (config) # show ib sm subnet-prefix-override
disable
```

5.3.3 Commands

ib router

	ib router **no ib router** Enables the set of commands that allow control of IB router functionality. The no form of the command disables IB router commands and removes all related configurations.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.0500
Role	admin
Example	`switch (config) # ib router` `switch (config) #`
Related Commands	system profile
Notes	

ib router shutdown

	ib router shutdown **no ib router shutdown** Disables IB router. The no form of the command enables IB router.
Syntax Description	N/A
Default	Disabled
Configuration Mode	config
History	3.6.0500
Role	admin
Example	`switch (config) # no ib router shutdown` `switch (config) #`
Related Commands	
Notes	This command does not clear IB router configuration

interface ib-subnet

interface ib-subnet <swid-name>
no interface ib-subnet <swid-name>

Creates routing on IB router subnet.
The no form of the command removes routing on router interface.

Syntax Description	swid-name	Name of the SWID: infiniband-default, infiniband-1…infiniband-5
Default	N/A	
Configuration Mode	config	
History	3.6.0500	
Role	admin	
Example	`switch (config) # interface ib-subnet infiniband-3` `switch (config) #`	
Related Commands	system profile	
Notes	The maximum number of SWIDs depends on the number of SWIDs defined in the profile	

interface ib-subnet shutdown

	interface ib-subnet <swid-name> shutdown **no interface ib-subnet <swid-name> shutdown** Disables routing on IB router subnet. The no form of the command enables routing on router interface.	
Syntax Description	swid-name	Name of the SWID: infiniband-default, infiniband-1…infiniband-5
	shutdown	Admin down on router interface Admin up on router interface with no form of command
Default	Disabled	
Configuration Mode	config	
History	3.6.0500	
Role	admin	
Example	`switch (config) # no interface ib-subnet infiniband-3 shutdown` `switch (config) #`	
Related Commands		
Notes		

show ib router

	show ib router Displays current IB router functionality.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.0500
Role	admin

Example	`switch (config) # show ib router`
	`Routing state: enabled`
	
	`IB Subnet Routing enabled`
	`infiniband-default enabled`
	`infiniband-1 disabled`
	`infiniband-2 enabled`
	`infiniband-3 enabled`
	
	`switch (config) #`

Related Commands	
Notes	

show interfaces ib-subnet

show interfaces ib-subnet [<swid-name>] [brief]

Displays statistics of one or all IB subnets with enabled IB routing.

Syntax Description	swid-name	Name of the SWID: infiniband-default, infiniband-1…infiniband-5
	brief	Displays output in a table format
Default	Disabled	
Configuration Mode	config	
History	3.6.0500	
Role	admin	

Example	`switch (config) # show interfaces ib-subnet infiniband-3`
	`infiniband-3 state:`
	`  GUID  : F4:52:14:03:00:6E:F2:8B`
	`  Alias GID  : N/A`
	`  LID  : 10`
	`  Subnet prefix  : FE:C0:00:00:00:00:00:08`
	`  Physical state  : LinkUp`
	`  Logical state  : Active`
	`  L3 interface state  : Up`	

Related Commands		
Notes		

5.4 Interface

5.4.1 Transceiver Information

Mellanox MLNX-OS offers the option of viewing the transceiver information of a module or cable connected to a specific interface. The information is a set of read-only parameters burned onto the EEPROM of the transceiver by the manufacture. The parameters include identifier (connector type), cable type, speed and additional inventory attributes.

➢ ***To display transceiver information of a specific interface, run:***

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

switch (config) #
```

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

5.4.2 High Power Transceivers

Mellanox switch systems offer high power transceiver (e.g. LR4) support on all ports of the Switch-IB family switch systems.

If a high power transceiver (e.g. LR4) is inserted to a port that does not support it, the link does not go up, and the following warning message is displayed: “Warning: High power transceiver is not supported” when the command “show interfaces ib” is run.

5.4.3 Forward Error Correction

Forward Error Correction (FEC) mechanism adds extra data to the transmitted information. The receiving device uses this additional data to verify that the received data contains no errors. If the receiving side discovers errors within the received data it is able to correct some of these errors. The number or errors that can be corrected depends on the FEC algorithm.

Switch-IB™ EDR (100Gb/s) Mellanox-to-Mellanox InfiniBand connections enable standard low-latency Reed Solomon (LL RS) FEC on active optical cables longer than 30 meters and passive copper cables longer than 2m.

5.4.4 Break-Out Cables

This feature is available only for Quantum based switch systems.

The break-out cable is a unique Mellanox capability, where a single physical quad-lane QSFP port is divided into 2 dual-lane ports. It maximizes the flexibility of the end user to use the Mellanox switch with a combination of dual-lane and quad-lane interfaces according to the specific requirements of its network. All system ports may be split into 2-lane ports. 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 single-lane port (1,2). Each sub-physical port is then handled as an individual port. For example, splitting port 5 into 2 lanes gives the following new ports: 1/5/1 & 1/5/2.

Figure 18: Break-Out Cable

Splitting the interface deletes all configuration on that interface.

In order to use this feature, the system's profile must be configured to "ib split-ready" as described in Section 5.4.4.1, "Changing System Profile to Allow for Split-Ready Configuration," on page 594 using the command "system profile" on page 461.

5.4.4.1 Changing System Profile to Allow for Split-Ready Configuration

➢ ***If system does not have system-ready configuration, change its profile to allow for it.***

Step 1. Change the system's profile to "ib split-ready". Run:

```
switch (config) # system profile ib split-ready
Warning - confirming will cause system reboot and all configuration will be deleted
Type 'yes' to confirm profile change: yes
```

Step 2. Verify system profile configuration. Run:

```
switch (config) # show system profile
Profile: ib
Number of SWIDs: 1
Adaptive Routing: yes
Adaptive Routing Groups: N/A
Split Ready: yes
IB Routing: no
```

5.4.4.2 Changing the Module Type to a Split Mode

➢ ***To split an interface:***

Step 1. Shut down all the ports related to the interface. In case of split-2, shut down the current interface only.

Step 2. Split the ports as desired. Run:

```
switch (config interface ib 1/4) # module-type qsfp-split-2
```

Step 3. New ports can be shown by the interfaces IB status command:

```
switch (config) # show interfaces ib status
Interface    Description      IB Subnet             Speed      Current line rate   Logical port state   Physical port state
---------    -----------      ---------             -------    -----------------   ------------------   -------------------
IB1/1/1                       infiniband-default    edr             25.0 Gbps           Active           LinkUp
IB1/1/2                       infiniband-default    -               -                   Down             Polling
IB1/2                         infiniband-default    edr             100.0 Gbps          Active           LinkUp
IB1/3                         infiniband-default    -               -                   Down             Polling
IB1/4/1                       infiniband-default    -               -                   Down             Polling
IB1/4/2                       infiniband-default    -               -                   Down             Polling
IB1/5                         infiniband-default    -               -                   Down             Polling
IB1/6                         infiniband-default    -               -                   Down             Polling
IB1/7                         infiniband-default    -               -                   Down             Polling
IB1/8                         infiniband-default    -               -                   Down             Polling
```

5.4.4.3 Unsplitting a Split Port

➢ ***To unsplit a split port:***

Step 1. Shut down all of the split ports. Run:

```
switch (config) # interface ib 1/4/1
switch (config interface ib 1/4/1) # shutdown
switch (config interface ib 1/4/1) # exit
switch (config) # interface ib 1/4/2
switch (config interface ib 1/4/2) # shutdown
switch (config interface ib 1/4/2) # exit
```

Step 2. From the first member of the split (1/4/1), change the module-type back to QSFP. Run:

```
switch (config interface ib 1/4/1) # module-type qsfp
```

5.4.5 Commands

interface ib

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

mtu

mtu <frame-size>

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

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

shutdown

	shutdown **no shutdown** Disables the interface. The no form of the command enables the interface.
Syntax Description	N/A
Default	The interface is enabled.
Configuration Mode	config interface ib
History	3.1.0000
Role	admin
Example	`switch (config interface ib 1/1) # shutdown` `switch (config interface ib 1/1) #`
Related Commands	show interfaces ib
Notes	N/A

description

description <string>

Sets an interface description.

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

speed

speed <port speed> [force]

Sets the speed negotiation of the interface.

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

op-vls

op-vls <value>

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

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

width

	width <value> **no width** Sets the width of the interface. The no form of the command resets the parameter to its default value.	
Syntax Description	value	Possible value for width: • 1 – 1X • 5 – 1X, 4X
Default	5 (1X, 4X)	
Configuration Mode	config interface ib	
History	3.1.0000	
	3.6.5000	Added “no” option
Role	admin	
Example	`switch (config interface ib 1/1) # width 1` `switch (config interface ib 1/1) #`	
Related Commands	show interfaces ib	
Notes		

clear counters

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

interface ib internal notification link-speed-mismatch

interface ib internal notification link-speed-mismatch [<time>]
no interface ib internal notification link-speed-mismatch

Enables notifications on internal link speed mismatch in SNMP.
The no form of the command disables notifications on internal inks speed mismatch in SNMP.

Syntax Description	time	Enables periodic notifications (traps and log) on internal link speed mismatch status. The time is in hours. "0" disables the feature
Default	Disabled	
Configuration Mode	config	
History	3.4.3000	
Role	admin	

Example	`switch (config) # interface ib internal link-speed-mismatch 6`
	`switch (config) # show interfaces ib internal notification`
	`========================`
	`Internal links information`
	`========================`
	`State change enabled     :    no`
	`Speed mismatch enabled   :    yes`
	`Periodic notifications   :    6 (hours)`	

Related Commands	show interfaces ib internal notification	
Notes	Link-speed-mismatch shows internal link entries in the ifVPITable.	

interfaces ib internal notification link-state-change

	interfaces ib internal notification link-state-change **no interfaces ib internal notification link-state-change** Enables notifications on internal links state change in SNMP. The no form of the command disables notifications on internal links state change in SNMP.
Syntax Description	N/A
Default	Disabled
Configuration Mode	config
History	3.3.4318 3.3.4550 Added note
Role	admin
Example	`switch [master] (config) # interfaces ib internal notification` `switch [master] (config) #`
Related Commands	show interfaces ib internal notification
Notes	Link-state-change shows internal link entries in the ifTable and the ifXTable

switchport access subnet

switchport access subnet <swid-name> [force]
no switchport access subnet <swid-name> [force]

Maps interface to SWID.
The no form of the command unmaps an interface from a SWID.

Syntax Description	swid-name	Name of the SWID: infinibad-default, infiniband-1…infinibad-5
	force	Forces configuration (no need to shutdown interface before running command)
Default	Unmapped	
Configuration Mode	config interface ib	
History	3.6.0500	
Role	admin	
Example	`switch (config interface ib1/36) # switchport access subnet infiniband-1`	
Related Commands		
Notes	• Mapping an interface automatically enables it • Remapping an interface resets all its configuration except for interface description • Unmapping an interface resets all its configuration except for interface description • An interface needs to be disabled before remapping/unmapping unless the “force” parameter is used	

show interfaces ib

show interfaces ib <inf>

Displays the configuration and status for the interface.

Syntax Description	internal	Internal interfaces.
	inf	• Slot/Port (i.e. 1/1) • LXX/SXX (i.1 L01 or S01)
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.0000	
	3.4.1604	Updated Example
	3.6.1002	Updated Example
	3.6.6105	Updated Example
Role	admin	
Example		

```
switch (config) # show interfaces ib 1/36
IB1/36 state:
        Logical port state           : Active
        Physical port state          : LinkUp
        Current line rate            : 10.0 Gbps
        Supported speeds             : sdr
        Speed                        : sdr
        Supported widths             : 1X, 4X
        Width                        : 4X
        Max supported MTUs           : 4096
        MTU                          : 4096
        VL capabilities              : VL0 - VL7
        Operational VLs              : VL0 - VL7
        Description                  : Test
        IB Subnet                    : infiniband-default
        Phy-profile                  : high-speed-ber
        Width reduction mode         : Not supported

        RX bytes                     : 33258342076
        RX packets                   : 16231513
        RX errors                    : 0
        Symbol errors                : 0
        VL15 dropped packets         : 0

        TX bytes                     : 34313606888
        TX packets                   : 16046018
```

Related Commands	
Notes	

show interfaces ib capabilities

show interfaces ib <inf> capabilities

Shows interface capabilities.

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

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

Related Commands		
Notes		

show interfaces ib status

show interfaces ib [<inf>] status

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

Syntax Description	internal	Internal interfaces
	leaf-ports	filter to leaf-ports only
	inf	Interface number: <slot>/<port>
Default	N/A	
Configuration Mode	Any command mode	
History	3.2.0500	
	3.4.1604	Updated Example
	3.6.1002	Updated Example
Role	admin	
Example	`switch (config) # show interfaces ib status`	
Related Commands		
Notes		

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

show interfaces ib internal

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

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

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

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

Related Commands	
Notes	

show interfaces ib internal capabilities

	show interfaces ib internal [leaf | spine] [<slot/module/port>] capabilities Displays capabilities of internal leaf or spine interfaces.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.2.0500
Role	admin

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

Related Commands	
Notes	

show interfaces ib internal llr

	show interfaces ib internal [leaf | spine] [<slot/module/port>] llr Displays LLR state of internal leaf or spine interfaces.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.2.0500 3.6.6000 Updated Example
Role	admin

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

Related Commands	
Notes	

show interfaces ib internal status

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

Displays detailed running state of internal leaf or spine interfaces.

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

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

Related Commands	
Notes	

show interfaces ib transceiver

show interfaces ib [<inf>] transceiver

Displays the transceiver info.

Syntax Description	inf	interface number: <slot>/<port>
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show interfaces ib 1/1 transceiver`
	`IB1/1 state`
	`identifier : QSFP+`
	`cable/module type : Passive copper, unequalized`
	`infiniband speeds : SDR , DDR , QDR`
	`vendor : Mellanox`
	`cable length : 2 m`
	`part number : MC2207130-002`
	`revision : B0`
	`serial number : AA051150077`
	`switch (config) #`	

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

show interfaces ib transceiver diagnostics

show interfaces ib [<inf>] transceiver diagnostics

Displays cable channel monitoring and diagnostics info for this interface.

Syntax Description	inf	Interface number: <slot>/<port>
Default	N/A	
Configuration Mode	Any command mode	
History	3.6.2002	
	3.6.6000	Updated Example
Role	admin	
Example		

```
switch (config) # show interfaces ib transceiver diagnostics

IB1/1 Transceiver Diagnostic Data:
  Message: No Diagnostic Data Available. Module is not DDMI capable

IB1/3 Transceiver Diagnostic Data:
  Message: Non present module

IB1/5 Transceiver Diagnostic Data:
  Temperature (-127C to +127C):
    Temperature          : 28 C
    Hi Temp Alarm Thresh : 80 C
    Low Temp Alarm Thresh: -10 C
    Temperature Alarm    : None

  Voltage (0 to 6.5535 V):
    Voltage              : 3.28980 V
    Hi Volt Alarm Thresh : 3.50000 V
    Low Volt Alarm Thresh: 3.10000 V
    Voltage Alarm        : None

  Tx Bias Current (0 to 131 mA):
    Ch1 Tx Current          : 6.60000 mA
    Ch2 Tx Current          : 6.60000 mA
    Ch3 Tx Current          : 6.60000 mA
    Ch4 Tx Current          : 6.60000 mA
    Hi Tx Crnt Alarm Thresh : 8.50000 mA
    Low Tx Crnt Alarm Thresh: 5.49200 mA
    Ch1 Tx Current Alarm    : None
    Ch2 Tx Current Alarm    : None
    Ch3 Tx Current Alarm    : None
    Ch4 Tx Current Alarm    : None
```

```
Tx Power (0 mW to 6.5535 mW / 8.1647 dBm):
  Ch1 Tx Power             : 1.01170 mW / 0.05052 dBm
  Ch2 Tx Power             : 0.96240 mW / -0.16644 dBm
  Ch3 Tx Power             : 0.95980 mW / -0.17819 dBm
  Ch4 Tx Power             : 0.95800 mW / -0.18634 dBm
  Hi Tx Power Alarm Thresh : 3.46730 mW / 5.39991 dBm
  Low Tx Power Alarm Thresh: 0.07240 mW / -11.40261 dBm
  Ch1 Tx Power Alarm       : None
  Ch2 Tx Power Alarm       : None
  Ch3 Tx Power Alarm       : None
  Ch4 Tx Power Alarm       : None

Rx Power (0 mW to 6.5535 mW / 8.1647 dBm):
  Ch1 Rx Power             : 0.99160 mW / -0.03663 dBm
  Ch2 Rx Power             : 1.08800 mW / 0.36629 dBm
  Ch3 Rx Power             : 1.09810 mW / 0.40642 dBm
  Ch4 Rx Power             : 0.97500 mW / -0.10995 dBm
  Hi Rx Power Alarm Thresh : 3.46730 mW / 5.39991 dBm
  Low Rx Power Alarm Thresh: 0.04670 mW / -13.30683 dBm
  Ch1 Rx Power Alarm       : None
  Ch2 Rx Power Alarm       : None
  Ch3 Rx Power Alarm       : None
  Ch4 Rx Power Alarm       : None

Vendor Date Code (dd-mm-yyyy): 07-11-2016
```

Related Commands

Note This example is for a QSFP transceiver

show interfaces ib transceiver raw

show interfaces ib [<inf>] transceiver raw

Displays cable info for this interface.

Syntax Description	inf	interface number: <slot>/<port>
Default	N/A	
Configuration Mode	Any command mode	
History	3.6.1002	
Role	admin	
Example		

```
switch (config) # show interfaces ib 1/7 transceiver raw
IB1/7 raw transceiver data:

I2C Address 0x50, Page 0, 0:255:
  0000  0d 02 06 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  0080  0d 00 23 08 00 00 00 00 00 00 00 05 8d 00 00 00  ..#.............
  0090  00 00 01 a0 4d 65 6c 6c 61 6e 6f 78 20 20 20 20  ....Mellanox
  00a0  20 20 20 20 0f 00 02 c9 4d 43 32 32 30 37 31 33  ....MC220713
  00b0  30 2d 30 30 41 20 20 20 41 33 02 03 05 00 46 66  0-00A   A3....Ff
  00c0  00 00 00 00 4d 54 31 32 32 37 56 53 30 30 36 34  ....MT1227VS0064
  00d0  32 20 20 20 31 32 30 37 30 38 20 20 00 00 00 e4  2   120708  ....
  00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  00f0  00 00 00 00 00 00 00 00 00 00 02 00 00 30 00 00
I2C Address 0x50, Pages 1, 128:255:
  0080  0d 02 06 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
...
```

Related Commands	
Notes	

5.5 Subnet Manager (SM)

The InfiniBand Subnet Manager (SM) is a centralized entity running in the switch. The SM discovers and configures all the InfiniBand fabric devices to enable traffic flow between those devices.

The SM applies network traffic related configurations such as Quality of Service (QoS), routing, and partitioning of the fabric devices. You can view and configure the Subnet Parameters (SM) via the CLI/WebUI menu. The embedded SM on the MLNX-OS can be used to manage fabrics up to 2048 nodes on x86 based systems.

The SM is used to discover and configure all the InfiniBand fabric devices to enable traffic flow between those devices.

➢ ***To enable Subnet Manager:***

Step 1. Enable Subnet Manager (disabled by default). Run:

```
switch (config) # ib smnode my-sm enable
```

Step 2. (Optional) Set the priority for the Subnet Manager. Run:

```
switch (config) # ib smnode my-sm sm-priority <priority>
```

5.5.1 Partitions

Partitioning enforces isolation among systems sharing an InfiniBand fabric. Partitioning is not related to boundaries established by subnets, switches, or routers. Rather, a partition describes a set of end nodes within the fabric that may communicate. Each port of an end node is a member of at least one partition and may be a member of multiple partitions. A partition manager (part of the SM) assigns partition keys (PKEYs) to each channel adapter port. Each PKEY represents a partition. Reception of an invalid PKEY causes the packet to be discarded. Switches and routers may optionally be used to enforce partitioning. In this case the partition manager programs the switch or router with PKEY information and when the switch or router detects a packet with an invalid PKEY, it discards the packet.

Fabric administration can assign certain Service Levels (SLs) for particular partitions. This allows the SM to isolate traffic flows between those partitions, and even if both partitions operate at the same QoS level, each partition can be guaranteed its fair share of bandwidth regardless of whether nodes in other partitions misbehave or are over subscribed.

The switch enables the configuration of partitions in an InfiniBand fabric.

The default partition is created by the SM unconditionally (whether it was defined or not).

5.5.1.1 Relationship with ib0 Interface

IP interface “ib0” is running under the default PKEY (0x7fff) and can be used for in-band management connectivity to the system.

5.5.1.2 Configuring Partition

The partitions configuration is applicable and to be used only when the SM is enabled and running on the system.

➢ ***To configure a partition:***

Step 1. Create a partition. Run:

```
switch (config) # ib partition my-partition pkey 0x7ff2
```

Step 2. Enter partition configuration mode. Run:

```
switch (config) # partition my-partition
switch (config partition name my-partition) #
```

Step 3. Add partition members. Run:

```
switch (config partition my-partition) # member all
```

Step 4. Verify the partition configuration. Run:

```
switch (config partition my-partition) # show ib partition
Default
    PKey      = 0x7FFF
    defmember = full
    ipoib     = yes
  members
    GUID='ALL' member='full'
  my-partition
    PKey      = 0x7ff2
  members
    GUID='ALL' member='default'
switch (config partition name my-partition) #
```

5.5.2 Adaptive Routing

Adaptive routing (AR) allows optimizing data traffic flow. The InfiniBand protocol uses multiple paths between any two points. Thus, when unexpected traffic patterns cause some paths to be overloaded, AR can automatically move traffic to less congested paths according to the current temporal state of the network.

The embedded SM over the switch does not support configuring adaptive routing. To use this option in the fabric please use an external SM.

AR support is enabled by default on system profile “ib-single-switch”. To disable AR run either the command “system profile ib-no-adaptive-routing-single-switch” or “system profile ib” with no-adaptive-routing parameter.

The AR option needs to be enabled in the SM for it to take affect.

5.5.3 Scatter Ports

When assigning logical paths to physical links, the UpDn algorithm tries to map the same number of paths per link to maximize use of the available bandwidth. This balancing is done statically, without knowledge of actual workloads and traffic patterns. Path balancing decisions are made locally, at each switch, without assuming anything about the physical topology. The resulting path assignments may not be optimal for typical Clos/Fat Tree workloads.

A routing option called “scatter-ports” is available for MinHop and UpDn routing engines which instructs the routing algorithm to randomize the local assignments of paths to links, which often results in better link utilization. The scatter-ports option requires an integer argument, which is the seed for the random number generator. It is recommended to use a prime number for the seed; a seed of zero turns off randomization.

5.5.4 GUID Routing Order

GUID routing order list allows managing the order in which the SM processes the destination LIDs in the calculations of output port as part of MinHop or Up/Down routing algorithms only.

The order of GUID appearance is important as destinations corresponding to GUIDs appearing earlier in the routing list get precedence during the routing calculations over other destinations in the fabric. This can improve load balancing towards a specific set of end ports (e.g. storage nodes or other service nodes requiring high throughput).

If scatter-ports (randomization of the output port) option is set to non-zero, guid-routing-order-no-scatter defines whether or not a randomization should be applied to the destinations GUIDs mentioned in GUID routing order list.

5.5.5 Bulk Update Mode

Bulk update mode allows users to set multiple IB SM configurations without applying them until bulk mode is disabled.

When bulk update is disabled (default situation) every SM configuration is applied immediately. When bulk is enabled, all SM configuration is saved internally and is not applied until this mode is disabled.

Bulk mode is a non-persistent state. That is, if the switch is restarted, it boots up with this mode disabled, and all the configuration changes which are saved before system restart are applied.

Show commands convey every configuration change even if it is not applied yet.

5.5.6 Commands

5.5.6.1 Subnet Manager (SM)

ib sm

	ib sm **no ib sm** Enables the SM on this node. The no form of the command disables the SM on this node.
Syntax Description	N/A
Default	disable
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # ib sm` `switch (config) #`
Related Commands	show ib sm
Notes	

ib sm accum-log-file

	ib sm accum-log-file **no ib sm accum-log-file** Adds SM log entries at the end of the current log. The no form of the command overwrites SM log file on every restart.
Syntax Description	N/A
Default	Enabled
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm accum-log-file`
	`switch (config) # show ib sm accum-log-file`
	`enable`
	`switch (config) #`

Related Commands	show ib sm accum-log-file
Notes	

ib sm allow-both-pkeys

	ib sm allow-both-pkeys **no ib sm allow-both-pkeys** Enables having both full and limited membership on the same partition. The no form of the command disables having both full and limited membership on the same partition.
Syntax Description	N/A
Default	Disabled
Configuration Mode	config
History	3.4.1100
Role	admin
Example	`switch (config) # ib sm allow-both-pkeys` `switch (config) #`
Related Commands	defmember member
Notes	

ib sm babbling-policy

	ib sm babbling-policy **no ib sm babbling-policy** Enables the SM to disable babbling ports (i.e., generating frequent traps). The no form of the command disables the SM babbling policy.
Syntax Description	N/A
Default	disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # no ib sm babbling-policy`
	`switch (config) # show ib sm babbling-policy`
	`disable`
	`switch (config) #`

Related Commands	show ib sm babbling-policy
Notes	In case the babbling policy is enabled, and decides to close a babbling interface (one which sends 129,130,131 traps, for example), the SM disables the port.

ib sm connect-roots

	ib sm connect-roots **no ib sm connect-roots** Forces the routing engine to make connectivity between root switches. The no form of the command disables logical LID path between root switches.
Syntax Description	N/A
Default	true
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm connect-roots`
	`switch (config) # show ib sm connect-roots`
	`true`
	`switch (config) #`

Related Commands	show ib sm connect-roots
Notes	• This command is relevant only for ‘updn’ and ‘ftree’ algorithm (refer to ‘ib sm routing-engines’ command) • This option enforces routing engines (up/down and fat-tree) to make connectivity between root switches and in this way to be fully IBA complaint. This may violate the “deadlock-free” status of the algorithm. Hence, it is recommended to use the command carefully.

ib sm drop-event-subscription

	ib sm drop-event-subscription **no ib sm drop-event-subscription** Configures IB SM to drop interface subscribe or unsubscribe events. The no form of the command resets this parameter to its default value.
Syntax Description	N/A
Default	IB SM does not drop interface subscribe or unsubscribe events
Configuration Mode	config
History	3.4.2008
Role	admin
Example	`switch (config) # ib sm drop-event-subscription` `switch (config) #`
Related Commands	
Notes	

ib sm enable-quirks

	ib sm enable-quirks **no ib sm enable-quirks** Enables the SM to use high risk features and handle hardware workarounds. The no form of the command disables the SM from using high risk features and hardware workarounds.
Syntax Description	N/A
Default	disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm enable-quirks`
	`switch (config) # show ib sm enable-quirks`
	`enable`
	`switch (config) #`

Related Commands	show ib sm enable-quirks
Notes	

ib sm exit-on-fatal

	ib sm exit-on-fatal **no ib sm exit-on-fatal** Enables the SM to exit upon fatal initialization errors. The no form of the command disables the SM from exiting upon fatal initialization errors.
Syntax Description	N/A
Default	enable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm exit-on-fatal`
	`switch (config) # show ib sm exit-on-fatal`
	`enable`
	`switch (config) #`

Related Commands	show ib sm exit-on-fatal
Notes	

ib sm force-link-speed

ib sm force-link-speed <speed-options>
no ib sm force-link-speed

Defines the SM behavior for PortInfo:LinkSpeedEnabled, PortInfo:LinkSpeedExtEnabled and MLNX ExtendedPortInfo on the switch ports.

Syntax Description	speed-options	The following options are available: • sdr – 10.0 Gb/s rate on 4 lane width • ddr – 20.0 Gb/s rate on 4 lane width • qdr – 40.0 Gb/s rate on 4 lane width • fdr10 – 40.0 Gb/s rate on 4 lane width • fdr – 56.0 Gb/s rate on 4 lane width • edr – 100.0 Gb/s rate on 4 lane width
Default	Set to PortInfo:LinkSpeedExtSupported	
Configuration Mode	config	
History	3.1.0000	
	3.4.1604	Updated Syntax Description, Example and Notess
Role	admin	
Example	`switch (config) # ib sm force-link-speed sdr ddr qdr fdr10` `switch (config) #`	
Related Commands	show ib sm force-link-speed show ib sm force-link-speed-ext show ib sm fdr10	
Notes	• The following options, as defined in *InfiniBand Specification 1.2.1* section 14.2.5.6, table 145 “PortInfo” • This command updates force-link-speed, force-link-speed ext and fdr10 which are open sm parameters • This command is backwards compatible so old configuration file containing this command with the old form (with legal bit mask) are still supported • If the speed-options list does not include SDR speed, it is configured automatically • Configuring more than one speed is possible by typing in consecutive speed names separated by spaces	

ib sm force-log-flush

	ib sm force-log-flush **no ib sm force-log-flush** Forces every log message generated to be flushed. The no form of the command does not force a flush after every log write.
Syntax Description	N/A
Default	disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm force-log-flush`
	`switch (config) # show ib sm force-log-flush`
	`enable`
	`switch (config) #`

Related Commands	show ib sm force-log-flush
Notes	

ib sm guid2lid-cache

	ib sm guid2lid-cache **no ib sm guid2lid-cache** Allows SM to use cached GUID-to-lid mapping data. When enabled, the SM honors the cached GUID-to-lid mapping information if: • It exists • It is valid • sm_reassign_lids is disabled The no form of the command disallows use of cached GUID-to-lid mapping data.
Syntax Description	N/A
Default	disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm guid2lid-cache`
	`switch (config) # show ib sm guid2lid-cache`
	`enable`
	`switch (config) #`

Related Commands	show ib sm guid2lid-cache
Notes	

ib sm honor-partitions

	ib sm honor-partitions **no ib sm honor-partitions** Sets the no_partition_enforcement flag to 0. This setting controls global support for partitioning in the subnet. The no form of the command disables subnet partition support.
Syntax Description	N/A
Default	Enable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # no ib sm honor-partitions`
	`switch (config) # show ib sm honor-partitions`
	`disable`
	`switch (config) #`

Related Commands	show ib sm honor-partitions
Notes	• If partitioning is disabled (no_partition_enforcement=1), then no named partitions can be enabled • If partitioning is enabled globally, the no_partition_enforcement changes from 1 to 0, and all defined partitions with state enabled are instantiated • If partitioning is globally disabled, all partitions are removed from the subnet, but the state (enabled or disabled) associated with defined partitions is not modified

ib sm hoq-lifetime

ib sm hoq-lifetime <time>

Sets the maximum time a frame can wait at the head of a switch-to-switch port queue before it is dropped.

Syntax Description	time	The time is 4.096 uS * 2time. The range of time is 0 to 20. A time of 20 means infinite, and the default value is 18 which translates to about 1 second.
Default	0x12 (~ 1 second)	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm hoq-lifetime 15`
	`switch (config) # show ib sm hoq-lifetime`
	`0xF (About 134 mS)`
	`switch (config) #`	

Related Commands	show ib sm hoq-lifetime	
Notes		

ib sm ignore-other-sm

	ib sm ignore-other-sm **no ib sm ignore-other-sm** Ignores all the rules governing SM elections and attempts to manage the fabric. The no form of the command does not allow the SM to manage fabric if it loses the election.
Syntax Description	N/A
Default	Disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm ignore-other-sm`
	`switch (config) # show ib sm ignore-other-sm`
	`enable`
	`switch (config) #`

Related Commands	show ib sm ignore-other-sm
Notes	

ib sm ipv6-nsm

	ib sm ipv6-nsm **no ib sm ipv6-nsm** Consolidates IPv6 SNM group joins to 1 MC group per-MGID PKEY. The no form of the command disables the consolidation of IPv6 SNM.
Syntax Description	N/A
Default	Disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm ipv6-nsm`
	`switch (config) # show ib sm ipv6-nsm`
	`enable`
	`switch (config) #`

Related Commands	show ib sm ipv6-nsm
Notes	

ib sm lash

ib sm lash {do-mesh-analysis | start-vl <vl-value>}
no ib sm lash do-mesh-analysis

Modifies “lash” routing method parameters.
The no form of the command disables SM “lash” routing for mesh analysis.

Syntax Description	do-mesh-analysis	Enables SM “lash” routing for mesh analysis.
	start-vl <vl-value>	Configures the starting VL for SM “lash” routing for mesh analysis (assuming that lash routing is enabled)
Default	do-mesh-analysis: disable start-vl: 0	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm lash do-mesh-analysis`
	`switch (config) # show ib sm lash do-mesh-analysis`
	`enable`
	`switch (config) #`	

Related Commands	show ib sm lash do-mesh-analysis	
Notes		

ib sm leafhoq-lifetime

ib sm leafhoq-lifetime <time>

Sets the maximum time a frame can wait at the head of a switch-to-CA_or_Router port queue before it is dropped.

Syntax Description	time	The time is 4.096 uS * 2time. The range of time is 0 to 20. A time of 20 means infinite, and the default value is 16 which translates to about 268 millisecond.
Default	0x10 (about 268 mS)	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm leafhoq-lifetime 8`
	`switch (config) # show ib sm leafhoq-lifetime`
	`0x8 (About 1 mS)`
	`switch (config) #`	

Related Commands	show ib sm leafhoq-lifetime	
Notes		

ib sm leafvl-stalls

ib sm leafvl-stalls <count>

Sets the number of sequential frame drops that cause a switch-to-CA_or_Router port to enter the VLStalled state.

Syntax Description	count	1-255
Default	7	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm leafvl-stalls 3`
	`switch (config) # show ib sm leafvl-stalls`
	`3`
	`switch (config) #`	

Related Commands	show ib sm leafvl-stalls	
Notes		

ib sm lmc

ib sm lmc <mask>

Sets the LID Mask Control (LMC) value to be used on this subnet.

Syntax Description	mask	Valid values are 0-7.
Default	The default value is 0, which means that every port has exactly one unique LID.	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm lmc 7`
	`switch (config) # show ib sm lmc`
	`0x7`
	`switch (config) #`	

Related Commands	show ib sm lmc	
Notes		

ib sm lmc-esp0

	ib sm lmc-esp0 **no ib sm lmc-esp0** Sets the LMC for the subnet to be used for Enhanced Switch Port 0.
Syntax Description	N/A
Default	disable
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # ib sm lmc-esp0` `switch (config) #`
Related Commands	show ib sm lmc-esp0
Notes	

ib sm log-flags

ib sm log-flags [all] [debug] [error] [frames] [funcs] [info] [none] [routing] [verbose]
no ib sm log-flags

Controls what messages the SM logs.
The no form of the command indicates to the SM not to run on this node.

Syntax Description	all	Turns on all the flags that follow (error info verbose debug funcs frames routing).
	debug	Logs diagnostic messages, high volume.
	error	Logs error messages.
	frames	Logs all SMP and GMP frames.
	funcs	Logs function entry/exit, very high volume.
	info	Logs basic messages, low volume.
	none	Turns off all logging flags.
	routing	Logs FDB routing information.
	verbose	Logs interesting stuff, moderate volume.
Default	0x3 (error, info)	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm log-flags error verbose funcs frames`
	`switch (config) # show ib sm log-flags`
	`0x35 (error, verbose, funcs, frames)`
	`switch (config) #`	

Related Commands	show ib sm log-flags	
Notes	• Every execution of this command replaces the current logging flags • The options “all” and “none” must be specified as the only parameter	

ib sm log-max-size

ib sm log-max-size <size>

Sets the maximum size of the log file to be <size> megabytes.

Syntax Description	size	Range: 1-60
Default	20 MBytes	
Configuration Mode	config	
History	3.1.0000	
	3.5.1000	Updated Syntax Description, and Default
Role	admin	

Example	`switch (config) # ib sm log-max-size 50`
	`switch (config) # show ib sm log-max-size`
	`50 MBytes`
	`switch (config) #`	

Related Commands	show ib sm log-max-size	
Notes	• The log file “opensm_<switch_name>.log” is rotated when it exceeds the configured maximum file size up to 5 compressed files • When the log gets to the maximum size, or system storage fills up, the current log is deleted and messages start accumulating • To successfully upgrade from a version prior to 3.5.1000, this parameter must be set to a value in the range specified in the syntax description	

ib sm m-key

ib sm m-key <m-key>

Sets the MKey used by SM.

Syntax Description	m-key	64-bit MKey.
Default	00:00:00:00:00:00:00:00	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm m-key 00:00:00:00:00:00:00:05`
	`switch (config) # show ib sm m-key`
	`00:00:00:00:00:00:00:05`
	`switch (config) #`	

Related Commands	show ib sm m-key	
Notes		

ib sm max-op-vls

ib sm max-op-vls <count>

Sets the maximum number of VLs supported on this subnet.

Syntax Description	count	Possible values: 1, 2, 4, 8, or 15.
Default	15	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm max-op-vls 4`
	`switch (config) # show ib sm max-op-vls`
	`4`
	`switch (config) #`	

Related Commands	show ib sm max-op-vls	
Notes		

ib sm max-reply-time

ib sm max-reply-time <time>

Sets the maximum time the SM waits for a reply before the transaction times out.

Syntax Description	time	Must be an integer (in milliseconds).
Default	200 milliseconds	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm max-reply-time 500`
	`switch (config) # show ib sm max-reply-time`
	`500 milliseconds`
	`switch (config) #`	

Related Commands	show sm max-reply-time	
Notes		

ib sm max-reverse-hops

ib sm max-reverse-hops <max-reverse-hops>

Sets the maximum number of hops from the top switch to an I/O node.

Syntax Description	N/A
Default	0 hops
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm max-reverse-hops 500`
	`switch (config) # show ib sm max-reverse-hops`
	`500 hops`
	`switch (config) #`

Related Commands	show ib sm max-reverse-hops
Notes	

ib sm max-reverse-hops

ib sm max-reverse-hops <max-reverse-hops>

Sets the maximum number of hops from the top switch to an I/O node.

Syntax Description	N/A
Default	0 hops
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm max-reverse-hops 500`
	`switch (config) # show ib sm max-reverse-hops`
	`500 hops`
	`switch (config) #`

Related Commands	show ib sm max-reverse-hops
Notes	

ib sm aguid_default_hop_limit

ib sm aguid_default_hop_limit <count>
no ib sm aguid_default_hop_limit

Configures the default value for hop limit returned in path records where either the source or destination are alias an GUID.
The no form of the command resets the count to its default value.

Syntax Description	count	Number of concurrent management packets (must be an integer)
Default	1	
Configuration Mode	config	
History	3.6.6102	
Role	admin	
Example	`switch (config) # ib sm aguid-default-hop-limit 3`	
Related Commands	show ib sm aguid-default-hop-limit	
Notes		

ib sm max-wire-smps2

ib sm max-wire-smps2 <count>

Sets the maximal timeout based outstanding SM management packets.

Syntax Description	count	Number of concurrent management packets. The value must be an integer.
Default	4	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm max-wire-smps 8`
	`switch (config) # show ib sm max-wire-smps`
	`8`
	`switch (config) #`	

Related Commands	show ib sm max-wire-smps2	
Notes		

ib sm m-key

ib sm m-key <mkey>
no ib sm m-key

Configures the MKey used by the SM.
The no form of the command resets the MKey configuration to its default value.

Syntax Description	mkey	64-bit MKey
Default	00:00:00:00:00:00:00:00	
Configuration Mode	config	
History	3.1.0000	
	3.6.2002	Added no form of the command
	3.7.00xx	Added note
Role	admin	
Example	`switch (config) # ib sm m-key 11:33:55:77:99:aa:cc:ee`	
Related Commands	ib sm mkey-lease ib sm mkey-lookup ib sm mkey-protect-level show ib sm m-key show ib sm mkey-lease	
Notes	• All nodes in the subnet may have to be reset or power-cycled after altering the SM MKey configuration • Fabric inspector, and many standalone InfiniBand utilities, may not function on subnets with a non-default MKey.	

ib sm mkey-lease

ib sm mkey-lease <time>
no ib sm mkey-lease

Configures the lease period used when MKey is non-zero.
The no form of the command resets this value to its default.

Syntax Description	time	MKey lease period in seconds Range: 0-65535; 0=unlimited
Default	0	
Configuration Mode	config	
History	3.6.2002	
Role	admin	
Example	`switch (config) # ib sm mkey-lease 660`	
Related Commands	`show ib sm mkey-lease`	
Notes		

ib sm mkey-lookup

	ib sm mkey-lookup **no ib sm mkey-lookup** Enables using a file cache (guid2mkey) to resolve unknown node MKey. The no form of the command disables using a file cache to resolve unknown node MKey and the configured MKey is used for all ports.
Syntax Description	N/A
Default	Enabled
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # ib sm mkey-lookup`
Related Commands	`show ib sm mkey-lookup`
Notes	MKey lookup is a boolean value that controls how the SM finds the MKey of ports.

ib sm mkey-protect-level

ib sm mkey-protect-level <level>
no ib sm mkey-protect-level

Controls what data is returned to a get_PortInfo MAD request when the MKey in the request does not match the MKey on the port.
The no form of the command resets the parameter to its default value.

Syntax Description	level	• 0 – when PortInfo is “read”, the actual MKey is returned in port info data • 1 – when PortInfo is “read”, and the MKey in the MAD does not match the MKey on the port, the MKey value in the returned PortInfo data is set to 0. • 2 – when PortInfo is “read”, and the MKey in the MAD does not match the MKey on the port, no data is returned.
Default	0	
Configuration Mode	config	
History	3.6.2002	
Role	admin	
Example	`switch (config) # ib sm mkey-protect-level 0`	
Related Commands	`show ib sm mkey-protect-level`	
Notes		

ib sm msgfifo-timeout

ib sm msgfifo-timeout <time>

Sets the time value to be used by the subnet administrator to control when a BUSY status is returned to a client.

Syntax Description	time	In milliseconds.
Default	10 seconds	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm msgfifo-timeout 50000`
	`switch (config) # show ib sm msgfifo-timeout`
	`50.000 seconds`
	`switch (config) #`	

Related Commands	`show ib sm msgfifo-timeout`	
Notes	If there is more than one message in the SA queue, and it has been there longer than time milliseconds, all additional incoming requests are immediately replied to with BUSY status.	

ib sm multicast

	ib sm multicast **no ib sm multicast** Enables the SM to support multicasts on the fabric. The no form of the command disables the SM from supporting multicasts on the fabric.
Syntax Description	N/A
Default	Disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm multicast`
	`switch (config) # show ib sm multicast`
	`enable`
	`switch (config) #`

Related Commands	show ib sm multicast
Notes	

ib sm no-client-rereg

	ib sm no-client-rereg **no ib sm no-client-rereg** Enables client re-registration requests. The no form of the command disables client re-registration requests.
Syntax Description	N/A
Default	disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm no-client-rereg`
	`switch (config) # show ib sm no-client-rereg`
	`enable`
	`switch (config) #`

Related Commands	show ib sm no-client-rereg
Notes	

ib sm overrun-trigger

ib sm overrun-trigger <count>

Enables SMA to generate standard InfiniBand trap number 130 when the number of local buffer overrun errors equals the count value, and the port's SMA supports traps.

Syntax Description	count	Range: 0-255.
Default	8	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm overrun-trigger 3`
	`switch (config) # show ib sm overrun-trigger`
	`3`
	`switch (config) #`	

Related Commands	show ib sm overrun-trigger	
Notes	Refer to the *InfiniBand Architecture Specification V1 r1.2.1*, section 14.2.5.1 table 131: Traps.	

ib sm packet-life-time

ib sm packet-life-time <time>

Sets the maximum time a frame can live in a switch.

Syntax Description	time	The time is 4.096 uS * 2*<time>. The rang is: 0-20. A time of 20 means infinite. The value 0x14 disables this mechanism.
Default	0x12 (about 1 second)	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm packet-life-time 20`
	`switch (config) # show ib sm packet-life-time`
	`0x14 (Infinite)`
	`switch (config) #`	

Related Commands	show ib sm packet-life-time	
Notes		

ib sm phy-err-trigger

ib sm phy-err-trigger <count>

Enables SMA to generate trap 129 when the number of local link integrity errors equals the <count> value, and the port's SMA supports traps.

Syntax Description	count	Range is: 0-255.
Default	8	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm phy-err-trigger 5`
	`switch (config) # show ib sm phy-err-trigger`
	`5`
	`switch (config) #`	

Related Commands	show ib sm phy-err-trigger	
Notes		

ib sm polling-retries

ib sm polling-retries <value>

This variable defines the number of consecutive times an active SM must fail to respond before it is declared dead.

Syntax Description	value	Must be an integer.
Default	4	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm polling-retries 8`
	`switch (config) # show ib sm polling-retries`
	`8`
	`switch (config) #`	

Related Commands	show ib sm polling-retries	
Notes	The time between when the active SM fails and the time this SM declares it dead is: (sm_sminfo_polling_timeout * value) milliseconds.	

ib sm port-prof-switch

	ib sm port-prof-switch **no ib sm port-prof-switch** Enables the counting of adapters, routers, and switches routed through links. The no form of the command disables the counting of adapters, routers, and switches routed through links.
Syntax Description	N/A
Default	False
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm port-prof-switch`
	`switch (config) # show ib sm port-prof-switch`
	`true`
	`switch (config) #`

Related Commands	show ib sm port-prof-switch
Notes	

ib sm reassign-lids

	ib sm reassign-lids **no ib sm reassign-lids** Controls the ability of the SM to reassign LIDs to nodes it finds already configured with a valid LID. The no form of the command disables the SM from reassigning LIDs to nodes it finds already configured with a valid LID.
Syntax Description	N/A
Default	disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm reassign-lids`
	`switch (config) # show ib sm reassign-lids`
	`enable`
	`switch (config) #`

Related Commands	show ib sm reassign-lids
Notes	• If enabled (ib sm reassign-lids), the SM can, but is not required to, reassign the LID on a node with a pre-configured LID • If disabled (no ib sm reassign-lids), the SM does not reassign LIDs • There are times when the SM is required to reassign LIDs or the fabric cannot be brought to a stable state, or a fabric option (like LMC) can not be fully applied

ib sm reset-config

	ib sm reset-config Resets all SM configuration options to defaults.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # ib sm reset-config` `switch (config) #`
Related Commands	
Notes	

ib sm root-guid

ib sm root-guid <guid>
no ib sm root-guid <guid>

Adds a root GUID for the SM.
The no form of the command removes the GUID from the root GUID list.

Syntax Description	guid	The root GUID number in hexadecimal notation
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config)# ib sm root-guid aa:bb:00:11:22:33:44:55` `switch (config) #`	
Related Commands	show ib sm routing-engines	
Notes	The list of root GIDs are relevant when IB SM is running on the switch, and the routing algorithm is up-down or fat-tree.	

ib sm routing-engines

ib sm routing-engines [dor] [file] [ftree] [lash] [minhop] [none] [updn]
no ib sm routing-engines

Sets the routing engine of the SM.
The no form of the command sets the routing engine to be “none”. The default SM routing engine is used.

Syntax Description	dor	Includes “dor” engine in selection of routing engines
	file	Includes “file” engine in selection of routing engines
	ftree	Includes “ftree” engine in selection of routing engines
	lash	Includes “lash” engine in selection of routing engines
	minhop	Includes “minhop” engine in selection of routing engines
	none	No routing engines specified; use SM default(s)
	updn	Includes “up/down” engine in selection of routing engines
Default	None	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ib sm routing-engines none`	
Related Commands	show ib sm routing-engines	
Notes	Multiple routing engines can be specified separated by spaces so that specific ordering of routing algorithms will be tried if earlier routing engines fail.	

ib sm rtr-aguid-enable

ib sm rtr-aguid-enable <value>
sm ib sm rtr-aguid-enable <value>

Configures SM alias GUID control option.
The no form of the command resets SM alias GUID control to its default value.

Syntax Description	value	Possible values: • 0 – does not configure alias GIDs required by routers • 1 – configures alias GIDs required by routers • 2 – clears and does not configure alias GIDs required by routers
Default	0	
Configuration Mode	config	
History	3.6.2002	
Role	admin	
Example	`switch (config) # ib sm rtr-aguid-enable 1`	
Related Commands		
Notes		

ib sm rtr-pr-flow-label

ib sm rtr-pr-flow-label <value>
no ib sm rtr-pr-flow-label <value>

Configures inter-subnet PathRecord FlowLabel.
The no form of the command resets inter-subnet PathRecord FlowLabel to its default value.

Syntax Description	value	Range: 0-1048575
Default	0	
Configuration Mode	config	
History	3.6.2002	
Role	admin	
Example	`switch (config) # ib sm rtr-pr-flow-label 1`	
Related Commands		
Notes		

ib sm rtr-pr-mtu

ib sm rtr-pr-mtu <value>
no ib sm rtr-pr-mtu <value>

Configures inter-subnet PathRecord MTU.
The no form of the command resets inter-subnet PathRecord MTU to its default value.

Syntax Description	value	Possible values: 256, 512, 1K, 2K, 4K
Default	2K	
Configuration Mode	config	
History	3.6.2002	
Role	admin	
Example	`switch (config) # ib sm rtr-pr-mtu 2k`	
Related Commands		
Notes		

ib sm rtr-pr-rate

ib sm rtr-pr-rate <value>
no ib sm rtr-pr-rate <value>

Configures inter-subnet PathRecord rate.
The no form of the command resets inter-subnet PathRecord rate to its default value.

Syntax Description	value	Possible values: 2.5, 5, 10, 14, 20, 25, 40, 56, 100
Default	100	
Configuration Mode	config	
History	3.6.2002	
Role	admin	
Example	`switch (config) # ib sm rtr-pr-rate 5`	
Related Commands		
Notes		

ib sm rtr-pr-sl

ib sm rtr-pr-sl <value>
no ib sm rtr-pr-sl <value>

Configures inter-subnet PathRecord SL.
The no form of the command resets inter-subnet PathRecord SL to its default value.

Syntax Description	value	Range: [0-15]
Default	0	
Configuration Mode	config	
History	3.6.2002	
Role	admin	
Example	`switch (config) # rtr-pr-sl 0`	
Related Commands		
Notes		

ib sm rtr-pr-tclass

	ib sm rtr-pr-tclass <value> **no ib sm rtr-pr-tclass <value>** Configures inter-subnet PathRecord T-class. The no form of the command resets inter-subnet PathRecord T-class to its default value.
Syntax Description	value Range: [0-255]
Default	0
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # ib sm rtr-pr-tclass 1`
Related Commands	
Notes	

ib sm sa-key

ib sm sa-key <SA_Key>

Sets the SA_Key 64-bit value used by SA to qualify that a query is “trusted”.

Syntax Description	SA Key 64 bit
Default	00:00:00:00:00:00:00:01
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm sa-key 5`
	`switch (config) # show ib sm sa-key`
	`00:00:00:00:00:00:00:05`
	`switch (config) #`

Related Commands	show ib sm sa-key
Notes	OpenSM version 3.2.1 and lower used the default value of “1” in host byte order. You may need to change this value to inter-operate with older subnet managers.

ib sm single-thread

	ib sm single-thread **no ib sm single-thread** Enables the Subnet Manager to use a single thread to service all requests. The no form of the command enables SA to use multiple service threads.
Syntax Description	N/A
Default	Disable (use multiple service threads).
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm single-thread`
	`switch (config) # show ib sm single-thread`
	`enable`
	`switch (config) #`

Related Commands	show ib sm single-thread
Notes	

ib sm sm-inactive

	ib sm sm-inactive **no ib sm sm-inactive** Configures the SM to start in the “inactive” SM state. This option can be used to run a standalone system without the SM/SA function. The no form of the command configures the SM to start in “init” SM state.
Syntax Description	N/A
Default	Disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm sm-inactive`
	`switch (config) # show ib sm sm-inactive`
	`enable`
	`switch (config) #`

Related Commands	show ib sm sm-inactive
Notes	

ib sm sm-key

ib sm sm-key <SM_Key>

Sets the SM 64-bit SM_Key.

Syntax Description	SM Key 64 bit
Default	00:00:00:00:00:00:00:01
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm sm-key 00:00:00:00:00:00:00:05`
	`switch (config) # show ib sm sm-key`
	`00:00:00:00:00:00:00:05`
	`switch (config) #`

Related Commands	show ib sm sm-key
Notes	OpenSM version 3.2.1 and lower used the default value of "1" in host byte order. You may need to change this value to inter-operate with older subnet managers.

ib sm sm-priority

ib sm sm-priority <priority>

Prioritizes the desired SM compared to other SMs on the fabric.

Syntax Description	priority	Priority 0 is the least important, 15 the most important.
Default	0	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm sm-priority 1`
	`switch (config) # show ib sm sm-priority`
	`1`
	`switch (config) #`	

Related Commands	show ib sm sm-priority	
Notes	If two or more active SMs have the same highest priority, the one with the lowest port GUID manages the fabric.	

ib sm sm-sl

ib sm sm-sl <sm-sl>

Sets the SM service level for SM/SA communication.

Syntax Description	sm-sl	0-15.
Default	0	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm sm-sl 10`
	`switch (config) # show ib sm sm-sl`
	`10`
	`switch (config) #`	

Related Commands	show ib sm sm-sl	
Notes	Selects the SL that is used for MADs.	

ib sm sminfo-poll-time

ib sm sminfo-poll-time <time>

This variable controls the timeout between two polls of an active subnet manager.

Syntax Description	time	In milliseconds.
Default	10 seconds	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	switch (config) # ib sm sminfo-poll-time 15 switch (config) # show ib sm sminfo-poll-time 15 milliseconds switch (config) #	
Related Commands	show ib sm sminfo-poll-time	
Notes		

ib sm subnet-prefix

ib sm subnet-prefix <prefix>
no ib sm subnet-prefix <prefix>

Sets the SM "Subnet Prefix" used to create scope qualifiers for all elements managed by the SM.
The no form of the command resets the subnet prefix to its default value.

Syntax Description	prefix	64 bit
Default	FE:80:00:00:00:00:00:00	
Configuration Mode	config	
History	3.6.1002	
	3.6.2002	Added no form of the command
Role	admin	

Example	`switch (config) # ib sm subnet-prefix ff:ff:ff:ff:ff:ff:ff:00`
	`switch (config) # show ib sm subnet-prefix`
	`FF:FF:FF:FF:FF:FF:FF:00`
	`switch (config) #`	

Related Commands	show ib sm subnet-prefix	
Notes	The default value is also the InfiniBand default for a locally administered subnet.	

ib sm subnet-prefix-override

	ib sm subnet-prefix-override **no ib sm subnet-override** Disables IB Router subnet prefix checking. The no form of the command enables IB Router subnet prefix checking.
Syntax Description	N/A
Default	Enabled
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # ib sm subnet-prefix-override` `switch (config) #`
Related Commands	show ib sm subnet-prefix-override
Notes	

ib sm subnet-timeout

ib sm subnet-timeout <time>

Sets the global per-port subnet timeout value (PortInfo:SubnetTimeOut). This value also controls the maximum trap frequency in which no traps are allowed to be sent faster than the subnet_timeout value.

Syntax Description	time	The actual timeout is 4.096 uS * 2*<time>. The range of time is 0-31 for this parameter which supports 32 discrete time values between 4 uS and about 2.4 hours.
Default	0x12 (About 1 second)	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm subnet-timeout 5`
	`switch (config) # show ib sm subnet-timeout`
	`0x5 (About 131 uS)`
	`switch (config) #`	

Related Commands	show ib sm subnet-timeout	
Notes	If the SMA generates a sequence of traps, the interval between successive traps should not be smaller than <time>.	

ib sm sweep-interval

ib sm sweep-interval <time>
no ib sm sweep-interval

Specifies the time between subnet sweeps.
The no form of the command disables periodic sweeps.

Syntax Description	time	Range: Between 0 and 36000 seconds (0 - disable).
Default	10 seconds	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm sweep-interval 20`
	`switch (config) # show ib sm sweep-interval`
	`20 seconds`
	`switch (config) #`	

Related Commands	show ib sm sweep-interval	
Notes		

ib sm sweep-on-trap

	ib sm sweep-on-trap **no ib sm sweep-on-trap** Enables every TRAP received by the SM to initiate a heavy sweep in addition to the processing required by the TRAP. The no form of the command enables SM to use a combination of light and heavy sweeps based on the type of TRAP and other internal states.
Syntax Description	N/A
Default	enable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm sweep-on-trap`
	`switch (config) # show ib sm sweep-on-trap`
	`enable`
	`switch (config) #`

Related Commands	show ib sm sweep-on-trap
Notes	More than 10 successive identical TRAPs disable the automatic sweep behavior until at least one different TRAP has been received.

ib sm transaction-retries

ib sm transaction-retries <transaction-retries-count>

Sets the maximum retries for failed transactions.

Syntax Description	transaction-retries-count	Must be an integer.
Default	3	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm transaction-retries 10`
	`switch (config) # show ib sm transaction-retries`
	`10`
	`switch (config) #`	

Related Commands	show ib sm transaction-retries	
Notes		

ib sm use-heavy-sweeps

	ib sm use-heavy-sweeps **no ib sm use-heavy-sweeps** Turns every fabric sweep to a heavy sweep. The no form of the command enables the SM to use a combination of light and heavy sweeps.
Syntax Description	N/A
Default	disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm use-heavy-sweeps`
	`switch (config) # show ib sm use-heavy-sweeps`
	`enable`
	`switch (config) #`

Related Commands	show ib sm use-heavy-sweeps
Notes	

ib sm use-ucast-cache

	ib sm use-ucast-cache **no ib sm use-ucast-cache** Enables the SM to use cached routine data (LMC=0 only). The no form of the command disables the SM to use cached routine data.
Syntax Description	N/A
Default	Disable
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib sm use-ucast-cache`
	`switch (config) # show ib sm use-ucast-cache`
	`true`
	`switch (config) #`

Related Commands	show ib sm use-ucast-cache
Notes	

ib sm vl-stalls

ib sm vl-stalls <count>

Sets the number of sequential frame drops that cause a switch-to-switch port to enter the VLStalled state.

Syntax Description	count	1-255
Default	7	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib sm vl-stalls 10`
	`switch (config) # show ib sm vl-stalls`
	`10`
	`switch (config) #`	

Related Commands	show ib sm vl-stalls	
Notes		

ib sm virt

ib sm virt {enable | disable | ignore}
no ib sm virt

Configures IB SM port virtualization support.
The no form of the command resets this parameter to its default value.

Syntax Description	enable	IB SM supports virtualization, and configures virtual ports
	disable	IB SM disables virtual ports
	ignore	IB SM ignores virtual ports and does not change their configuration
Default	Ignore	
Configuration Mode	config	
History	3.4.2008	
Role	admin	
Example	`switch (config) # ib sm virt configure` `switch (config) #`	
Related Commands		
Notes		

ib sm virt-default-hop-limit

ib sm virt-default-hop-limit <value>
no ib sm virt-default-hop-limit

Configures the default value for hop limit to be returned in path records. The no form of the command resets this parameter to its default value.

Syntax Description	value	Range: 0-255
Default	2	
Configuration Mode	config	
History	3.6.2002	
Role	admin	
Example	`switch (config) # ib sm virt-default-hop-limit 3`	
Related Commands		
Notes		

ib sm virt-max-ports-in-process

ib sm virt-max-ports-in-process <value>
no ib sm virt-max-ports-in-process

Configures the maximum number of ports to be processed simultaneously. The no form of the command resets this parameter to its default value.

Syntax Description	value	Range:0-65535 ‘0’ processes all pending ports
Default	4	
Configuration Mode	config	
History	3.6.2002	
Role	admin	
Example	`switch (config) # ib sm virt-max-ports-in-process 5`	
Related Commands		
Notes		

show ib sm

	show ib sm Displays the SM admin state.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm`
	`enable`
	`switch (config) #`

Related Commands	ib sm
Notes	

show ib sm accum-log-file

	show ib sm accum-log-file Displays the accum-log-file configuration.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm accum-log-file`
	`enable`
	`switch (config) #`

Related Commands	ib sm accum-log-file
Notes	

show ib sm babbling-policy

	show ib sm babbling-policy Displays the ability of the SM to disable babbling ports (i.e., generating frequent traps).
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm babbling-policy`
	`disable`
	`switch (config) #`

Related Commands	ib sm babbling-policy
Notes	

show ib sm connect-roots

	show ib sm connect-roots Displays the IBA compliant multi-stage switch directive.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm connect-roots`
	`true`
	`switch (config) #`

Related Commands	ib sm connect-roots
Notes	

show ib sm enable-quirks

	show ib sm enable-quirks Displays if the SM uses high risk features and handles HW workarounds.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm enable-quirks`
	`disable`
	`switch (config) #`

Related Commands	ib sm enable-quirks
Notes	

show ib sm exit-on-fatal

	show ib sm exit-on-fatal Displays if the SM exits upon a fatal error.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm exit-on-fatal`
	`enable`
	`switch (config) #`

Related Commands	ib sm exit-on-fatal
Notes	

show ib sm fdr10

show ib sm fdr10

Displays the status of the SM use of FDR10.

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

Example	`switch (config) # show ib sm fdr10`
	`SM use of fdr10 is off`
	`switch (config) #`

Related Commands	
Notes	

show ib sm force-link-speed

	show ib sm force-link-speed Displays SM behavior for PortInfo:LinkSpeedEnabled parameter on switch ports.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000 3.4.1604 Updated Syntax Description, Example and Notess
Role	admin

Example	`switch (config) # show ib sm force-link-speed`
	`Default: set to PortInfo:LinkSpeedSupported`
	`switch (config) #`

Related Commands	ib sm force-link-speed
Notes	Possible outputs: • Default: set to PortInfo:LinkSpeedExtSupported • Disabled: extended link speed not in use • Negotiate: <a list containing fdr, edr speeds>

show ib sm force-link-speed-ext

	show ib sm force-link-speed-ext Displays SM behavior for PortInfo:LinkSpeedExtEnabled parameter on the switch ports.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000 3.4.1604 Updated description and Example
Role	admin

Example	`switch (config) # show ib sm force-link-speed-ext`
	`Negotiate: fdr edr`
	`switch (config) #`

Related Commands	
Notes	Possible outputs: • Default: set to PortInfo:LinkSpeedExtSupported • Disabled: extended link speed not in use • Negotiate: <a list containing fdr, edr speeds>

show ib sm force-log-flush

	show ib sm force-log-flush Displays if every log message generated forces the log to be flushed.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm force-log-flush`
	`enable`
	`switch (config) #`

Related Commands	ib sm force-log-flush
Notes	

show ib sm guid2lid-cache

	show ib sm guid2lid-cache Displays whether or not the SM honors the cached GUID-to-LID mapping information.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm guid2lid-cache`
	`disable`
	`switch (config) #`

Related Commands	ib sm guid2-lid-cache
Notes	

show ib sm honor-partitions

show ib sm honor-partitions

Displays the partition enforcement settings in the subnet.

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

Example	`switch (config) # show ib sm honor-partitions`
	`disable`
	`switch (config) #`

Related Commands	ib sm honor-partitions
Notes	

show ib sm hoq-lifetime

show ib sm hoq-lifetime

Displays the maximum time a frame can wait at the head of a switch-to-switch port queue before it is dropped.

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

Example	`switch (config) # show ib sm hoq-lifetime`
	`0x12 (About   1 second)`
	`switch (config) #`

Related Commands	ib sm hoq-lifetime
Notes	

show ib sm ignore-other-sm

	show ib sm ignore-other-sm Displays if the rules governing SM elections and attempt to manage the fabric on the node are ignored by the SM.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm ignore-other-sm`
	`enable`
	`switch (config) #`

Related Commands	ib sm ignore-other-sm
Notes	

show ib sm ipv6-nsm

	show ib sm ipv6-nsm Displays the consolidation of IPv6 Solicited Node Multicast (SNM) group join requests.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm ipv6-nsm`
	`enable`
	`switch (config) #`

Related Commands	ib sm ipv6-nsm
Notes	

show ib sm lash

show ib sm lash {do-mesh-analysis | start-vl}

Display 'lash' routing method parameters.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # show ib sm lash do-mesh-analysis enable` `switch (config) #`
Related Commands	ib sm lash
Notes	

show ib sm leafhoq-lifetime

	show ib sm leafhoq-lifetime Displays the maximum time a frame can wait at the head of a switch-to-CA_or_Router port queue before it is dropped.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm leafhoq-lifetime`
	`0x10 (About 268 mS)`
	`switch (config) #`

Related Commands	ib sm leafhoq-lifetime
Notes	

show ib sm leafvl-stalls

	show ib sm leafvl-stalls Displays the number of sequential frame drops that case a switch-to-CA_or_Router port to enter the VLStalled state.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm leafvl-stalls`
	`7`
	`switch (config) #`

Related Commands	ib sm leafvl-stalls
Notes	

show ib sm lmc

	show ib sm lmc Displays the LID Mask Control (LMC) value to be used on this subnet.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm lmc`
	`0x0`
	`switch (config) #`

Related Commands	ib sm lmc
Notes	

show ib sm lmc-esp0

	show ib sm lmc-esp0 Displays whether the LMC for the subnet is also used for Enhanced Switch Port 0 (ib sm lmc-esp0) or if the LMC for ESP0 ports is 0 (no ib sm lmc-esp0).
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm lmc-esp0`
	`enable`
	`switch (config) #`

Related Commands	ib sm lmc-esp0
Notes	

show ib sm log

show ib sm log [continuous] [[not] [matching <reg-expression>]]

Displays IB SM event logs.

Syntax Description	continuous	Displays IB SM new event log messages as they arrive
	not	Displays IB SM new event logs that do not match a given regular expression.
	matching <regular expression>	Displays IB SM event log messages that match a given regular expression.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example		

```
switch (config) # show ib sm log
Jul 18 12:00:40 165863 [48026660] 0x03 -> OpenSM 3.3.13.MLNX-
_20121224_9b362db
Jul 18 12:00:40 168685 [48026660] 0x80 -> OpenSM 3.3.13.MLNX-
_20121224_9b362db
Jul 18 12:00:40 170789 [48026660] 0x02 -> osm_vendor_init: 1000 pending
umads specified
Jul 18 12:00:40 175696 [48026660] 0x80 -> Entering DISCOVERING state
Jul 18 12:00:40 249448 [48026660] 0x02 -> osm_vendor_bind: Binding to
port 0x2c903008b0440
Jul 18 12:00:40 293959 [48026660] 0x02 -> osm_vendor_bind: Binding to
port 0x2c903008b0440
Jul 18 12:00:40 296921 [48026660] 0x02 -> osm_vendor_bind: Binding to
port 0x2c903008b0440
Jul 18 12:00:40 304702 [48026660] 0x02 -> osm_opensm_bind: Setting
IS_SM on port 0x0002c903008b0440
Jul 18 12:00:40 399744 [4A85D4B0] 0x80 -> Entering MASTER state

switch (config) #
```

Related Commands	show ib sm log-flags
Notes	

show ib sm log-flags

show ib sm log-flags

Displays what type of messages the SM will log.

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

Example	`switch (config) # show ib sm log-flags`
	`0x3 (error, info)`
	`switch (config) #`

Related Commands	ib sm log-flags
Notes	

show ib sm log-max-size

	show ib sm log-max-size Displays the maximum size of the log file.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm log-max-size`
	`50 MBytes`
	`switch (config) #`

Related Commands	is sm log-max-size
Notes	

show ib sm max-op-vls

	show ib sm max-op-vls Displays the maximum number of VLs supported on this subnet.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm max-op-vls`
	`15`
	`switch (config) #`

Related Commands	ib sm max-op-vls
Notes	

show ib sm max-ports

	show ib sm max-ports Displays the number of CA ports SM can manage
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm max-ports`
	`2048`
	`switch (config) #`

Related Commands	ib sm max-ports
Notes	

show ib sm max-reply-time

show ib sm max-reply-time

Displays the maximum time in milliseconds that the SM will wait for a reply before the transaction times out.

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

Example	`switch (config) # show ib sm max-reply-time`
	`200 milliseconds`
	`switch (config) #`

Related Commands	ib sm max-reply-time
Notes	

show ib sm max-reverse-hops

	show ib sm max-reverse-hops Displays max hops IO node to top switch
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # show ib sm max-reverse-hops` `0 hops`
Related Commands	ib sm max-reverse-hops
Notes	

show ib sm max-reverse-hops

	show ib sm max-reverse-hops Displays max hops IO node to top switch
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm max-reverse-hops`
	`0 hops`
	`switch (config) #`

Related Commands	ib sm max-reverse-hops
Notes	

show ib sm aguid-default-hop-limit

	show ib sm aguid-default-hop-limit Displays the default value for hop limit returned in path records where either the source or destination is an alias GUID.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.6102
Role	admin
Example	`switch (config) # show ib sm aguid-default-hop-limit` `1`
Related Commands	ib sm aguid-default-hop-limit
Notes	

show ib sm max-wire-smps

	show ib sm max-wire-smps Displays the maximal number of MADs the SM will have outstanding at one time to count.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm max-wire-smps`
	`8`
	`switch (config) #`

Related Commands	ib sm max-wire-snmps
Notes	

show ib sm max-wire-smps2

	show ib sm max-wire-smps2 Displays maximal SM timeout based packets allowed to be outstanding.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm max-wire-smps2`
	`4`
	`switch (config) #`

Related Commands	
Notes	

show ib sm mkey-lease

	show ib sm mkey-lease Displays MKey period in seconds.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm mkey-lease`
	`0 (No timeout)`
	`switch (config) #`

Related Commands	ib sm mkey-lease
Notes	

show ib sm m-key

	show ib sm m-key Displays the MKey used by the SM
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000 3.6.2002 Updated example
Role	admin
Example	`switch (config) # show ib sm m-key` `11:33:55:77:99:aa:cc:ee`
Related Commands	ib sm m-key
Notes	

show ib sm mkey-lookup

	show ib sm mkey-lease Displays whether SM looks in file cache for unknown node MKeys or not.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # show ib sm mkey-lookup` `enable`
Related Commands	ib sm mkey-lookup
Notes	

show ib sm mkey-protect-level

	show ib sm mkey-protect-level Displays MKey protection level.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # show ib sm mkey-protect-level` `0`
Related Commands	ib sm mkey-protect-level
Notes	

show ib sm msgfifo-timeout

	show ib sm msgfifo-timeout Displays the elapsed time in milliseconds before a frame at the head of Subnet Agent queue causes an immediate BUSY state.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm msgfifo-timeout`
	`10.000 seconds`
	`switch (config) #`

Related Commands	ib sm msgfifo-timeout
Notes	

show ib sm multicast

	show ib sm multicast Displays whether the SM supports multicast on the fabric.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm multicast`
	`enable`
	`switch (config) #`

Related Commands	ib sm multicast
Notes	

show ib sm no-client-rereg

	show ib sm no-client-rereg Displays client re-registration admin state.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm no-client-rereg`
	`enable`
	`switch (config) #`

Related Commands	ib no-client-rereg
Notes	

show ib sm overrun-trigger

	show ib sm overrun-trigger Displays count of local buffer overrun errors for Infiniband trap 130
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm overrun-trigger`
	`3`
	`switch (config) #`

Related Commands	ib sm overrun-trigger
Notes	

show ib sm packet-life-time

show ib sm packet-life-time

Displays the maximum time a frame can live in a switch.

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

Example	`switch (config) # show ib sm packet-life-time`
	`0x14 (Infinite)`
	`switch (config) #`

Related Commands	ib sm packet-life-time
Notes	

show ib sm phy-err-trigger

	show ib sm phy-err-trigger Displays the number of local link integrity errors and the port's SMA supports traps.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm phy-err-trigger`
	`5`
	`switch (config) #`

Related Commands	ib sm phy-err-trigger
Notes	

show ib sm polling-retries

	show ib sm polling-retries Displays the number of consecutive times an active SM must fail to respond before it is declared dead.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm polling-retries`
	`8`
	`switch (config) #`

Related Commands	ib sm polling-retries
Notes	

show ib sm port-prof-switch

	show ib sm port-prof-switch Displays whether or not the counting of adapters, routers, and switches through the links is being done.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm port-prof-switch`
	`true`
	`switch (config) #`

Related Commands	ib sm port-prof-switch
Notes	

show ib sm reassign-lids

	show ib sm reassign-lids Displays the ability of the SM to reassign LIDs to nodes it finds already configured with a valid LID.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm reassign-lids`
	`enable`
	`switch (config) #`

Related Commands	ib sm reassign-lids
Notes	

show ib sm root-guid

	show ib sm root-guid Displays the configured root GUIDs for the SM.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config)# show ib sm root-guid`
	`AA:00:11:22:33:44:55`
	`AA:00:11:22:33:44:56`
	`AA:00:11:22:33:44:57`
	`…`
	`switch (config)#`

Related Commands	ib sm routing-engine
Notes	The list of root GUIDs are relevant when IB SM is running on the switch, and the routing algorithm is up-down or fat-tree.

show ib sm routing-engines

	show ib sm routing-engines Displays an ordered list of routing engines
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm routing-engine`
	`none`
	`switch (config) #`

Related Commands	ib sm routing-engine
Notes	

show ib sm routing-info

	show ib sm routing-info Displays current routing engine information.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm routing-info`
	`Current routing engine minhop`
	`switch (config) #`

Related Commands	
Notes	

show ib sm rtr-aguid-enable

	show ib sm rtr-aguid-enable Displays GUID option configuration.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # show ib sm rtr-aguid-enable` `0`
Related Commands	`ib sm rtr-aguid-enable`
Notes	

show ib sm rtr-pr-flow-label

show ib sm rtr-pr-flow-label

Displays inter-subnet PathRecord FlowLabel.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # show ib sm rtr-pr-flow-label` `0`
Related Commands	`ib sm rtr-pr-flow-label`
Notes	‘0’ means Inter-subnet PathRecord FlowLabel is disabled

show ib sm rtr-pr-mtu

	show ib sm rtr-pr-mtu Displays inter-subnet PathRecord MTU.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # show ib sm rtr-pr-mtu` `2K`
Related Commands	`ib sm rtr-pr-mtu`
Notes	

show ib sm rtr-pr-rate

	show ib sm rtr-pr-rate Displays inter-subnet PR rate.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # show ib sm rtr-pr-rate` `100`
Related Commands	`ib sm rtr-pr-rate`
Notes	

show ib sm rtr-pr-sl

	show ib sm rtr-pr-sl Displays inter-subnet PathRecord service level.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # show ib sm rtr-pr-sl` `0`
Related Commands	`ib sm rtr-pr-sl`
Notes	

show ib sm sa-key

	show ib sm sa-key Displays the SM sa-key value used by SA to qualify that a query is “trusted”.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm sa-key`
	`00:00:00:00:00:00:00:05`
	`switch (config) #`

Related Commands	ib sm sa-key
Notes	

show ib sm single-thread

	show ib sm single-thread Displays if the SM uses a single thread to service all requests.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm single-thread`
	`enable`
	`switch (config) #`

Related Commands	ib sm single-thread
Notes	

show ib sm sm-inactive

	show ib sm sm-inactive Displays whether or not the SM starts in “inactive” rather than “init” SM state.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm sm-inactive`
	`enable`
	`switch (config) #`

Related Commands	ib sm sm-inactive
Notes	

show ib sm sm-key

	show ib sm sm-key Displays the SM 64-bit SM_Key.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm sm-key`
	`00:00:00:00:00:00:00:05`
	`switch (config) #`

Related Commands	ib sm sm-key
Notes	

show ib sm sm-priority

	show ib sm sm-priority Displays the importance of this SM compared to other SMs on the fabric.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm sm-priority`
	`1`
	`switch (config) #`

Related Commands	ib sm sm-priority
Notes	Priority 0 is the least important, 15 the most important. If 2 or more active SMs have the same highest priority, the one with the lowest port GUID will manage the fabric.

show ib sm sm-sl

	show ib sm sm-sl Display SL used for SM/SA communication
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm sm-sl`
	`1`
	`switch (config) #`

Related Commands	ib sm sm-sl
Notes	

show ib sm sminfo-poll-time

	show ib sm sminfo-poll-time Displays the timeout in milliseconds between two polls of an active SM.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm sminfo-poll-time`
	`15 milliseconds`
	`switch (config) #`

Related Commands	ib sm sminfo-poll-time
Notes	

show ib sm subnet-prefix

	show ib sm subnet-prefix Displays the SM “Subnet Prefix” used to create scope qualifiers for all elements managed by the SM.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm subnet-prefix`
	`FF:FF:FF:FF:FF:FF:FF:00`
	`switch (config) #`

Related Commands	ib sm subnet-prefix
Notes	

show ib sm subnet-prefix-override

	show ib sm subnet-prefix Displays whether IB Router subnet prefix checking is enabled or disabled.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # show ib sm subnet-prefix-override` `disable`
Related Commands	ib sm subnet-prefix-override
Notes	

show ib sm subnet-timeout

	show ib sm subnet-timeout Displays the global per-port subnet timeout value (PortInfo:SubnetTimeOut). This value also controls the maximum trap frequency in which no traps are allowed to be sent faster than the subnet_timeout value. The time is 4.096 uS * 2*time.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm subnet-timeout`
	`0x5 (About 131 uS)`
	`switch (config) #`

Related Commands	ib sm subnet-timeout
Notes	

show ib sm sweep-interval

show ib sm sweep-interval

Displays the time in seconds between subnet sweeps.

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

Example	`switch (config) # show ib sm sweep-interval`
	`20 seconds`
	`switch (config) #`

Related Commands	ib sm sweep-interval
Notes	

show ib sm sweep-on-trap

	show ib sm sweep-on-trap Displays whether or not a heavy sweep is initiated by the TRAP received by the SM.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm sweep-on-trap`
	`enable`
	`switch (config) #`

Related Commands	ib sm sweep-on-trap
Notes	

show ib sm transaction-retries

	show ib sm transaction-retries Displays maximum retries before failing a transaction
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm transaction-retries`
	`3`
	`switch (config) #`

Related Commands	ib sm transaction-retries
Notes	

show ib sm use-heavy-sweeps

	show ib sm use-heavy-sweeps Displays SM requirement to always use heavy sweeps.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm use-heavy-sweeps`
	`disable`
	`switch (config) #`

Related Commands	ib sm use-heavy-sweeps
Notes	

show ib sm use-ucast-cache

	show ib sm use-ucast-cache Displays if the SM uses cached routine data.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm use-ucast-cache`
	`false`
	`switch (config) #`

Related Commands	ib sm user-ucase-cache
Notes	

show ib sm version

	show ib sm version Displays the open SM version that is currently running.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.2.3000
Role	admin

Example	`switch (config) # show ib sm version`
	`OpenSM3.3.7`
	`switch (config) #`

Related Commands	
Notes	

show ib sm virt-default-hop-limit

show ib sm virt-default-hop-limit

Displays the default value for hop limit to be returned in path records.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # show ib sm virt-default-hop-limit` `2`
Related Commands	ib sm virt-default-hop-limit
Notes	

show ib sm virt-max-ports-in-process

	show ib sm virt-max-ports-in-process Displays the maximum number of ports to be processed simultaneously.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.2002
Role	admin
Example	`switch (config) # show ib sm virt-max-ports-in-process` `4`
Related Commands	ib sm virt-max-ports-in-process
Notes	

show ib sm vl-stalls

	show ib sm use-vl-stalls Displays the number of sequential frame drops that cause a switch-to-switch port to enter the VLStalled state.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # show ib sm vl-stalls`
	`7`
	`switch (config) #`

Related Commands	ib sm vl-stalls
Notes	

5.5.6.2 Partitions

ib partition

ib partition <partition-name> [pkey <pkey number>]
no ib partition <partition-name> [force]

Enters the context of the partition specified.
The no form of the command deletes the partition.

Syntax Description	partition-name	Name of partition context to be entered
	pkey	Creates a partition and enters a new configuration mode
	force	Forces configuration
Default	Default partition is available (PKEY 0x7fff)	
Configuration Mode	config	
History	3.2.0500	
	3.6.8008	Added “force” parameter to “no” form
Role	admin	
Example	`switch (config) # ib partition my-partition` `switch (config partition my-partition) #`	
Related Commands		
Notes		

pkey

	pkey <number> [force] **no pkey <number>** Specifies PKEY number for this partition. The no form of the command removes the PKEY configuration from partitions.conf file.	
Syntax Description	number	0x001-0x7fff
	force	Forces configuration
Default	N/A	
Configuration Mode	Config Partition	
History	3.2.0500	
	3.5.1000	Added “force” parameter
Role	admin	

Example	`switch (config) # ib partition my-partition`
	`switch (config partition my-partition) # pkey 0x7777`
	`switch (config partition my-partition) #`	

Related Commands		
Notes	PKEY must be unique.	

defmember

defmember <type> [force]
no defmember

Sets the default membership for port GUID list.
The no form of the command set the defmember configuration to default (it will not appear in the partitions.conf file).

Syntax Description	type	Default membership for GUIDs in this partition: • full • limited • both
	force	Forces configuration
Default	limited	
Configuration Mode	Config Partition	
History	3.2.0500	
	3.4.1100	Added “both” option
	3.5.1000	Added “force” parameter
Role	admin	

Example	`switch (config) # ib partition my-partition`
	`switch (config ib partition my-partition) # defmember full`
	`switch (config ib partition my-partition) #`	

Related Commands	ib sm allow-both-pkeys member	
Notes	This parameter can be overwritten for specific GUID, using the “member” command.	

member

member {<guid> | all | self} [type <member-type>] [force]
no member {<guid> | all | self} [type] [force]

Adds static members to partition.
The no form of the command will remove the static member from the partition (it will not appear in the partitions.conf file).

Syntax Description	guid	The GUID number
	all | self	The option “all” can be used for all GUIDs in the fabric, or “self” for the switch guide
	member-type	Default membership for GUIDs in this partition: • full • limited • both
	force	Forces configuration
Default	N/A	
Configuration Mode	Config Partition	
History	3.2.0500	
	3.4.1100	Added “both” parameter
	3.5.1000	Added “force” parameter
Role	admin	
Example	`switch (config) # ib partition my-partition` `switch (config ib partition my-partition) # member all`	
Related Commands	ib partition ib sm allow-both-pkeys defmember	
Notes		

ipoib

ipoib [force]
no ipoib [force]

Enables this partition to use IPoIB. As a result IPoIB multicast group will be created. The no form of the command removes the use of IPoIB in this partition (it will not appear in the partitions.conf file).

Syntax Description	force	Forces configuration
Default	no ipoib	
Configuration Mode	Config Partition	
History	3.2.0500	
	3.5.1000	Added “force” parameter
	3.6.8008	Added “force” parameter to “no” form
Role	admin	
Example	`switch (config) # ib partition my-partition` `switch (config partition my-partition) # ipoib`	
Related Commands	ib partition rate mtu sl scope	
Notes	“rate”, “mtu”, “sl” and “scope” commands can be used only when the IPoIB parameter is enabled.	

mtu

mtu <256, 512, 1K, 2K,4K> [force]
no mtu

Specifies MTU for this IPoIB multicast group.
The no form of the command sets the mtu to default (it will not appear in the partitions.conf file).

Syntax Description	force	Forces configuration
Default	2K	
Configuration Mode	Config Partition	
History	3.2.0500	
	3.5.1000	Added “force” parameter
Role	admin	

Example	`switch (config) # ib partition my-partition`
	`switch (config partition my-partition) # mtu 4K`
	`switch (config partition my-partition) #`	

Related Commands	ipoib	
Notes	IPoIB parameter on the partitions must be enabled in order to use this parameter	

rate

	rate <rate> [force] **no rate** Specifies rate for this IPoIB multicast group. The no form of the command set the rate to default (removes the rate from the partitions.conf)	
Syntax Description	rate	• default - Default • 2.5 - 2.5 Gbps • 5 - 5 Gbps • 10 - 10 Gbps • 14 - 14 Gbps • 20 - 20 Gbps • 25 - 25 Gbps • 40 - 40 Gbps • 56 - 56 Gbps • 100 - 100 Gbps
	force	Forces configuration
Default	10 Gbps.	
Configuration Mode	Config Partition	
History	3.2.0500	
	3.4.1100	Updated rate Syntax Description
	3.5.1000	Added “force” parameter
Role	admin	

Example	`switch (config) # ib partition my-partition`
	`switch (config partition my-partition) # rate 20`
	`switch (config partition my-partition) #`	

Related Commands		
Notes	• Ports that do not support the IPoIB rate are not added to the partition	

scope

scope <type> [force]
no scope <link-local, site-local, organization-local, global>

Specifies scope for this IPoIB multicast group.
The no form of the command removes the scope configuration from the partitions.conf file

Syntax Description	type	link-local site-local organization-local global
	force	Forces configuration
Default	link-local	
Configuration Mode	Config Partition	
History	3.2.0500	
	3.5.1000	Added “force” parameter
Role	admin	

Example	`switch (config) # ib partition my-partition`
	`switch (config partition my-partition) # scope global`
	`switch (config partition my-partition) #`	

Related Commands		
Notes	ipoib parameter on the partitions must be enabled in order to use this parameter.	

sl

	sl <0-14, “default”> [force] **no sl** Specifies SL (Service Level - QoS) for this IPoIB multicast group. The no form of the command sets it to default (the sl configuration is removed from the partitions.conf file).	
Syntax Description	0-14	
	force	Forces configuration
Default	default (0)	
Configuration Mode	Config Partition	
History	3.2.0500	
	3.5.1000	Added “force” parameter
Role	admin	

Example	`switch (config) # ib partition my-partition`
	`switch (config partition my-partition) # sl 7`
	`switch (config partition my-partition) #`	

Related Commands		
Notes	ipoib parameter on the partitions must be enabled in order to use this parameter.	

show ib partition

show ib partition [<partition-name> [member [<member-name>]]]

Displays partition info, with optional to filters.

Syntax Description	partition-name	Filters the output per partition name
	member <member-name>	Filters the output by a specific member
Default	N/A	
Configuration Mode	Any command mode	
History	3.2.0500	
	3.6.8008	Updated Example and note
Role	admin	

Example	`switch (config) # show ib partition Default`
	
	`Default`
	`  PKey = 0x7FFF`
	`  ipoib = yes`
	
	`  members`
	`    GUID='ALL' member='full'`	

Related Commands		
Notes	If bulk update mode is enabled, this command notifies the user that these changes may not have been applied yet.	

5.5.6.3 Quality of Service (SM)

ib baseqos <port-type> high-limit

ib baseqos <port-type> high-limit <count>

Sets the high-limit value for the indicated port type. Thus the system will send at least 4096 * <count> bytes from the high priority list before sending any from the low priority list.

Syntax Description	port-type	• ca - channel adapters • rtr - routers • sw0 - ports 0 only of the switches • swe - external ports of the switches
	high-limit	Possible values are: -1...255 • -1 - default SM high-limit • 0 - 1 frame • i =1...254 - 4K * i • 255 - unlimited
Default	-1 (default SM high-limit).	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ib baseqos ca high-limit 255` `switch (config) #`	
Related Commands	show ib baseqos	
Notes	A high-limit value of 255 means unlimited, and that makes it possible to starve the low priority list.	

ib baseqos <port-type> max-vls <value>

ib baseqos <port-type> max-vls <value>

Sets the maximum number of VLs for the indicated port type.

Syntax Description	port-type	ca - channel adapters rtr - routers sw0 - ports 0 only of the switches swe - external ports of the switches
	value	Max VLs range between 1 and 15.
Default	15	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib baseqos ca max-vls 15`
	`switch (config) # show ib baseqos ca max-vls`
	`15`
	`switch (config) #`	

Related Commands	show ib baseqos	
Notes		

ib baseqos <port-type> sl2vl

ib baseqos <port-type> sl2vl {sl0 | sl0 sl1 | sl0 sl1 sl2 |…}
no ib baseqos <port-type> sl2vl

Sets a list of up to 16 entries that map the SL entry to an appropriate VL.
The no form of the command sets the attributes to their default settings.

Syntax Description	port-type	ca - channel adapters rtr - routers sw0 - ports 0 only of the switches swe - external ports of the switches
	sl[i]	A single vector (1 ... 16 elements), the command line vector determine the SL [0...15] that is mapped to the specified VL [0...15].
Default	The default mapping is: 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,7	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) #show ib baseqos ca sl2vl`
	`0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,7`
	`switch (config) # ib baseqos ca sl2vl 10 10 10`
	`switch (config) # show ib baseqos ca sl2vl`
	`10,10,10,15,15,15,15,15,15,15,15,15,15,15,15,15`
	`switch (config) #`	

Related Commands	show ib baseqos	
Notes	Any missing SLs will be mapped to VL15.	

ib baseqos <port-type> vlarb-high <value>

ib baseqos <port-type> vlarb-high {VW1 | VW1 VW2 | …}
no ib baseqos <port-type> vlarb-high

Sets up to 15 VL to Weight mapping pairs for high priority processing.
The no form of the command sets the attributes to their default settings.

Syntax Description	port-type	ca - channel adapters rtr - routers sw0 - ports 0 only of the switches swe - external ports of the switches
	VW[i]	There are two possible options for this parameter: • A single vector (1 ...15) in the format of "#:#" separated by spaces, see example below. • Format of "i#=X:Y" in order to change a specific entry (see example below)
Default	The default mapping is: 0:4,1:0,2:0,3:0,4:0,5:0,6:0,7:0,8:0,9:0,10:0,11:0,12:0,13:0,14:0	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) #show ib baseqos ca vlarb-high`
	`0:4,1:0,2:0,3:0,4:0,5:0,6:0,7:0,8:0,9:0,10:0,11:0,12:0,13:0,14:0`
	`switch (config) # ib baseqos ca vlarb-high 0:10 1:10`
	`switch (config) # show ib baseqos ca vlarb-high`
	`0:10,1:10,2:0,3:0,4:0,5:0,6:0,7:0,8:0,9:0,10:0,11:0,12:0,13:0,14:0`
	`switch (config) # ib baseqos sw0 vlarb-high i2=4:3`
	`switch (config) # show ib baseqos sw0 vlarb-high`
	`0:10,1:10,4:3,3:0,4:0,5:0,6:0,7:0,8:0,9:0,10:0,11:0,12:0,13:0,14:0`	

Related Commands	show ib baseqos	
Notes	• Unspecified elements will be filled with (index:0) • You may have multiple entries with the same VL on this list.	

ib baseqos <port-type> vlarb-low <value>

ib baseqos <port-type> vlarb-low {VW1 | VW1 VW2 | …}
no ib baseqos <port-type> vlarb-low

Sets up to 15 VL to Weight mapping pairs for low priority processing.
The no form of the command sets the attributes to their default settings.

Syntax Description	port-type	ca - channel adapters rtr - routers sw0 - ports 0 only of the switches swe - external ports of the switches
	VW[i]	There are two possible options for this parameter: • A single vector (1 ...15) in the format of "#:#" separated by spaces, see example below. • Format of "i#=X:Y" in order to change a specific entry (see example below)
Default	The default mapping is: 0:0,1:4,2:4,3:4,4:4,5:4,6:4,7:4,8:4,9:4,10:4,11:4,12:4,13:4,14:4	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib baseqos sw0 vlarb-low 1:1`
	`switch (config) # show ib baseqos sw0 vlarb-low`
	`1:1, 1:0, 2:0, 3:0, 4:0, 5:0, 6:0, 7:0, 8:0, 9:0, 10:0, 11:0, 12:0, 13:0, 14:0`
	`switch (config) # ib baseqos sw0 vlarb-low i2=4:3`
	`switch (config) # show ib baseqos sw0 vlarb-low`
	`1:1, 1:0, 4:3, 3:0, 4:0, 5:0, 6:0, 7:0, 8:0, 9:0, 10:0, 11:0, 12:0, 13:0, 14:0`
	`switch (config) #`	

Related Commands	show ib baseqos	
Notes	You may have multiple entries with the same VL on this list.	

ib baseqos reset-config

	ib baseqos reset-config Resets all basic QoS configuration options to defaults.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.0000
Role	admin
Example	`switch (config) # ib baseqos reset-config` `switch (config) #`
Related Commands	
Notes	

show ib baseqos

show ib baseqos <port-type> <baseqos-parameters>

Displays the base ib QoS configuration.

Syntax Description	port-type	• ca - channel adapters • rtr - routers • sw0 - ports 0 only of the switches • swe - external ports of the switches
	baseqos-parameters	Possible values are: • high-limit - Display high limit (how many high pri before low) • max-vls - Display maximum number of VLs supported on CAs in subnet • sl2vl - Display current SL-to-VL mapping vector • vlarb-high - Display current high priority VL arbitration • vlarb-low - Display current low priority VL arbitration
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show ib baseqos ca high-limit`
	`0`
	`switch (config) #`	

Related Commands		
Notes		

ib qos

	ib qos **no ib qos** Enables advanced QoS management on this node The no form of the command disables advance QoS on this node.
Syntax Description	N/A
Default	advance qos is disabled.
Configuration Mode	config
History	3.1.0000
Role	admin

Example	`switch (config) # ib qos`
	`switch (config) # show ib qos`
	`enable`
	`switch (config) #`

Related Commands	show ib qos
Notes	

ib qos level

ib qos level {<name> | default} {mtu-limit <mtu> | packet-life <time> | pkey <number> | rate-limit <rate-value> | sl <sl-value>| use <description>}
no ib qos level {<name> | default} {mtu-limit | packet-life | pkey | rate-limit | sl | use}

Specifies a QoS level <name> or "default" parameters.
The no form of the command set the parameters to default.

Syntax Description	<name> | default	Specify a name for this qos group, or use the "default" for the default qos parameters.
	mtu-limit <mtu>	MTU in bytes. Possible values are: 1k, 256, 2k, 4k, 512
	packet-life <time>	Time a packet can wait in switch egress queue before being dropped. The bytes from 4 microsecond up to 2 seconds or infinite. Possible values are 0-20 0 - 4usec 1 - 8usec ... 20 - unlimited
	pkey <number>	PKEY value: ranges between -1 and 32767 (hex 0x7fff)
	rate-limit <rate-value>	Manages rate limits for QoS Policy levels. Possible values are (in Gbps): default, 2.5, 5, 10, 14, 20, 25, 40, 56, 100.
	sl <sl-value>	Manages service level for QoS Policy levels. Range: 0-15.
	use <description>	Specify usage description for this QoS level
Default	The default values are: use = "default QoS Level" sl = 0 mtu-limit = default rate-limit = default packet-life = 0x12 pkey = -1	
Configuration Mode	config	
History	3.1.0000	
	3.4.1100	Updated description of "rate-limit" parameter
Role	admin	

Example	`switch (config) # ib qos level my-qos-group mtu-limit 2K`
	`switch (config) # show ib qos my-qos-group`
	`my-qos-group:`
	`  use  = default QoS Level`
	`  sl  = 0`
	`  mtu-limit  = 2K`
	`  rate-limit  = default`
	`  packet-life  = 0x12`
	`  pkey  = -1`
	`switch (config) #`

Related Commands	show ib qos
Notes	

ib qos match-rule

	ib qos match-rule <rule-index> { {destination | source} <string> | {pkey | qos-class | service-id} <index> {first | last} <value>} | qos-level-name <name>| use <description>} **no ib qos match-rule <rule-index> { {destination | source} | {pkey | qos-class | service-id} <index> {first | last} } | qos-level-name | use }** Manages QoS Policy match rules. The no form of the command set the QoS match-rule to default.	
Syntax Description	rule-index	Index of this match-rule. Possible range is: 0-4294967295
	destination | source <string>	Manages destination or source for QoS Policy match rules.
	pkey | qos-class | service-id <index>	Manages values for QoS Policy match rules.
	{first | last} <value>	First or last value range (per PKEY / qos-class of service id.
	qos-level-name <name>	Name for the QoS level
	use <description>	Specify usage description for this QoS level
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # ib qos match-rule 10 use my-use`
	`switch (config) # show ib qos match-rule 10`
	`match-rule/10:`
	`match-rules: use = my-use`
	`match-rules: qos-level-name = DEFAULT`
	`switch (config) #`	

Related Commands	show ib qos	
Notes		

ib qos port-group

ib qos port-group <name> {node-type <index> type <node-type> | partition <name>| pkey <number> | port-guid <index> {first | last} <value> | port-name <index> name <name-value>| use <description>}
no ib qos port-group <name> {node-type <index> type | partition | pkey | port-guid <index> {first | last} | port-name <index> name | use }

Manages QoS Policy port groups.
The no form of the command removes a QoS port-group.

Syntax Description	<name>	Port group name
	node-type <index>	Node type index
	type <node-type>	A node type for this port group
	partition <name>	A Partition name
	pkey <number>	A PKEY number
	port-guid <index> {first | last} <value>	Port-guid range
	port-name <index> name <name-value>	Port index name
	use <description>	Specify usage description for this QoS level
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config)# ib qos port-group my-group use my-use`
	`switch (config)# show ib qos port-group my-group`
	`port-group/my-group:`
	`port-groups: pkey = -1`
	`port-groups: use = my-use`
	`switch (config)#`	

Related Commands	show ib qos	
Notes		

ib qos ulp any

ib qos ulp any {pkey | service-id | target-port-guid <index> {first | last | sl} <value> | sl <sl-vlaue>}
no ib qos ulp any {pkey | service-id | target-port-guid <index> {first | last | sl} | sl}

Configures ULP any attributes.
The no form of the command deletes ULP any attributes.

Syntax Description	pkey <index>	Manages ULP default PKEY assignment.
	service-id <index>	Manages default ULP Service ID match rule.
	target-port-quid <index>	Manages ULP default target port GUID rule.
	first | last | sl <value>	• first - first value in range • last - last value n range • sl - Service level for the ULP rule
	sl <sl-value>	Sets default SL.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ib qos ulp any sl 2` `switch (config) #`	
Related Commands	show ib qos	
Notes		

ib qos ulp ipoib

ib qos ulp ipoib {default sl <sl-value>| pkey <index> {first | last | sl} <value> }
no ib qos ulp ipoib {default sl | pkey <index>}

Manages ULP IPoIB settings.
The no form of the command deletes IPoIB settings.

Syntax Description	default sl <sl-value>	Set the default sl. Range 1-15
	pkey <index>	Manages ULP default PKEY assignment.
	first | last | sl <value>	• first - first value in range • last - last value n range • sl - Service level for the ULP rule
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ib qos ulp ipoib default sl 5` `switch (config) #`	
Related Commands	show ib qos	
Notes		

ib qos ulp <protocol-type>

	ib qos ulp <protocol-type> {default sl <sl-value> | port-num< index> <first | last | sl> <value>} **no ib qos ulp iser {default <sl> | port-num1 <first | last | sl>}** Configures ULP IScsi Extensions for RDMA, Reliable Datagram Sockets or Sockets Direct Protocol attributes. The no form of the command deletes all rules.	
Syntax Description	protocol-type	iser - Scsi Extensions for RDMA rds - Reliable Datagram Sockets sdp - Sockets Direct Protocol
	default sl <sl-value>	Set the default sl. Range 1-15
	port-num< index>	Port number index
	first | last | sl	• first - First in range • last - in range • sl - Service level for the ULP rule
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ib qos ulp iser default sl 2` `switch (config) #`	
Related Commands	show ib qos	
Notes		

ib qos ulp srp

ib qos ulp srp target-port-guid <index> <first | last | sl> <value>
no ib qos ulp srp target-port-guid <index>

Configures Scsi Rdma Protocol attributes
The no form of the command deletes the rules.

Syntax Description	target-port-guid <index>	The index of the target port GUID
	first | last | sl	• first - First in range • last - in range • sl - Service level for the ULP rule
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ib qos ulp srp target-port-guid 1 sl 2` `switch (config) #`	
Related Commands	show ib qos	
Notes		

show ib qos

show ib qos [level | match-rule | port-group | ulp]

Displays InfiniBand QoS configurations

Syntax Description	level	Displays QoS level configurations
	match-rule	Displays QoS match-rule configurations
	port-group	Displays QoS port-group configurations
	ulp	Displays QoS ulp configurations
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show ib qos level my-qos-level`
	`my-qos-level:`
	`  use  = my-use`
	`  sl  = 0`
	`  mtu-limit  = 2K`
	`  rate-limit  = default`
	`  packet-life  = 0x12`
	`  pkey  = -1`
	`switch (config) #`	

Related Commands		
Notes		

5.5.6.4 Scatter Ports

ib sm scatter-ports

ib sm scatter-ports <seed>
no ib sm scatter-ports

Activates scatter ports and sets seed for random number generation.
The no form of the command deactivates the partition.

Syntax Description	seed	Integer between 0-4294967295
Default	Disabled	
Configuration Mode	config	
History	3.6.8008	
Role	admin	
Example	`switch (config) # ib sm scatter-ports 123`	
Related Commands	ib sm guid-routing-order-no-scatter	
Notes	Setting seed value 0 disables scatter ports	

show ib sm scatter-ports

	show ib sm scatter-ports
	Displays scatter port seed.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.8008
Role	admin

Example	`switch (config) # show ib sm scatter-ports`
	`Scatter ports seed: 234`
	`switch (config) # show ib sm scatter-ports`
	`Scatter ports: disable`

Related Commands	ib sm scatter-ports
Notes	

5.5.6.5 GUID Routing Order

ib sm guid-routing-order add

ib sm guid-routing-order add <guid> [position <pos>]

Adds a new GUID to routing order list.

Syntax Description	guid	GUID to add
	position	A position for the new GUID may be specified
Default	If no position is specified, the new GUID is added to the end of the list	
Configuration Mode	config	
History	3.6.8008	
Role	admin	
Example	`switch (config) # ib sm guid-routing-order add E4:1D:2D:03:00:3D:5E:87 position 6`	
Related Commands	ib sm guid-routing-order-no-scatter	
Notes		

ib sm guid-routing-order delete

ib sm guid-routing-order delete {<guid> | position <pos>}

Deletes a guid from routing order list. The guid can be chosen by its guid or by its position on guid routing order list.

Syntax Description	guid	GUID to delete
	position	Deletes a GUID by specifying position number
Default	N/A	
Configuration Mode	config	
History	3.6.8008	
Role	admin	
Example	`switch (config) # ib sm guid-routing-order delete position 3` `switch (config) # ib sm guid-routing-order delete E4:1D:2D:03:00:3D:5E:91`	
Related Commands	ib sm guid-routing-order-no-scatter	
Notes		

ib sm guid-routing-order move

ib sm guid-routing-order move <guid> to-position <pos>

Moves a GUID in the list to a specified position.

Syntax Description	guid	GUID to move
	position	A position for the new GUID may be specified
Default	N/A	
Configuration Mode	config	
History	3.6.8008	
Role	admin	
Example	`switch (config) # ib sm guid-routing-order move E4:1D:2D:03:00:3D:5E:91 to-position 2`	
Related Commands	ib sm guid-routing-order-no-scatter	
Notes		

ib sm guid-routing-order move-down

ib sm guid-routing-order move-down <guid>

Moves a GUID position down in the GUID routing order list.

Syntax Description	guid	GUID to move
Default	N/A	
Configuration Mode	config	
History	3.6.8008	
Role	admin	
Example	`switch (config) # ib sm guid-routing-order move-down E4:1D:2D:03:00:3D:5E:91`	
Related Commands	ib sm guid-routing-order-no-scatter	
Notes		

ib sm guid-routing-order move-up

ib sm guid-routing-order move-up <guid>

Moves a GUID position up in the GUID routing order list.

Syntax Description	guid	GUID to move
Default	N/A	
Configuration Mode	config	
History	3.6.8008	
Role	admin	
Example	`switch (config) # ib sm guid-routing-order move-up E4:1D:2D:03:00:3D:5E:91`	
Related Commands	ib sm guid-routing-order-no-scatter	
Notes		

no ib sm guid-routing-order

no ib sm guid-routing-order

Disables the GUID routing order feature and cleans GUID routing order list.

Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.8008
Role	admin
Example	`switch (config) # no ib sm guid-routing-order`
Related Commands	ib sm guid-routing-order-no-scatter
Notes	

show ib sm guid-routing-order

show ib sm guid-routing-order

Displays current GUID routing order list.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.8008
Role	admin

Example	`switch (config) # show ib sm guid-routing-order`
	
	`1: E4:1D:2D:03:00:3D:5E:85`
	`2: E4:1D:2D:03:00:3D:5E:82`
	`3: E4:1D:2D:03:00:3D:5E:81`
	`4: E4:1D:2D:03:00:3D:5E:84`
	`5: E4:1D:2D:03:00:3D:5E:86`
	`6: E4:1D:2D:03:00:3D:5E:87`
	`7: E4:1D:2D:03:00:3D:5E:90`
	`8: E4:1D:2D:03:00:3D:5E:88`
	`9: E4:1D:2D:03:00:3D:5E:83`

Related Commands	ib sm guid-routing-order-no-scatter
Notes	

ib sm guid-routing-order-no-scatter

	ib sm guid-routing-order-no-scatter **no ib sm guid-routing-order-no-scatter** Enables randomization for destinations mentioned in GUID order list. The no form of the command disables randomization for destinations mentioned in GUID order list.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.6.8008
Role	admin
Example	`switch (config) # ib sm guid-routing-order-no-scatter`
Related Commands	ib sm guid-routing-order * ib sm scatter-ports
Notes	If scatter ports (randomization of the output port) is set to anything but zero, guid-routing-order-no-scatter defines whether or not randomization should be applied to the destination GUIDs mentioned in the GUID routing order list.

show ib sm guid-routing-order-no-scatter

	show ib sm guid-routing-order-no-scatter Displays the status of the GUID-routing-order-no-scatter feature
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.8008
Role	admin

Example	`switch (config) # show ib sm guid-routing-order-no-scatter`
	
	`guid_routing_order_no_scatter: disabled`

Related Commands	ib sm guid-routing-order * ib sm scatter-ports
Notes	

5.5.6.6 Bulk Update Mode

ib sm bulk-update enable

ib sm bulk-update enable
no ib sm bulk-update enable

Enables bulk update mode.
The no form of the command disables bulk update mode.

Syntax Description	N/A
Default	Disabled
Configuration Mode	config
History	3.6.8008
Role	admin
Example	`switch (config) # ib sm bulk-update enable`
Related Commands	show ib partition show ib sm bulk-update
Notes	

show ib sm bulk-update

	show ib sm bulk-update Displays the status of bulk-update mode.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.8008
Role	admin

Example	`switch (config) # show ib sm bulk-update`
	
	`ib sm bulk-update: enabled`

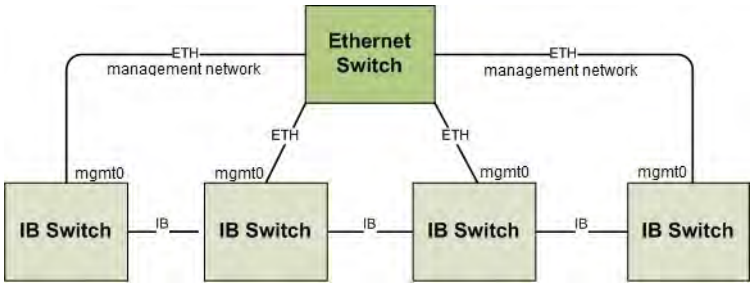
Related Commands	show ib partition ib sm bulk-update enable
Notes	

5.6 Subnet Manager (SM) High Availability (HA)

All nodes in an SM HA subnet must be of the same CPU type (e.g. x86), and must run the same MLNX-OS version.

High availability (HA) refers to a system or component that is continuously operational for a desirably extended period of time.

Figure 19: SM HA Subnet



Mellanox Subnet Manager (SM) HA reduces subnet downtime and disruption as it is continuously operational for a desirably long length of time. It assures continuity of the work even when one of the SMs dies. The database is synchronized with all the nodes participating in the InfiniBand subnet and a configuration change is prepared. The synchronization is done out-of-band using an Ethernet management network.

Mellanox SM HA allows the systems' manager to enter and modify all InfiniBand SM configuration of different subnet managers from a single location. It creates an InfiniBand subnet and associates all the Mellanox management appliances that are attached to the same InfiniBand subnet into that InfiniBand subnet ID. All subnet managers can be controlled, started, or stopped from this address.

All the nodes that participate in the Mellanox SM HA are joined to the InfiniBand subnet ID and once joined, the synchronized SMs are launched. One of the nodes is elected as Master and the others are Slaves (or down). Mellanox SM HA uses an IP address (VIP) that is always directed to the SM HA master to monitor the SM state and to verify that all configurations are executed.

5.6.1 Joining, Creating or Leaving an InfiniBand Subnet ID

When transitioning from standalone into a group or vice versa, a few seconds are required for the node state to stabilize. During that time, group feature commands (e.g. SM HA commands) should not be executed. To run group features, wait for the CLI prompt to turn into [standalone:master], [<group>:master] or [<group>:standby] instead of [standalone:*unknown*] or [<group>:*unknown*].

An InfiniBand subnet is formed by a network of InfiniBand nodes interconnected via InfiniBand switches. It includes all systems that can run an SM and is part of the SM HA domain. A switch that can potentially run an SM must be a member of an InfiniBand subnet ID to be associated with the Mellanox SM HA domain. An IB subnet is recognized by its ID which is used by the system to either join or leave the subnet.

Every system that is not associated to an existing IB subnet (has never been part of an IB subnet or has left an existing one) or does not have MLNX-OS license installed, is by default associated to a subnet called “Standalone”.

In order to create, join or leave an InfiniBand subnet, one may use the following commands:

- Create – “ib ha <IB_subnet_ID> ip <ip_addr> <netmask>”
- Join – “ib ha <IB_subnet_ID>”
- Leave – “no ib ha”

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

For further information see Section 5.6.5, “Creating and Adding Systems to an InfiniBand Subnet ID,” on page 805.

5.6.2 MLNX-OS Management Centralized Location

MLNX-OS centralized management infrastructure enables the user to configure or modify an existing configuration and monitor the subnet running status. MLNX-OS centralized management IP (VIP) is defined when a new subnet manager is created by running the command `ib ha <IB_subnet_ID> ip <ip_addr> <netmask>`. The created VIP is used as the current subnet master’s alias thus, assumes the same roles as the master.

The VIP always points to one of the systems part of the SM HA domain. It is always active even if one or more of the members are down. For example:

```
switch [standalone: master] (config) # ib ha subnet2 ip 192.168.10.110
255.255.255.0
switch [subnet2: master] (config) #
```

5.6.3 High Availability Node Roles

A node is an InfiniBand switch system. Every node member of an IB subnet ID has one of the following roles:

- Master – the node that manages SM configurations and provides services to the Virtual IP (VIP) addresses
- Standby – the node that replaces the Master node and takes over its responsibilities once the Master node is down
- Offline – has run an SM in the past and is currently offline, or it was created manually by the “ib smnode <node name> create” command. If the node has been removed from the environment, you can remove it from the list with the “no ib smnode xxx” command.

➢ ***To see the mode of the current node, look at the CLI prompt for the following format:***

```
<host name> [<subnet ID>:<mode>] [standalone: master] (config) #
```

For example:

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

To see a list of the existing nodes and details about the running state, run the command `show ib smnodes {brief}`.

5.6.4 Configuring MLNX-OS SM HA Centralized Location

The IP is used to configure or modify the existing configuration and monitor the subnet running status.

➢ ***To configure the IP:***

Step 1. Enter config mode. Run:

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

Step 2. Configure your IP using the `ib ha <IB_subnet_ID> ip <ip_addr> <netmask>` command.

```
switch [standalone: master] (config) # ib ha subnet2 ip 192.168.10.110 255.255.255.0
switch [subnet2: master] (config) #
```

5.6.5 Creating and Adding Systems to an InfiniBand Subnet ID

➢ ***To create and add systems to a subnet:***

Step 1. Log into the system from where you are creating the subnet.

Step 2. Enter config mode. Run:

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

Step 3. Create a new subnet using the `ib ha <IB_subnet_ID> ip <ip_addr> <netmask>` command.

```
switch [standalone: master] (config) # ib ha subnet2 ip 192.168.10.110 255.255.255.0
switch [subnet2: master] (config) #
```

You must run the `ib ha <IB_subnet_ID> ip <ip_addr> <netmask>` command **only once** per subnet ID.

Step 4. Log into the system that you are going to join to the new created subnet.

Step 5. Join the system to the subnet, using the `ib ha <IB_subnet_ID>` command.

```
switch [standalone: master] (config) # ib ha subnet2
switch [subnet2: standby] (config) #
```

5.6.6 Restoring Subnet Manager Configuration

In cases where the Subnet Manger configuration becomes corrupted or the subnet manager cannot raise any logical links it is suggested that you restore the default SM configuration.

➢ ***To restore subnet manager configuration:***

Step 1. Enter config mode. Run:

```
switch [subnet2: master] > enable
switch [subnet2: master] # configure terminal
switch [subnet2: master] (config) #
```

Step 2. Run the command `ib sm reset-config`.

```
switch [subnet2: master] (config) # ib sm reset-config
```

The asterisk in the example above (***switch-11a15e**) indicates the local system from where the command is running.

In order to receive information on the running state of a specific node one could run one of the following commands with its requested parameter:

- `show ib smnode <name> sm-licensed`
- `show ib smnode <name> sm-running`
- `show ib smnode <name> sm-state`
- `show ib smnode <name> sm-priority`
- `show ib smnode <name> active`
- `show ib smnode <name> ha-state`
- `show ib smnode <name> ha-role`

5.6.6.1 Subnet Manager Configuration

To configure the subnet manager, log into the centralized management IP (VIP). Once the SM configuration is created, the SM database is duplicated to the other nodes.

The SM **must** be configured from MLNX-OS centralized management IP (VIP). All the configurations that are not created or modified in the master node (using the VIP) are overridden by the master configuration.

The user can configure different SM parameters such as where to run the SM(s) or the SM priority by running the commands according to the desired action.

5.6.6.2 Mellanox High Availability and Opensm Handover/Failover

Mellanox Technologies products are fully compliant and interoperable with OpenSM.

Once an SM fails, the SM which takes over the subnet needs to reproduce the internal state of the failed master. Most of the information required is obtained by scanning the subnet and extracting the information from the devices. However, some information which is not stored directly in the network devices cannot be reproduced this way. InfiniBand management architecture limits such

information to data exchanged between clients (either user-level programs or kernel modules) and the Subnet Administration (SA) service (attached to the SM). The SA keeps this set of client registrations in an internal data structure called SA-DB. The SA-DB information includes the multicast groups, the multicast group members, subscriptions for event forwarding and service records.

The new SM may retrieve the SA-DB by requesting the clients to re-register with the SA or by obtaining a copy of the previous master SM internal SA-DB via an SA-DB dump file. The client-re-registration offers database correctness and the SA-DB dump file replication provides lower setup time. Client re-registration is required since the SA-DB may not be up-to-date on the registrations listed in the master SM.

Furthermore, since the SM does not maintain SA-DB information for unknown nodes, it is very possible that some of the SA-DB information relating to nodes momentarily disconnected from the master SM become purged. Therefore, these nodes must re-register with the new SM when they are reconnected (they receive a client-re-register request from the SM). Relying only on client re-registration is also non-optimal as it takes some time to recreate the entire SA-DB and the network state.

Mellanox SM HA replicates the SA-DB dump file from the current master SM to all the standby SMs running on Mellanox switches. The SA-DB dump file replication provides further optimization to the standby SM that becomes master.

Standby SM loads the existing SA-DB file the old master has used. By using the existing SA-DB the amount of processing needed on client re-registration is lessened resulting in a reduced time to complete setting up the network.

SM HA does not replace InfiniBand spec requirement for client reregistration.

5.6.7 Commands

ib ha

ib ha <IB_subnet_ID> [ip <IP address> <subnet mask> [force]]
no ib ha

Creates a subnet <IB_subnet_ID> with the specified IP.
The no form of the command removes this node from an InfiniBand subnet ID.

Syntax Description	IB subnet ID	Simple group name for shared IB config
	ip <IP address>	Assigns management IP address
	netmask	Netmask (e.g. 255.255.255.0 or /24)
	force	Joins if exists or creates if not
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ib ha my-subnet` `switch (config) #`	
Related Commands	show ib ha	
Notes	• A new subnet may be joined only after leaving the current one	

ib smnode

ib smnode <hostname> [create | disable | enable | sm-priority <priority>]
no ib smnode <hostname> [create | disable | enable | sm-priority]

Manages HA SM.
The no form of the command removes HA SM node configuration.

Syntax Description	hostname	Specifies <hostname> SM configuration to modify.
	create	Creates SM configuration for selected node.
	disable	Makes SM inactive on selected node.
	enable	Makes SM active on selected node.
	sm-priority <priority>	Sets SM selected node priority (0=low, 15=high).
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example	`switch (config) # ib smnode switch-1133ce create` `switch (config) #`	
Related Commands	show ib smnode show ib smnodes	
Notes		

show ib smnode

show ib smnode <hostname> {active | ha-role | ha-state | ip | sm-licensed | sm-priority | sm-running | sm-state}

Displays SM High availability information.

Syntax Description	hostname	Specifies <hostname> SM configuration to display.
	active	Displays whether <hostname> is currently active.
	ha-role	Displays the High Availability role of <hostname>. Possible return values are: offline, unknown, master, standby, or disabled.
	ha-state	Possible return values are: offline, init, searching, joining, online, creating, waiting, leaving, join-sync, failed, removed, or regroup.
	ip	Displays the local management IP address associated with the active node, <hostname>. If <hostname> is not active, the command displays “offline”.
	sm-licensed	Displays if <hostname> has an SM license. The command will display “active” only if <hostname> is currently active and has a license.
	sm-priority	Displays the SM priority for SM running on <hostname>.
	sm-running	Displays if <hostname> has an SM running. The command will display “active” (that is, SM is running) only if <hostname> is currently active, has a license, is enabled as a potential SM, is active as SM, and if there is a maximum of 2 SMs in the fabric.
	sm-state	Displays if SM is enabled to run on <hostname>.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example	`switch (config) # show ib smnode my-hostname sm-state`
	`enabled`
	`switch (config) #`	

Related Commands	show ib smnodes	
Notes		

show ib smnodes

show ib smnodes [brief]

Displays information about all the systems that are active or might be able to run SM.

Syntax Description	brief	Displays brief info on all HA nodes.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	

Example

```
switch (config) # show ib smnodes

HA state of switch infiniband-default
=====================================
IB Subnet HA name: Piranha-648-324
HA IP address:     10.7.6.238/22
Active HA nodes:   1

HA node local information
  Name:         43 (active)  <--- (local node)
  SM-HA state:  master
  SM Licensed:  yes
  SM Running:   stopped
  SM Enabled:   disabled
  SM Priority:  0
  IP:           10.7.7.43

HA node local information
  Name:         324-A (not active)
  SM Enabled:   enabled
  SM Priority:  10
  IP:           offline


switch (config) # show ib smnodes brief

HA state of switch infiniband-default
=====================================
IB Subnet HA name: Piranha-648-324
HA IP address:     10.7.6.238/22
Active HA nodes:   1

 ID      SM-HA state   IP              SM                 Priority
-------------------------------------------------------------------
*43       master        10.7.7.43       disabled           0
 324-A    offline       offline         enabled           10

switch (config) #
```

Related Commands	show ib smnode
Notes	

show ib ha

show ib ha [brief]

Displays information about all the systems that are active or might be able to run SM.

Syntax Description	brief	Displays HA information briefly.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Role	admin	
Example		

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

Related Commands	
Notes	

5.7 Fabric Inspector

5.7.1 Running Diagnostics

➢ ***To run ib fabric diagnostics:***

Step 1. Run `test ib fabric` to analyze the fabric.

```
switch (config) #  test ib fabric
% -W- Topology file is not specified.
    Reports regarding cluster links will use direct routes.
-I- Using port 0 as the local port.
-I- Discovering ... 25 nodes (24 Switches & 1 CA-s) discovered.


-I---------------------------------------------------
-I- Bad Guids/LIDs Info
-I---------------------------------------------------
-I- skip option set. no report will be issued

-I---------------------------------------------------
-I- Links With Logical State = INIT
-I---------------------------------------------------
-W- link with LOG=INI found at direct path "24,19,17,20"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=20
    To:   a Switch    PortGUID=0x0002c90200405f98 Port=18
-W- link with LOG=INI found at direct path "24,19,17,21"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=21
    To:   a Switch    PortGUID=0x0002c90200405fa0 Port=18
-W- link with LOG=INI found at direct path "24,19,17,22"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=22
    To:   a Switch    PortGUID=0x0002c90200405fa0 Port=17
-W- link with LOG=INI found at direct path "24,19,17,23"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=23
    To:   a Switch    PortGUID=0x0002c90200405f70 Port=17
-W- link with LOG=INI found at direct path "24,19,17,24"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=24
    To:   a Switch    PortGUID=0x0002c90200405f70 Port=18
-W- link with LOG=INI found at direct path "24,19,17,25"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=25
    To:   a Switch    PortGUID=0x0002c90200405f80 Port=17
-W- link with LOG=INI found at direct path "24,19,17,26"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=26
    To:   a Switch    PortGUID=0x0002c90200405f80 Port=18
-W- link with LOG=INI found at direct path "24,19,17,27"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=27
```

```
    To:   a Switch    PortGUID=0x0002c90200405f60 Port=17
-W- link with LOG=INI found at direct path "24,19,17,28"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=28
    To:   a Switch    PortGUID=0x0002c90200405f60 Port=18
-W- link with LOG=INI found at direct path "24,19,17,29"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=29
    To:   a Switch    PortGUID=0x0002c90200405f68 Port=17
-W- link with LOG=INI found at direct path "24,19,17,30"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=30
    To:   a Switch    PortGUID=0x0002c90200405f68 Port=18
-W- link with LOG=INI found at direct path "24,19,17,31"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=31
    To:   a Switch    PortGUID=0x0002c90200405f88 Port=17
-W- link with LOG=INI found at direct path "24,19,17,32"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=32
    To:   a Switch    PortGUID=0x0002c90200405f88 Port=18
-W- link with LOG=INI found at direct path "24,19,17,33"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=33
    To:   a Switch    PortGUID=0x0012c90200405fa9 Port=18
-W- link with LOG=INI found at direct path "24,19,17,34"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=34
    To:   a Switch    PortGUID=0x0012c90200405fa9 Port=17
-W- link with LOG=INI found at direct path "24,19,17,35"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=35
    To:   a Switch    PortGUID=0x0002c90200405f90 Port=17
-W- link with LOG=INI found at direct path "24,19,17,36"
    From: a Switch    PortGUID=0x0002c90200405b98 Port=36
    To:   a Switch    PortGUID=0x0002c90200405f90 Port=18

-I---------------------------------------------------
-I- PM Counters Info
-I---------------------------------------------------
-W- lid=0x0016 guid=0x0002c90200405a90 dev=48438 Port=23
      Performance Monitor counter     : Value
      symbol_error_counter            : 0xffff (overflow)

-I---------------------------------------------------
-I- Fabric Partitions Report (see ibdiagnet.pkey for a full hosts list)
-I---------------------------------------------------
-I-    PKey:0x7fff Hosts:1 full:1 partial:0

-I---------------------------------------------------
-I- IPoIB Subnets Check
-I---------------------------------------------------
```

```
-I- Subnet: IPv4 PKey:0x7fff QKey:0x00000b1b MTU:2048Byte rate:10Gbps SL:0x00
-W- Suboptimal rate for group. Lowest member rate:20Gbps > group-rate:10Gbps

-I---------------------------------------------------
-I- Bad Links Info
-I- No bad link were found
-I---------------------------------------------------

-I- Done. Run time was 511 seconds.
switch [subnet2: master] (config) #
```

Step 2. Run `show fabric sm` to list the subnet managers.

```
switch [subnet2: master] (config) #  show fabric sm

 SM - master
  Port=9 lid=0x0001 guid=0x0002c90200405f60 dev=48438 priority:0

 SM - standby
  The Local Device : Port=0 lid=0x0017 guid=0x0002c9020040c6d0    dev=48438 priority:0
 Port=10 lid=0x0018 guid=0x0002c9020040b2e8 dev=48438 priority:0
switch [subnet2: master] (config) #
```

Step 3. Run `show fabric pm` to display the performance counters' status.

```
switch [subnet2: master] (config) #  show fabric pm
% ------------------------------------------------------------------------------
Port=27 lid=0x0014 guid=0x0012c90200405a81 dev=48438
------------------------------------------------------------------------------
symbol_error_counter = 0x0
link_error_recovery_counter = 0x0
link_down_counter = 0x0
port_rcv_errors = 0x0
port_xmit_discard = 0x0
vl15_dropped = 0x0
port_rcv_constraint_errors = 0x0
local_link_integrity_errors = 0x0
port_xmit_constraint_errors = 0x0
excesive_buffer_errors = 0x0
port_xmit_data = 0x7a1d8
port_rcv_data = 0x7a1d8
port_xmit_pkts = 0x1b23
port_rcv_pkts = 0x1b23
port_rcv_remote_physical_errors = 0x0
port_rcv_switch_relay_errors = 0x0
------------------------------------------------------------------------------
Port=28 lid=0x0014 guid=0x0012c90200405a81 dev=48438
```

```
-----------------------------------------------------------------------------
symbol_error_counter = 0x0
link_error_recovery_counter = 0x0
link_down_counter = 0x0
port_rcv_errors = 0x0
port_xmit_discard = 0x0
vl15_dropped = 0x0
port_rcv_constraint_errors = 0x0
local_link_integrity_errors = 0x0
port_xmit_constraint_errors = 0x0
excesive_buffer_errors = 0x0
port_xmit_data = 0x7d7cf0
port_rcv_data = 0x7d7cf0
port_xmit_pkts = 0x1be2e
port_rcv_pkts = 0x1be2e
port_rcv_remote_physical_errors = 0x0
port_rcv_switch_relay_errors = 0x0
-----------------------------------------------------------------------------
Port=10 lid=0x0006 guid=0x0002c90200405f98 dev=48438
-----------------------------------------------------------------------------
symbol_error_counter = 0x0
link_error_recovery_counter = 0x0
link_down_counter = 0x0
port_rcv_errors = 0x0
...
...
...
-----------------------------------------------------------------------------
Port=26 lid=0x0014 guid=0x0012c90200405a81 dev=48438
-----------------------------------------------------------------------------
symbol_error_counter = 0x0
link_error_recovery_counter = 0x0
link_down_counter = 0x0
port_rcv_errors = 0x0
port_xmit_discard = 0x0
vl15_dropped = 0x0
port_rcv_constraint_errors = 0x0
local_link_integrity_errors = 0x0
port_xmit_constraint_errors = 0x0
excesive_buffer_errors = 0x0
port_xmit_data = 0x536d0
port_rcv_data = 0x536d0
port_xmit_pkts = 0x128a
port_rcv_pkts = 0x128a
```

```
port_rcv_remote_physical_errors = 0x0
port_rcv_switch_relay_errors = 0x0
switch [subnet2: master] (config) #
```

Step 4. Run `show interfaces ib` to display the status and configuration of the system's InfiniBand ports.

```
switch [subnet2: master] (config) #  show interfaces ib
Slot 1 port 1 state
        Logical port state  : Active
        Physical port state : 10
        Current line rate   : 40.0 Gbps
        Supported speeds    : 10
        Speed               : 10.0 Gbps
        Supported widths    : 10
        Width               : 12X
        Max supported MTUs  : 10
        MTU                 : 10
        VL capabilities     : 10
        Operational VLs     : 10

        RX bytes            : 255
        RX packets          : 255
        RX errors           : 255
        Symbol errors       : 255
        VL15 dropped packets: 255

        TX bytes            : 255
        TX packets          : 255
        TX wait             : 255
        TX discarded packets: 255

Slot 1 port 2 state
        Logical port state  : Active
        Physical port state : 10
        Current line rate   : 40.0 Gbps
        Supported speeds    : 10
        Speed               : 10.0 Gbps
        Supported widths    : 10
        Width               : 12X
        Max supported MTUs  : 10
        MTU                 : 10
        VL capabilities     : 10
        Operational VLs     : 10

        RX bytes            : 255
```

```
        RX packets          : 255
        RX errors           : 255
        Symbol errors       : 255
        VL15 dropped packets: 255

        TX bytes            : 255
        TX packets          : 255
        TX wait             : 255
        TX discarded packets: 255

Slot 1 port 3 state
...
...
Slot 1 port 36 state
        Logical port state  : Active
        Physical port state : 10
        Current line rate   : 40.0 Gbps
        Supported speeds    : 10
        Speed               : 10.0 Gbps
        Supported widths    : 10
        Width               : 12X
        Max supported MTUs  : 10
        MTU                 : 10
        VL capabilities     : 10
        Operational VLs     : 10

        RX bytes            : 255
        RX packets          : 255
        RX errors           : 255
        Symbol errors       : 255
        VL15 dropped packets: 255

        TX bytes            : 255
        TX packets          : 255
        TX wait             : 255
        TX discarded packets: 255

switch [subnet2: master] (config) #
```

5.7.2 Mapping GUIDs to Node Names

To replace module GUIDs and assign meaningful names to modules use the `ib nodename` command.

5.7.3 Importing ibdiagnet Fabric Data

The `ib fabric import` command imports a "snapshot" of fabric data. The imported file is an output of the ibdiagnet tool that has previously run on any node connected to the fabric. Prior to importing fabric data, it is required to run the ibdiagnet tool to produce fabric data files.

Note that there are two versions of the ibdiagnet tool. The earlier version produces three output files describing the fabric (`ibdiagnet.db`, `ibdiagnet.pm`, and `ibdiagnet.sm`), whereas the new version produces a single file (`ibdiagnet.db_csv`).

➢ ***To make an ibdiagnet run and import its fabric data:***

Step 1. Collect ibdiagnet data.

Run the following command from any node connected to the fabric. By default, ibdiagnet places the output file(s) under /tmp.

Old ibdiagnet version:

```
> ibdiagnet -csv -skip dup_guids zero_guids logical_state part ipoib -pm
```

New ibdiagnet version:

```
> ibdiagnet -pm
```

Step 2. Change directory to the ibdiagnet output directory.

The default directory is /tmp.

```
> cd <ibdiagnet output directory>
```

Step 3. Create an ibdiagnet output tarball. Run:

```
> tar cvzf <filename>.tgz ibdiagnet*
```

Step 4. Copy the tarball <filename>.tgz to the switch using the `image fetch` command. Run (in enable or config mode):

```
switch # image fetch scp://<user name>:<password>@<hostname>/<full path to <file-
name>.tgz>
100.0%[##########################################################################################
##################################################]
switch #
```

Step 5. Import the ibdiagnet file(s). Run:

```
switch [subnet2: master] (config) # ib fabric <filename>.tgz
Fabric data import successful
switch [subnet2: master] (config) #
```

5.7.4 Commands

ib fabric import

ib fabric import <filename>

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

Syntax Description	filename	The imported file. It is an output of the ibdiagnet tool that has previously run on any node connected to the fabric, and is assumed to be a zip file with a .gz or .tgz extension.
Default	N/A	
Configuration Mode	config	
History	3.1.1400	
Role	admin	
Example	`switch (config) # ib fabric import snapshot.tgz` `switch (config) #`	
Related Commands	show ib fabric node	
Notes	• To display the results of this import, you may run “show ib fabric” commands (e.g., “show ib fabric node type switch”) • Imported data can be displayed as long as you do not run the command “ib fabric refresh”, which overwrites the imported data • The import command cannot execute without the ibdiagnet.db file	

ib fabric monitor

	ib fabric monitor **no ib fabric monitor** Enables fabric monitoring. The no form of the command disables fabric monitoring.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.1400
Role	admin
Example	`switch (config) # ib fabric monitor`
Related Commands	show ib fabric monitor
Notes	

ib fabric nodenames

	ib fabric nodenames **no ib fabric nodenames** Imports fabric SysNames. The no form of the command removes imported SysNames.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.1400
Role	admin
Example	`switch (config) # ib fabric nodenames` `switch (config) #`
Related Commands	
Notes	

ib fabric refresh

ib fabric refresh

Takes a “snapshot” of the current fabric data.

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

ib fabric transceiver-info

	ib fabric transceiver-info enable **no ib fabric transceiver-info enable** Enables collection of active cable info. The no form of the command disables collection of active cable info.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.1.1400
Role	admin
Example	`switch (config) # ib fabric transceiver-info enable`
Related Commands	show ib fabric node
Notes	

test ib fabric

test ib fabric [route]

Perform infiniband fabric test

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

Example

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

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

-I- Duplicated GUIDs detection finished successfully

-I- Duplicated Nodes Descriptions detection finished successfully

-----------------------------------------------
Lids Check
-E- Lids Check finished with errors

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

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

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

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

-I- Ports counters value Check finished successfully

-I- Ports counters Difference Check will be skipped - pause time is zero
-----------------------------------------------
Nodes Information
-I- Lids Check failed, no response for some MADs can occurred
-W- Nodes Info retrieving finished with errors

-I- FW Check finished successfully

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

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

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

Related Commands
Notes

show ib fabric connections

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

Displays the ib fabric connections with optional relevant filter.

Syntax Description	attrib <speed/width>	Attribute of connection to filter on.
	details	Displays details info.
	type	Filter connections by type. • sw-2-sw-any - Any sort of switch to switch connection • sw-2-sw-int - Internal switch to switch connection • sw-2-sw-ext - External switch to switch connection • sw-2-ca - Switch to host connection • ca-2-ca - Host to host connection
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.1400	
	3.6.6000	Updated Example
Role	admin	
Example		
Related Commands		
Notes		

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

show ib fabric messages

show ib fabric messages

Displays the InfiniBand fabric error and warning messages.

Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.1400 3.7.00xx Updated Example
Role	admin

Example	`switch (config) # show ib fabric messages`
	
	`0:`
	`  Error  : No SM on fabric`
	
	`1:`
	`  Warning: Port m_key_violations found`
	
	`  Additional information:`
	`    port E4:1D:2D:03:00:5D:1E:A4-0001`
	
	`2:`
	`  Warning: Port m_key_violations found`
	
	`  Additional information:`
	`    port E4:1D:2D:03:00:68:EA:CA-0001`
	
	`3:`
	`  Warning: Loopback cable`
	
	`  Additional information:`
	`    port 7C:FE:90:03:00:A5:A4:60-0035`
	`    port 7C:FE:90:03:00:A5:A4:60-0036`

Related Commands	
Notes	

show ib fabric monitor

show ib fabric monitor [<type>]

Displays the InfiniBand fabric monitor admin state and statistics count.

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

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

Related Commands		
Notes		

show ib fabric node

show ib fabric node <system-guid>

Displays InfiniBand fabric info on one node.

Syntax Description	system-guid	GUID of node to be displayed
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.1400	
	3.6.6000	Updated Example
Role	admin	

Example	`switch (config) # show ib fabric node 7C:FE:90:03:00:6F:3A:6B`
	`System - 7C:FE:90:03:00:6F:3A:6A node 7C:FE:90:03:00:6F:3A:6B Node details:`
	`System GUID: 7C:FE:90:03:00:6F:3A:6A`
	`Type: CA standalone PCI 4115:713`
	`Ports: 1`
	`Cable support: Supported`
	`PCI Device ID: 4115`
	`PCI Vendor ID: 0x0002c9`
	`Base version: 1`
	`Class version: 1`
	`Revision: 0`
	`Partition cap: 128`
	`Descriptions: fit152 HCA-6`	

Related Commands		
Notes		

show ib fabric node ports

show ib fabric node <system-guid> ports

Displays InfiniBand fabric and port info for this node.

Syntax Description	system-guid	GUID of node to be displayed
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.1400	
	3.6.6000	Updated Example
Role	admin	

Example

```
switch (config) # show ib fabric node 7C:FE:90:03:00:6F:3A:6B ports
System - 7C:FE:90:03:00:6F:3A:6A node 7C:FE:90:03:00:6F:3A:6B Node details:
  System GUID:     7C:FE:90:03:00:6F:3A:6A
  Type:            CA  standalone PCI 4115:713
  Ports:           1
  Cable support:   Supported
  PCI Device ID:   4115
  PCI Vendor ID:   0x0002c9
  Base version:    1
  Class version:   1
  Revision:        0
  Partition cap:   128
  Descriptions:    fit152 HCA-6

------------------------------------------------------------------------------
Type     Port                          Desc               State    Rate
------------------------------------------------------------------------------
CA       7C:FE:90:03:00:6F:3A:6B-0001    Port 1             Link Up  100 Gbps
```

Related Commands	
Notes	

show ib fabric nodes

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

Displays InfiniBand fabric info on all nodes with filtering options.

Syntax Description	cable-options	Filters the list by cable type: • errors - Node with cable errors • no-errors - Node with no cable errors • supports - Node support active cables • no-support - Node does not support active cables
	role-options	Filters the list by role: • multi-chip - Systems with more than 1 nodes • single-chip - Systems with 1 node • leaf - Leaf node • spine - Spine node • <system> - Any supported system
	system-type	Filters the list by system type: • switch - Switches only • host - Hosts only • router - Routers only • unknown - Unknowns systems only
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.1400	
	3.6.6000	Updated Example
Role	admin	
Example		
Related Commands		
Notes		

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

show ib fabric port

show ib fabric port <port-guid>

Displays InfiniBand fabric info on one port in the fabric.

Syntax Description	port-guid	GUID of port to be displayed
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.1400	
	3.6.6000	Updated Example
Role	admin	

Example

```
switch (config) # show ib fabric port 7C:FE:90:03:00:6F:3A:6B-0001
System - Model  Node 7C:FE:90:03:00:6F:3A:6A port
7C:FE:90:03:00:6F:3A:6B-0001:
  Capabilities:          [Trap,SL_Map,sys-
GUID,Cbl_Info,Ext_Spd,Ext_CM2,CM,VendClass,CapMask,Rereg,Lcl_No-
tice,MC_Pkey_Trp]
  Type:                  CA
  Port state:            Link Up
  Speed:                 25 Gbps
  Supported speeds:      2.5 / 5 / 10 / 10 (FDR10) /14 / 25 Gbps
  Width:                 4X
  Supported widths:      1X, 4X
  Operational VLs:       VL0 - VL3
  VL capabilities:       VL0 - VL3
  LID:                   2
  LMC:                   0
  M-Key:                 00:00:00:00:00:00:00:00
  Lease period:          0
  Subnet prefix:         FE:80:00:00:00:00:00:00
  HOQ lifetime:          About   4 uS
  LID of master SM:      1 (SL 0)
  SM on port:            No
  Port GUID:             7C:FE:90:03:00:6F:3A:6B
  System GUID:           7C:FE:90:03:00:6F:3A:6A
  MTU:                   4096
  Max supported MTUs:    4096
  VL arbitration high:   8
  VL Arbitration low:    8
  VL high limit:         4
  VL stall count:        0
  Has errors:            true
  Has traffic:           true

Data traffic statistics:
  Xmit frames:           25032
  Recv frames:           25033
  Xmit bytes:            7209216
  Recv bytes:            7209504

Non-zero error counters:
```

Related Commands
Notes

show ib fabric ports

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

Displays InfiniBand fabric info on all ports with filtering options.

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

Default	
Configuration Mode	Any command mode
History	3.1.1400 3.6.6000 Updated Example
Role	admin

Example	`switch (config) # show ib fabric ports`
	`----------`
	`System GUID Type Port Desc State Rate`
	`----------`
	`F4:52:14:03:00:44:87:C0 SW F4:52:14:03:00:44:87:C2-0000 Switch port 0 Link Up 10 Gbps`
	`F4:52:14:03:00:44:87:C0 SW F4:52:14:03:00:44:87:C2-0001 Port 1 Polling Up to 10 Gbps`
	`F4:52:14:03:00:44:87:C0 SW F4:52:14:03:00:44:87:C2-0002 Port 2 Polling Up to 10 Gbps`
	`F4:52:14:03:00:44:87:C0 SW F4:52:14:03:00:44:87:C2-0003 Port 3 Polling Up to 10 Gbps`

Related Commands	
Notes	

show ib fabric sys

show ib fabric sys [config <config> | type <type>]

Displays list of all systems on the fabric.

Syntax Description	config	Configuration of system according to which to filter
	type	Type of system according to which to filter
Default	N/A	
Configuration Mode	Any command mode	
History	3.6.6000	
Role	admin	
Example	`switch (config) # show ib fabric sys`	

```
---------------------------------------------------------------------------------------
System GUID                         Model      Port Count      Type       Node Count
---------------------------------------------------------------------------------------
F4:52:14:03:00:71:55:30                        36              SW         1 node
7C:FE:90:03:00:6F:3A:6A                        1               host       1 node
7C:FE:90:03:00:2E:A2:B8                        1               host       1 node
```

Related Commands	
Notes	

show ib fabric system

show ib fabric system <system-guid>

Displays InfiniBand fabric info on a specific system.

Syntax Description	system-guid	GUID of system to be displayed
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.1400	
	3.6.6000	Updated Example
Role	admin	

Example	`switch (config) # show ib fabric system F4:52:14:03:00:71:55:30`
	`System - F4:52:14:03:00:71:55:30:`
	`  System:  36 port SW`
	`  Element count:  1`
	`  Description:  SB7800`	

Related Commands		
Notes		

show ib fabric system nodes

show ib fabric system <system-guid> nodes

Displays InfiniBand fabric info on a specific system as well as a list of node info.

Syntax Description	system-guid	GUID of system to be displayed
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.1400	
	3.6.6000	Updated Example
Role	admin	
Example		
Related Commands		
Notes		

```
switch (config) # show ib fabric system F4:52:14:03:00:71:55:30 nodes
System - F4:52:14:03:00:71:55:30:
  System:          36 port SW
  Element count:   1
  Description:     SB7800

------------------------------------------------------------------------
Node GUID                       Role       Ports  Type    Description
------------------------------------------------------------------------
F4:52:14:03:00:71:55:30         standalone  36    SW      PCI 52000:713
```

show ib fabric system ports

show ib fabric system <system-guid> ports

Displays InfiniBand fabric info on a specific system as well as a list of port info.

Syntax Description	system-guid	GUID of system to be displayed
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.1400	
	3.6.6000	Updated Example
Role	admin	

Example

```
switch (config) # show ib fabric system F4:52:14:03:00:71:55:30 ports
System - F4:52:14:03:00:71:55:30:
  System:          36 port SW
  Element count:   1
  Description:     SB7800

------------------------------------------------------------------------------
Type     Port                            Desc               State    Rate
------------------------------------------------------------------------------
SW       F4:52:14:03:00:71:55:30-0000    Switch port 0      Link Up  10 Gbps
SW       F4:52:14:03:00:71:55:30-0001    Port 1             Link Up  100 Gbps
SW       F4:52:14:03:00:71:55:30-0002    Port 2             Link Up  100 Gbps
SW       F4:52:14:03:00:71:55:30-0003    Port 3             Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0004    Port 4             Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0005    Port 5             Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0006    Port 6             Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0007    Port 7             Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0008    Port 8             Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0009    Port 9             Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0010    Port 10            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0011    Port 11            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0012    Port 12            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0013    Port 13            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0014    Port 14            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0015    Port 15            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0016    Port 16            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0017    Port 17            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0018    Port 18            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0019    Port 19            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0020    Port 20            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0021    Port 21            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0022    Port 22            Polling  Up to 100 Gbps
SW       F4:52:14:03:00:71:55:30-0024    Port 23            Link Up  56 Gbps
...
```

Related Commands	
Notes	

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

Mellanox switch systems comply by default with NIST SP 800-131A as described in the table below.

Table 41 - Supported Event Notifications and MIB Mapping

Component	Configuration	Command
HTTP	HTTP disabled	no web http enable
HTTPS	HTTPS enabled	no web https enable
	SSL ciphers = TLS1.2	web https ssl ciphers all
	SSL renegotiation disabled	web https ssl renegotiation enable
SSH	SSH version = 2	ssh server min-version 1
	SSH ciphers = aes256-ctr, aes192-ctr, aes128-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com	no ssh server security strict

A.1 Overview

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

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

A.2 Web Certificate

MLNX-OS 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-algo-
rithm sha256
```

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

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

A.5 SSH

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

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

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

The following ciphers are disabled for SSH when strict security is enabled:

- 3des-cbc
- aes256-cbc
- aes192-cbc
- aes128-cbc
- arcfour
- blowfish-cbc
- cast128-cbc
- rijndael-cbc@lysator.liu.se

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, MLNX-OS supports HTTPS encryption using TLS1.2 only. Working in TLS1.2 mode also bans MD5 ciphers which are not allowed per NIST 800-131a. In strict mode, the switch supports encryption with TLS1.2 only with the following supported ciphers:

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

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

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

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

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

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

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

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

```
switch (config)# show web
Web User Interface:
 Web interface enabled: yes
 HTTP enabled: yes
 HTTP port: 80
 HTTP redirect to HTTPS: no
 HTTPS enabled: yes
 HTTPS port: 443
 HTTPS ssl-ciphers: TLS1.2
 HTTPS certificate name: default-cert
 Listen enabled: yes
 No Listen Interfaces.

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

Web file transfer proxy:
 Proxy enabled: no

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

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

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

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

A.7 LDAP

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

- DHE-DSS-AES128-SHA256
- DHE-RSA-AES128-SHA256
- DHE-DSS-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256

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

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

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

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

Appendix B: Splunk Integration with Mellanox Products

Splunk automatically clusters millions of log records in real time back into their patterns and finds connections between those patterns to form the baseline flows of each software individually, thus enables you to search, monitor and analyze that data to discover powerful insights across multiple use cases.

This appendix provides a guide on the first steps with Splunk and helps you to begin enjoying reduced time in detecting and resolving production problems.

B.1 Getting Started with Splunk

Step 1. Download Splunk and extract the Splunk Enterprise version. (Splunk software is available as an RPM or TGZ.)

Step 2. Create a Splunk User /group. Run:

```
[root@server] groupadd splunk
[root@server] useradd -d /opt/splunk -m -g splunk splunk
```

Step 3. Splunk installation. Run:

```
[root@server] tar -xzvf splunk-7.0.0-c8a78efdd40f-Linux-x86_64.tgz
[root@server] ls
```

Step 4. A new folder called Splunk is created.

```
[root@server] cp -rp splunk/* /opt/splunk/
[root@server] chown -R splunk: /opt/splunk/
[root@server] su - splunk
[splunk@server] cd bin
[splunk@server] ./splunk start --accept-license
```

Now you can access your Splunk WebUI at http://IP:8000/ or http://hostname:8000/. You need to make sure that port 8000 is open in your server firewall.

B.2 Switch Configuration

In this example we are not using the default UDP port 514 to show that any other port can be also used.

Step 5. In order to add a task, the switch must be configured to send logs to our Splunk server. Run:

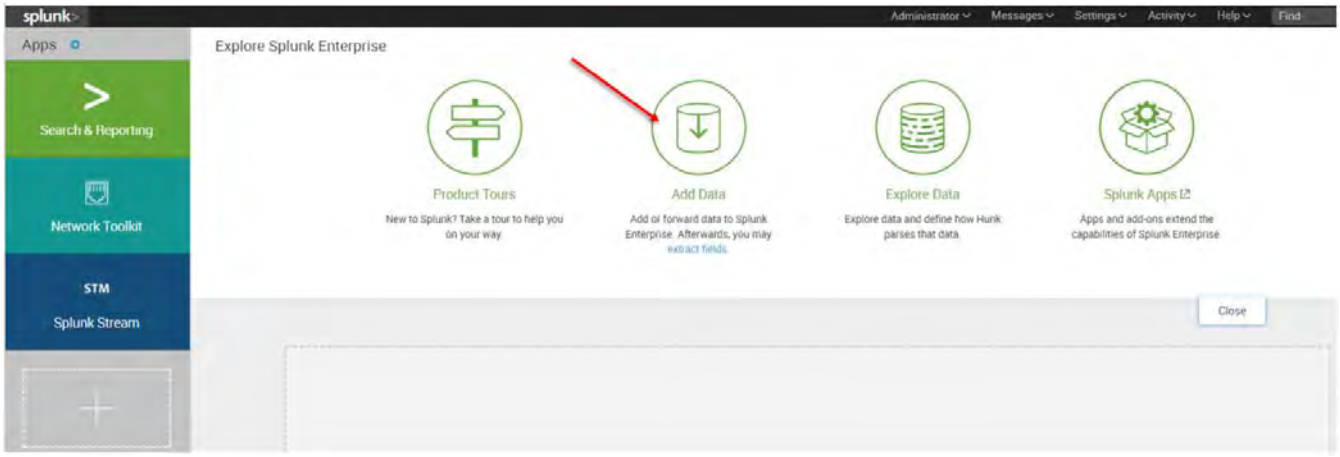
```
switch > enable
switch # configure terminal
switch (config) # show snmp
SNMP enabled:         yes
SNMP port:            161
System contact:
System location:

Read-only communities:
   public
```

```
Read-write communities:
   (none)

Interface listen enabled: yes
No Listen Interfaces.

switch (config) # snmp-server host 10.212.23.1 informs port 8597
switch (config) # snmp-server host 10.212.23.1 traps port 8597
switch (config) # snmp host 10.212.23.1 informs 8597
switch (config) # snmp host 10.212.23.1 traps  8597


Summary configuration:


switch (config) # show running-config
## Logging configuration
##
   logging 10.212.23.1
   logging 10.212.23.1 port 8597
   logging 10.212.23.1 trap info
   logging 10.212.23.1 trap override class events priority err
   logging monitor events notice
   logging receive
## SNMP configuration
no snmp-server host 10.209.21.221 disable
snmp-server host 10.209.21.221 traps port 8597 version 2c
no snmp-server host 10.212.23.1 disable
snmp-server host 10.212.23.1 traps port 8597 version 2c 8597
```

B.3 Adding a Task

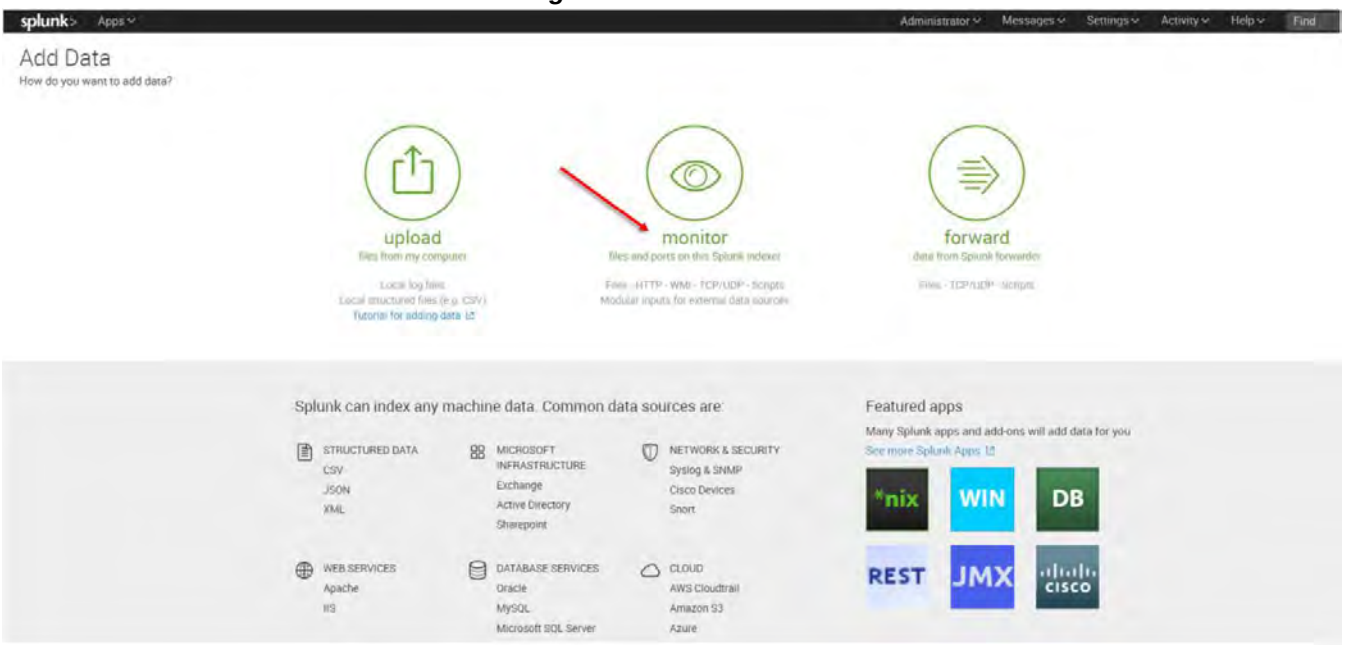
Step 6. The first screen encountered after signing into the Splunk WebUI includes the “Add Data” icon.

Figure 20: Add Data Option



Step 7. The “Add Data” tab opens up with three options: Upload, Monitor, and Forward. Here our task is to monitor a folder, so we click Monitor. to proceed

Figure 21: Monitor Icon



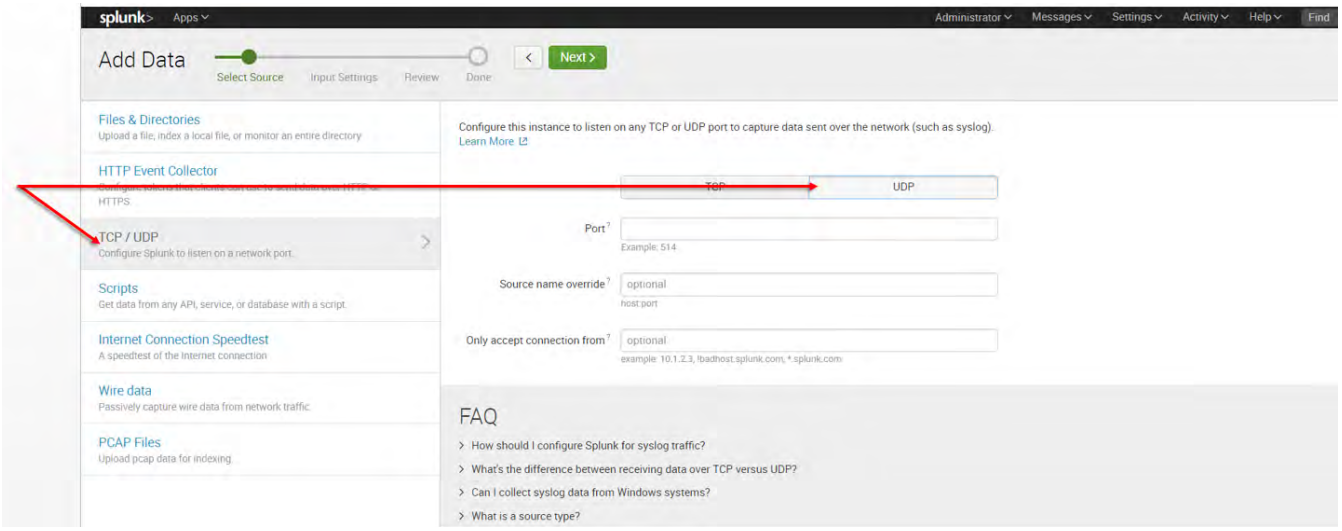
In the Monitor option, the following four categories are available:

- File & Directories: Monitor files/folders
- HTTP Event Collector: Monitor data streams over HTTP
- TCP/UDP: Monitor service ports
- Scripts: Monitor scripts

B.4 Retrieving Data from TCP and UDP Ports

Step 8. Per our current purpose, we choose TCP/UDP option.

Figure 22: TCP/UDP



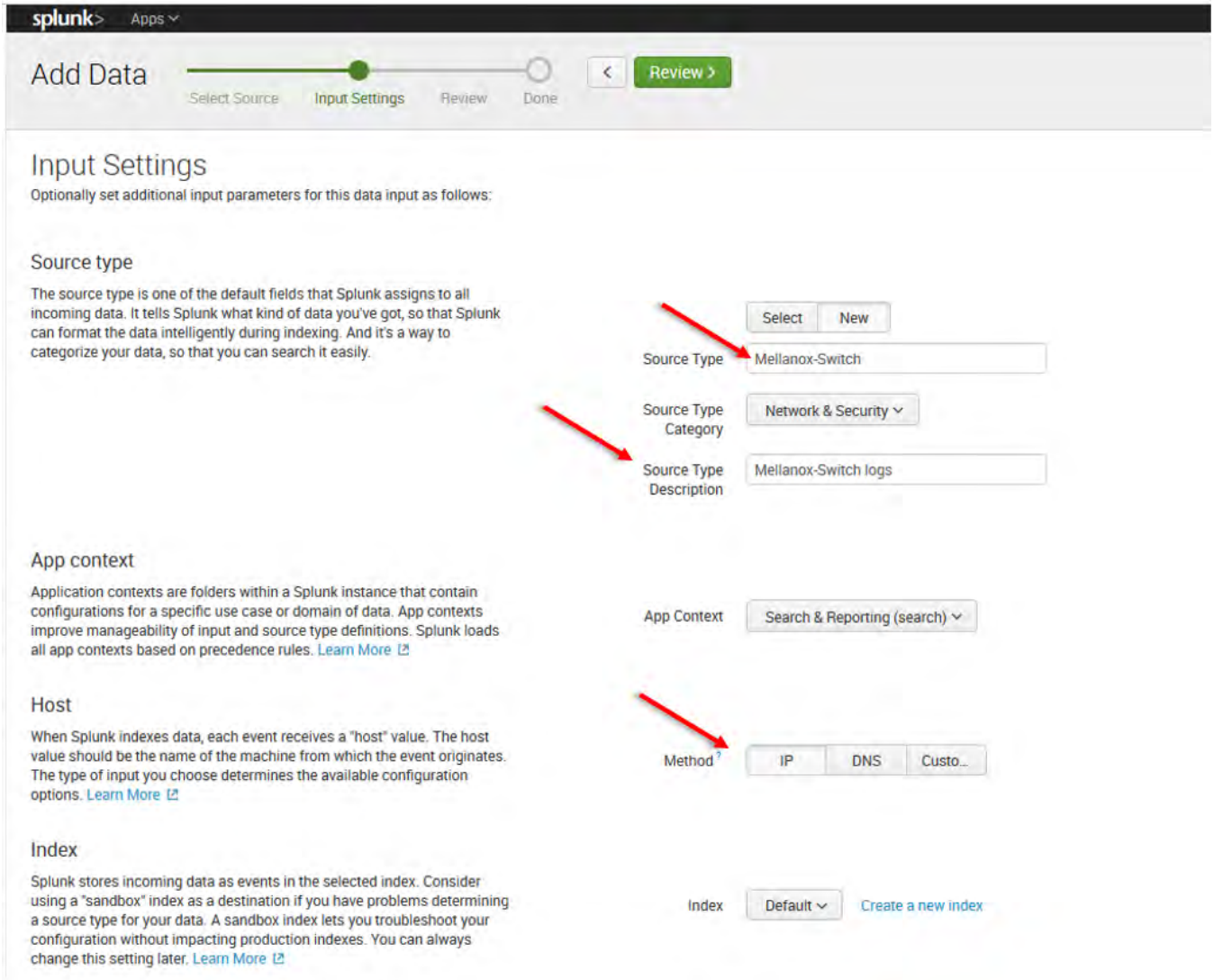
Step 9. Click the TCP or UDP button to choose between a TCP or UDP input, and enter a port number in the "Port" field.

Step 10. In the "Source name override" field, enter a new source name to override the default source value, if required.

Figure 23: TCP/UDP Fields

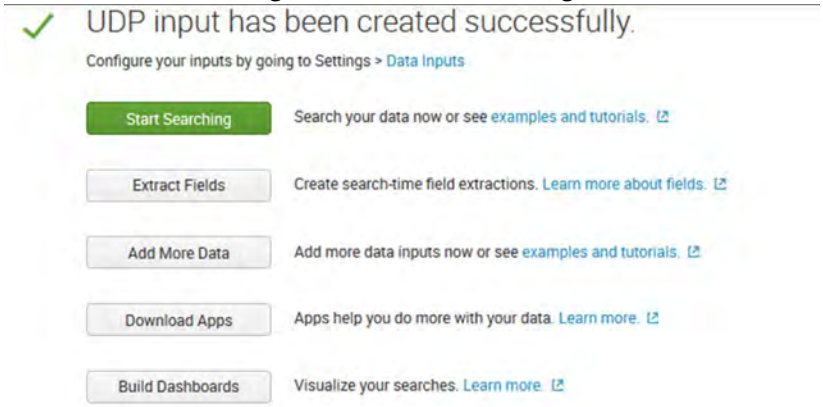
Step 11. Click “Next” to continue to the Input Settings page where we will create a new source type called Mellanox-Switch.

Figure 24: Input Settings



Step 12. Click Next > Review > Done > Start Searching

Figure 25: Start Searching



B.5 SNMP Input to Poll Attribute Values and Catch Traps

SNMP represents an incredibly rich source of data that you can get into Splunk for visibility across a very diverse IT landscape.

SNMP agents may also send notifications, called Traps, to an SNMP trap listening daemon.

B.5.1 Getting Started

Browse to Splunkbase and download the SNMP Modular Input from https://splunkbase.splunk.com/app/1537/.

To install, simply untar the file to SPLUNK_HOME/etc/apps and restart Splunk.

B.5.2 Configuration

Login to the Splunk WebUI and go to Manager > Add Data > Monitor > SNMP > New, and set up your input data.

Figure 26: SNMP

Figure 27: SNMP Attributes Polling Settings

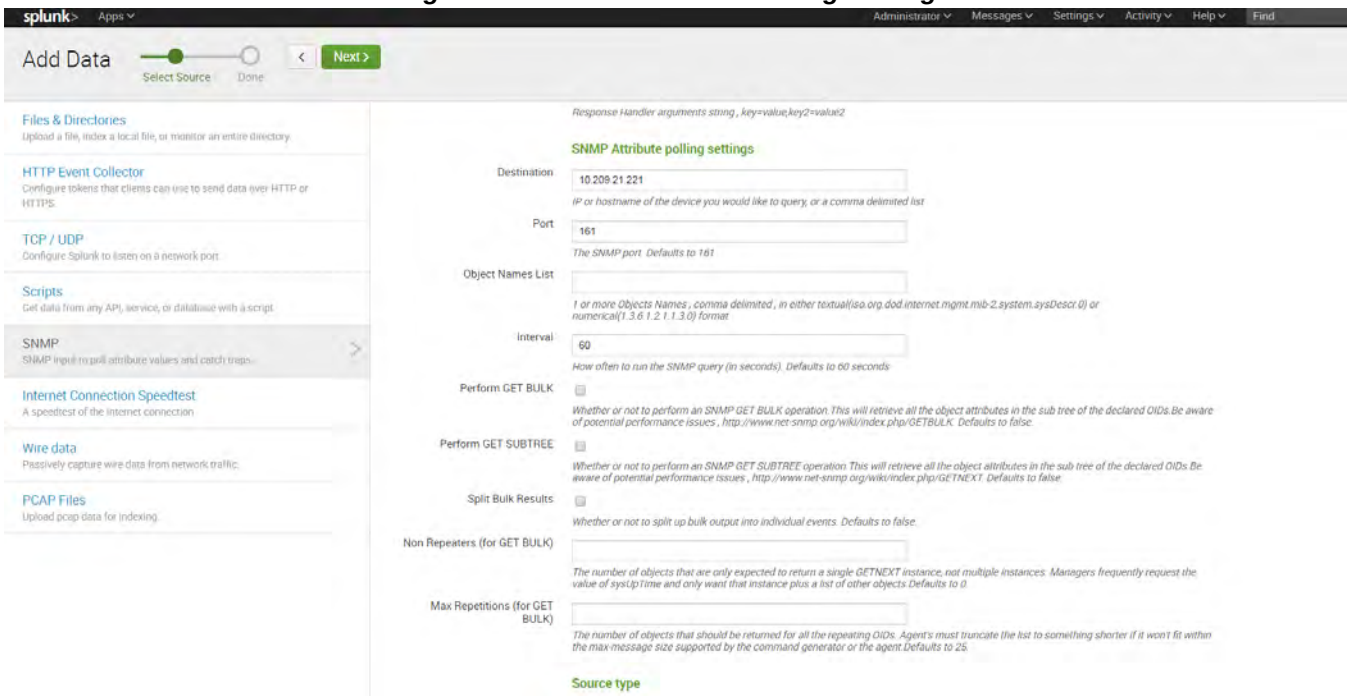
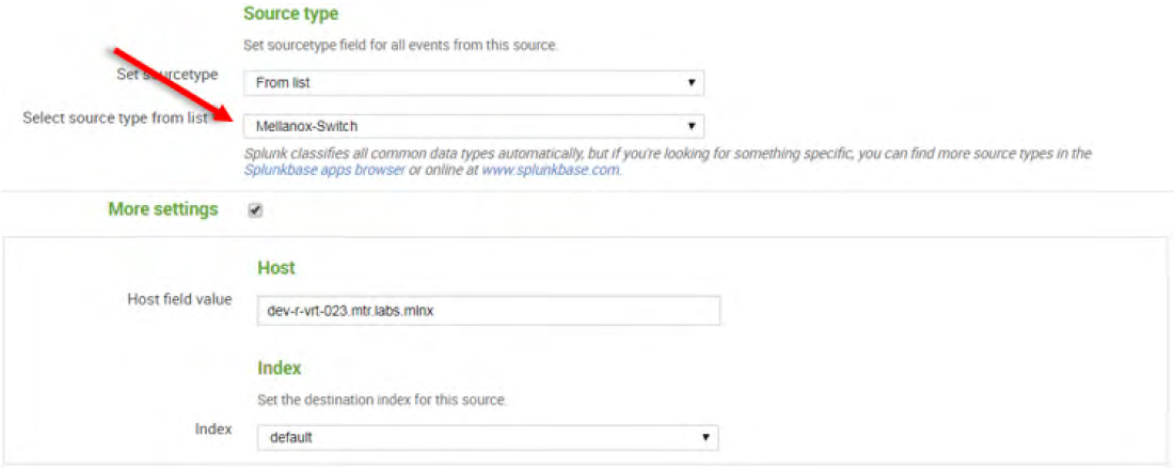
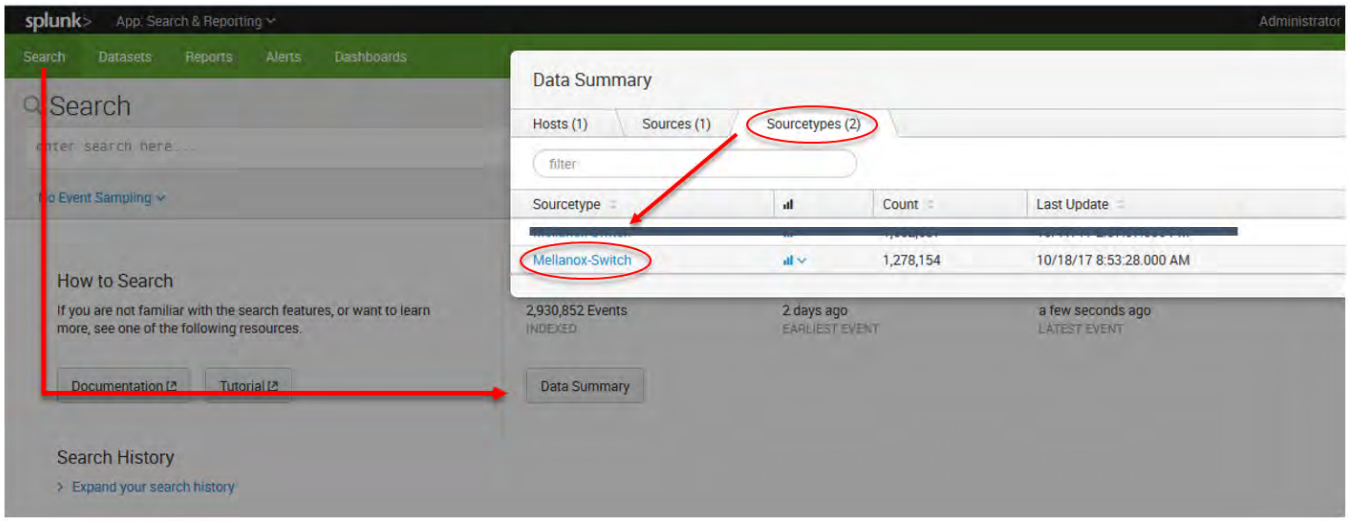


Figure 28: SNMP Attributes Polling Settings



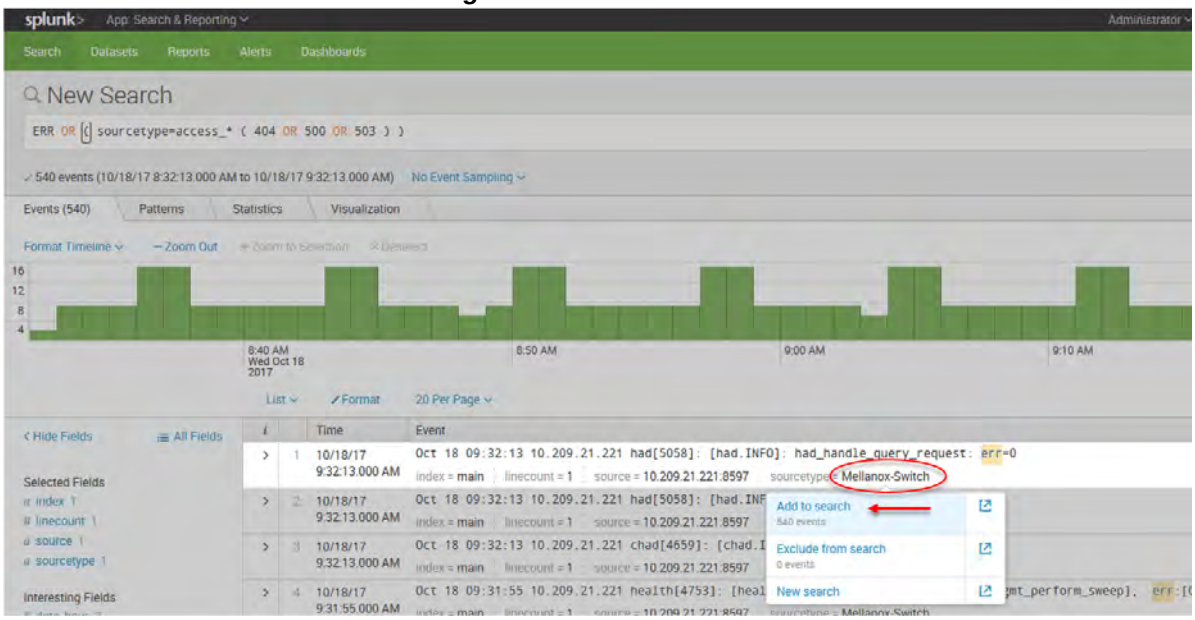
Step 13. After configuration is complete it is recommend to run Mellanox-Switch again: Search > Data Summary > Sourcetypes > Mellanox-Switch.

Figure 29: Mellanox-Switch



Step 14. Select “Mellanox-Switch” and “Add to search”.

Figure 30: Add to Search



Step 15. You can add to search any value that is relevant for you.

Figure 31: Search Options

Patterns can be viewed not on real time and you can create alert on most repeatable events.